POLITECNICO DI TORINO

Corso di Laurea Magistrale
in Ingegneria Informatica (Computer Engineering)

Tesi di Laurea Magistrale

Blockchain per la filiera alimentare: un'applicazione decentralizzata per il tracciamento dei fondi Europei destinati al pascolo

---

Relatore:
Fabrizio Lamberti
Correlatore:
Valentina Gatteschi
Tutor Aziendale:
Serena Ambrosini
(Consoft s.p.a)

Candidato:
Alessandro Pallante

Sessione di Ottobre 2020

Ognuno è un genio.
Ma se si giudica un pesce dalla sua abilità
di arrampicarsi sugli alberi lui passerà
tutta la sua vita a credersi stupido
Albert Einstein

Indice

Elenco delle figure

Elenco delle tabelle

Abstract

Dopo poco più di dieci anni dalla sua nascita, la Blockchain si presenta come una tecnologia non più conosciuta solamente da un ristretto gruppo di esperti e conoscitori della materia, ma da un pubblico ben più ampio.
Gli attori, interessati e coinvolti nell'innovazione tecnologica, che questo fenomeno ha portato, sono aumentati considerevolmente in relazione alla comprovata efficienza che la Blockchain ha dimostrato di perseguire in vari ambiti applicativi.
Nello specifico, questa tecnologia risulta essere particolarmente conveniente e utile nel settore agroalimentare e agro-produttivo. Infatti, a fronte di un costante aumento della complessità della filiera alimentare che la società moderna esige, la trasparenza e la tracciabilità sono state fortemente compromesse e numerose sono state le richieste di visibilità e chiarezza da parte dei produttori e dei consumatori. In tal senso, l'applicazione della Blockchain si è rivelata importante per fornire una risposta valida e concreta: monitorare passo dopo passo il ciclo del prodotto assicurando così una tracciabilità più chiara e trasparente della filiera, impedendo la diffusione di elementi contraffatti che contaminano il processo nel suo insieme.
Nel presente lavoro, si è voluto approfondire il ruolo della Blockchain definito all'interno del progetto di ricerca PININ della Regione Piemonte, in linea con le direttive Europee (*Smart Specialisation Strategy - S3*) per le strategie di crescita territoriali, le quali mirano a preservare e garantire la qualità dei prodotti alimentari piemontesi. Per rispettare questo principale obiettivo progettuale, in particolare è stata studiata e analizzata una soluzione per il tracciamento dell'erogazione dei fondi europei per l'allevamento del bestiame al pascolo. Sono state studiate le varie relazioni tra i diversi attori coinvolti e il rispettivo flusso dati che si genera per poter progettare una soluzione scalabile lungo tutto il processo. In particolare, sono stati implementati sia degli *smart contract* per la registrazione e la verifica delle informazioni ricavate dai collari del bestiame al pascolo, sia dei servizi esterni alla Blockchain, come un *Oracolo* e un'*applicazione decentralizzata* per poter interagire più facilmente con gli smart contract.

Capitolo 1

Introduzione

La *Blockchain* tecnologia spesso definita come "il futuro di Internet", rappresenta un vero e proprio stravolgimento infrastrutturale con possibili conseguenze in differenti settori. L'aspetto innovativo è legato alla possibilità di effettuare transazioni immutabili, di eliminare la necessità di ricorrere a terze parti autoritarie e di sviluppare applicazioni decentralizzate. Grazie alle sue caratteristiche, la Blockchain è destinata a cambiare molti aspetti della società moderna, e per questo motivo si trova al centro di discussioni tecnologiche ed economiche.
Nata ufficialmente alla fine del 2008 con la creazione di Bitcoin da parte dello pseudonimo Satoshi Nakamoto, il mondo della Blockchain e delle criptovalute è passato rapidamente da un argomento per pochi appassionati a una questione di fama mondiale. Tuttavia, le applicazioni della Blockchain non si limitano alle sole criptovalute, ma rappresentano una delle tecnologie più innovative a disposizione delle aziende per rinnovare processi, prodotti e transazioni.

Un settore particolarmente interessato da questa tecnologia innovativa è quello della catena di approvvigionamento. Al giorno d'oggi, si assiste ad un incremento costante di operazioni commerciali e rapporti di lavoro su scala internazionale. Ciò genera, nelle aziende coinvolte, un forte interesse verso la competitività e il miglioramento della catena produttiva esternalizzando i propri prodotti e le proprie risorse, che a loro volta aumentano la complessità dell'intera filiera produttiva.
Per gestire tutte le operazioni lungo la catena di approvvigionamento, dalla gestione dei contratti alla registrazione delle transazioni, le aziende hanno bisogno di visibilità e trasparenza e la tecnologia Blockchain, con le proprie caratteristiche, permette di risolvere queste problematiche.
Gli attori che partecipano alle attività coordinate di produzione e di creazione di valore aggiunto, necessarie alla realizzazione di prodotti alimentari, portano alla definizione della catena del valore alimentare (FVC), la quale si trova ad affrontare una delle sfide più urgenti: garantire la giusta nutrizione per tutti e affrontare il cambiamento climatico proteggendo la qualità dei prodotti.

L'attenzione in questo lavoro di tesi è posta sullo sviluppo di una soluzione che adotta la tecnologia Blockchain per offrire un servizio di trasparenza e fiducia tra le parti coinvolte ai fini di mantenere alta la qualità del prodotto finale.
Grazie alla Blockchain i prodotti possono essere monitorati in tempo reale durante il loro intero ciclo di vita lungo la filiera alimentare composta da produttori, trasformatori, distributori, dettaglianti e consumatori. Questo può portare a diversi benefici in termini di sicurezza alimentare. Senza la possibilità di verificare e raccogliere dati, le merci contraffatte possono muoversi in grande quantità lungo la catena di approvvigionamento creando un serio problema relativo al soddisfacimento delle esigenze e la fiducia dei consumatori.
La rivoluzione della Blockchain può cambiare radicalmente la catena alimentare globale e ogni prodotto può essere rintracciato in tempo reale dalla fattoria alla tavola. Sono tanti i fattori in gioco quando si tratta della scelta del cibo, l'aspetto, le origini e tutto ciò che influisce sulla sostenibilità lungo la filiera, come ad esempio la localizzazione dei capi al pascolo o la certezza circa la corretta esecuzione delle procedure amministrative.

Nonostante l'enorme interesse che la tecnologia Blockchain ha suscitato negli ultimi dieci anni, sono molte le aziende e gli enti di ricerca che stanno proseguendo con ulteriori indagini e sviluppi. Infatti, questo lavoro di tesi nasce proprio da un progetto di ricerca e innovazione tecnologica della regione Piemonte in linea con quelle che sono le direttive Europee (*Smart Specialisation Strategy - S3*) per le strategie di crescita territoriali. Il progetto PININ (PIemuNt chèINa) nasce dalla necessità di preservare e garantire la qualità dei prodotti alimentari piemontesi.

Il lavoro prende forma dalla realizzazione di uno dei casi dimostrativi del progetto PININ: la tracciabilità dell'erogazione dei fondi europei per gli allevamenti di bovini al pascolo. Nella prima parte della tesi, in particolare nel secondo capitolo (*Blockchain*), vi è una descrizione dettagliata della tecnologia blockchain in modo da poter comprendere al meglio le potenzialità e l'innovazione perseguita.
Nel terzo capitolo (*Food Chain: la blockchain nell'agroalimentare*), anch'esso descrittivo e di inquadramento al settore analizzato, è presente una descrizione dettagliata della catena del valore alimentare e l'illustrazione di come la tecnologia può immergersi nel settore agroalimentare. Viene inoltre realizzata una panoramica su tutto ciò che concerne lo stato dell'arte della tracciabilità alimentare, sia dal punto di vista della ricerca scientifica che da quello delle applicazioni commerciali già realizzate.
In seguito a questa prima parte che inquadra il problema di tesi analizzato, nel quarto capitolo si descrive il progetto di appartenenza (*Il progetto PININ*), dove viene presentato e descritto in dettaglio anche il caso d'uso specifico, con i relativi problemi e obiettivi realizzativi.

Negli ultimi capitoli viene fatta, inizialmente, una presentazione della progettazione e realizzazione dell'architettura implementata (Capitolo 5 - *Progettazione*) per poi passare ad una descrizione più dettagliata delle diverse componenti sviluppate. Infine, nel sesto capitolo (*Dettagli implementativi*) vengono descritti gli smart contract realizzati per il caso d'uso e vengono mostrate le altre strutture utilizzate, come, ad esempio, gli oracoli per una comunicazione con il mondo off-chain e l'applicazione decentralizzata per una più migliore comprensione e gestione da parte dell'utente.

Capitolo 2

Blockchain

Il concetto di "blockchain" viene introdotto per la prima volta da Satoshi Nakamoto, solo dodici anni fa, nel 2008, nel suo articolo "Bitcoin: a Peer-to-Peer Electronic cash System"[1]. Nel suo articolo Satoshi Nakamoto descrive in dettaglio tutta la struttura che deve avere il suo sistema decentralizzato, un sogno che sfocia nella idealizzazione della blockchain. Prima di capire bene cosa è la blockchain è importante sottolineare come il sistema Bitcoin e la blockchain siano due entità diverse e distinte, essendo Bitcoin solo una delle innumerevoli applicazioni odierne della blockchain.

2.1 Introduzione alla blockchain

Non è semplice definire in modo univoco la blockchain, infatti molte definizioni si soffermano sulla struttura stessa di quest'ultima, altre sulla parte tecnologica, altre ancora sulle implicazioni sociali che comporta. Una descrizione che cerca di racchiudere tutti gli aspetti può essere questa: "La Blockchain è una struttura digitale, decentralizzata e distribuita sulla rete, strutturata come una catena di blocchi immutabile, dove è possibile aggiungerne nuovi contenenti ulteriori informazioni ma non è possibile modificare o rimuovere blocchi precedentemente aggiunti alla catena. È controllata da sistemi crittografici e protocolli di consenso, in modo da garantire sicurezza e immutabilità. Ciò che ne risulta è un sistema aperto, neutrale, ma sicuro, con un potenziale nuovo livello di fiducia nelle applicazioni, introducendo un paradigma diverso nel modo in cui esse vengono realizzate, dando l'opportunità di innovare liberamente."
Il nucleo centrale della blockchain è il concetto di transazione, salvata nel registro distribuito (*Distributed Ledger*). In altri termini la blockchain è un registro distribuito, dove ogni transazione viene registrata e salvata andando così ad aggiungere

nuovi blocchi alla catena. Il concetto di *Ledger*[1] può a primo impatto ricordare quello di un database, ma ha una grande differenza, infatti, è vero che in entrambi si possono salvare i dati ma nel database è possibile aggiungere, cambiare e cancellare dati liberamente, mentre nel registro si può solo aggiungere.
Come citato poco sopra, le informazioni aggiunte al registro sono aggiunte attraverso i blocchi, i quali possono contenere più transazioni al proprio interno. Ognuno di essi contiene una prova matematica, generata dalla crittografia, che garantisce la sequenzialità dal blocco precedente ed è composto da due parti principali: un header e il body. In quest'ultimo sono contenute le transazioni, mentre nell'header, sono contenuti i campi di gestione del blocco stesso, come, ad esempio, il *PrevHash*, ovvero l'hash del blocco precedente, il *Timestamp* di quando la rete è giunta ad un consenso sulla sua validità, il *Merkle root* della lista di dati. Il risultato è una "catena di blocchi". Quindi i blocchi sono strutture dati aggiunte in modo sequenziale alla blockchain, un blocco alla volta.
Il tempo tra i blocchi è delimitato da una variabile programmata nel codice della rete chiamata *Block Time*, che è il tempo medio necessario alla rete per aggiungere permanentemente un nuovo blocco. L'hash crittografico collega i blocchi tra loro, quindi rappresenta il modo in cui si ottiene la "catena" nella catena di blocchi.

Come descritto nel libro di Tiana Laurence "Blockchain for Dummies" [2] la blockchain è composta da tre parti principali:

- *Block* - Blocco: una lista di transazioni registrate in un determinato periodo in un registro. Non tutte le blockchain hanno come obiettivo principale quello di registrare le transazioni nel minor tempo possibile, ma è garantito sempre che tutte le transazioni vengano registrate. A tal proposito ogni blockchain genera caratteristiche diverse in termini di dimensione, periodo e eventi di attivazione per i suoi blocchi;

- *Chain* - Catena: un hash che collega un blocco ad un altro, "incatenandoli" matematicamente insieme. In un certo senso è il collante che tiene unito una blockchain, ciò che rende possibile la veridicità dell'intero sistema attraverso l'*hash*. Quest'ultimo, spesso paragonato ad un'impronta digitale, viene creato a partire dai dati che si trovano nel blocco precedente, garantendo così un ordine temporale ai blocchi stessi;

- *Network* - Rete: La rete è composta da *Full Node*, paragonabili a dei computer che eseguono un algoritmo che mette in sicurezza la rete stessa. Ogni nodo contiene una registrazione completa di tutte le transazioni che sono state registrate in quella blockchain.

[1] registri, libri mastri

Ogni macchina[2] che è connessa alla rete rappresenta un nodo, ma è possibile fare una distinzione:

- Full Node: scarica e memorizza localmente una copia completa della blockchain. È in grado di controllare che ogni transazione e quindi ogni blocco segua le regole definite dal sistema. Ogni volta che compare un'anomalia, il blocco viene rifiutato. Un *Full Node*, potendo diffondere transazioni valide e ignorare quelle non valide, risulta essere indipendente. L'utilizzo di questo strumento ha dei vantaggi essendo sicuro, ma allo stesso tempo è reso scomodo dalla necessità di dover scaricare e memorizzare l'intera blockchain su una singola macchina;
- Light Node: non deve memorizzare completamente la blockchain dell'intera rete a cui appartiene, poiché riceve solo le informazioni necessarie. Ciò implica il fatto che la fiducia viene data ad una terza parte (un *Full Node*), in cambio però della facilità d'uso.

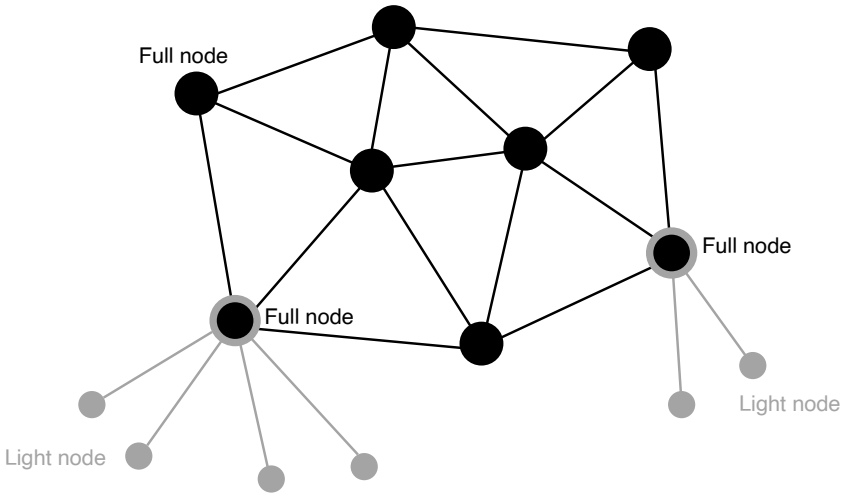

Figura 2.1. Rete distribuita con *Light Nodes*

Come si può vedere in Figura 2.1 l'intera rete assume una struttura articolata e distribuita, generando una connessione peer-to-peer. Tutti i nodi sono connessi

[2]computer, macchina automatizzata e programmabile in grado di elaborare dati e eseguire calcoli matematici

tra di loro, quindi ognuno agisce contemporaneamente come client (richiedente) e server (fornitore) per condividere e accedere alle risorse direttamente dagli altri. Ricevono e inviano le transazioni agli altri nodi, e le informazioni sono sincronizzate con tutti i nodi della rete specifica. In questo modo è possibile evitare il problema della doppia spesa, ovvero che la stessa "moneta" digitale venga spesa più di una volta, utilizzando i timestamp per registrare e confermare le transazioni in ordine cronologico.

2.1.1 Crittografia

Una delle principali discipline su cui si basa tutto il sistema di blockchain è la crittografia, per questo è importante capire di cosa si tratti e di come agisce sulla cifratura di informazioni.

La criptografia[3], è la scienza delle informazioni e delle comunicazioni sicure, rendendole accessibili solo a chi ne ha il permesso, attraverso l'uso di codici. Il prefisso *cripto*" significa "nascosto" e il suffisso *grafia* significa "scrittura", letteralmente la *scrittura nascosta*. Quindi ha come obiettivo quello impedire l'accesso non autorizzato sia in fase di scrittura che di lettura.
Esistono tre tipi di crittografia: simmetrica, asimmetrica e le funzioni di Hash

- Simmetrica: si tratta di un sistema di cifratura in cui il mittente e il destinatario del messaggio utilizzano un'unica chiave comune per cifrare e decifrare i messaggi. I sistemi a chiave simmetrica sono più veloci e semplici, ma è importante che il mittente e il destinatario si scambino la singola chiave di cifratura in modo sicuro, per evitare possibili attacchi del tipo "*man in the middle*"

- Asimmetrica: a differenza del tipo simmetrico, le chiavi per criptare e decriptare i dati sono diverse. Una coppia di chiavi viene utilizzata per cifrare e decifrare le informazioni. Per la cifratura si usa una chiave pubblica e per la decifratura si usa una chiave privata. Pur essendo la chiave pubblica nota a tutti, solo il destinatario effettivo del messaggio può decodificarlo perché solo lui conosce la chiave privata. L'uso di questo tipo di cifratura oltre allo scambio di messaggi cifrati ha permesso l'implementazione di altri servizi tra cui i sistemi a firma digitale, utilizzati per autenticare il mittente, e sistemi di non ripudio, ovvero sistemi dove attraverso la firma digitale un utente non può ripudiare/negare la paternità di un documento o comunicazione.

- Funzione di Hash: in questo algoritmo non viene utilizzata alcuna chiave per cifrare e decifrare le informazioni. Un valore di hash con lunghezza fissa

[3]crittografia

viene calcolato in base alle informazioni in chiaro ricevuto come input, il che rende impossibile il recupero dei contenuti del testo. Le funzioni di hash sono funzioni che ricevono come input il messaggio, o più in generale l'informazione, da cifrare e restituisce come output una stringa di n bit (*digest of message*) che apparentemente sembra casuale ma non lo è affatto. Infatti sottoponendo lo stesso messaggio alla funzione questa restituirà sempre lo stesso digest message; ma partendo dal digest message e conoscendo la funzione di hash a cui il messaggio originario è stato sottoposto non si è in grado di riottenerlo, se non con tecniche di *brute-force*. Matematicamente parlando le funzioni di hash sono funzioni non invertibili. Una funzione di hash deve avere delle caratteristiche:

- Determinismo: ricevuto in input uno stesso messaggio, l'output non cambia;
- Velocità computazionale: per ogni input risulta essere una funzione computazionalmente veloce;
- Effetto valanga: per input minimamente differenti, i valori di hash in output ottenuti sono molto differenti.

Sono diverse le applicazioni delle funzioni di hash nel campo della sicurezza informatica, infatti molti sistemi operativi le utilizzano per crittografare le password, in altri sistemi per generare firme digitali, in altri ancora per verificare esistenza di duplicati in strutture dati di tipo chiave-valore. Nella blockchain le funzioni di hash vengono sfruttate per il Proof of Work[4] nel calcolo dei blocchi validi, in particolare Bitcoin usa la funzione di hash *SHA-256*, mentre Ethereum sfrutta *KECCAK-256*. [3][4]

La crittografia può fornire diversi servizi di sicurezza come la riservatezza, l'integrità e l'autenticazione. La riservatezza si assume la responsabilità di assicurare che solo gli enti autorizzati abbiano accesso alle informazioni. L'integrità garantisce che le informazioni sono modificabili solo da entità autorizzate. L'autenticazione si assume la responsabilità di verificare l'identità o la validità di un messaggio [8]. Come facilmente intuibile, quindi, i servizi offerti dalla crittografia sposano perfettamente la filosofia e le caratteristiche principali del sistema blockchain.

2.2 Il consenso: la forza motrice della blockchain

La blockchain basa il suo funzionamento sulla fiducia che i diversi nodi hanno tra di loro e quindi dell'intero sistema. Grazie a questa fiducia riesce a garantire il suo

[4]vedi sezione 2.2.1

funzionamento senza l'intervento di un intermediario che faccia da garante tra le parti, e che imponga dei pagamenti di commissione, per le diverse transazioni tra i nodi. Questa fiducia viene generata principalmente da tre elementi chiave:

- Protezione e sicurezza dell'identità
- Controllo della proprietà
- Verifica e validazione dei dati

La blockchain quindi risulta essere uno strumento molto potente, in grado di autoregolarsi e autocorreggersi senza l'intervento di terze parti. Tutto ciò è reso possibile grazie agli algoritmi di consenso, i quali risultano essere diversi tra sistemi di blockchain, pur garantendo sempre tutte le caratteristiche che rendono quest'ultima uno strumento potenzialmente illimitato.

Cosa è il meccanismo di *consenso*? Il *consenso* è il processo continuo di un accordo che coinvolge diversi partecipanti (*Full Node*), tra loro diffidenti, ma ognuno con il proprio ruolo e le proprie responsabilità. L'idea di come una transazione venga validata dal sistema blockchain è riportato in Figura 2.2. Si noti che ogni blockchain ha il proprio algoritmo di consenso che porta all'accettazione o rifiuto di una transazione. Non esistendo, infatti, un nodo centrale che garantisca che i *Ledger* sui nodi distribuiti della rete siano tutti uguali è necessario avere protocolli per assicurare coerenza tra i registri nei diversi nodi al fine di raggiungere il consenso.
Ci sono tre diverse alternative che possono essere usate per risolvere il problema dell'assenza di un nodo centrale garante:

- Proof of work;
- Proof of stake;
- Proof of Authority.

2.2.1 Proof of work - *PoW*

La traduzione letterale è *prova di lavoro*, una visione più astratta può essere data come la notevole quantità di lavoro che i *miners*[5] devono compiere affinché un blocco possa essere aggiunto correttamente alla blockchain. Il Proof of Work, o PoW, è un algoritmo di consenso utilizzato da diversi sistemi blockchain - come Bitcoin, Ethereum, Litecoin [9]- per raggiungere un accordo decentralizzato. L'algoritmo

[5]minatori, potenze di calcolo che validano le transazioni

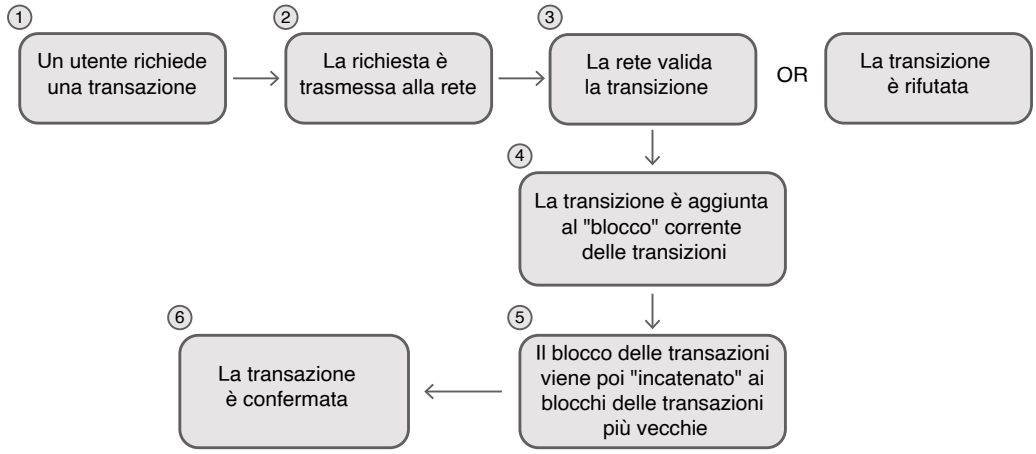

Figura 2.2. Come funzionano le blockchain

chiede a ogni nodo della rete di miner di calcolare un valore di hash dell'header del blocco da aggiungere. Il consenso richiede che il valore calcolato debba essere uguale o inferiore a un certo valore dato. La rete per garantire un lavoro continuo come quello svolto da miners, mette a disposizione un incentivo, delle "tasse", le *fee*[6]. Queste fee vengono retribuite al miner solo nel caso in cui il blocco viene minato con successo e sono pagate da chi ha compiuto le transazione appartenenti a quel blocco. Quando un nodo ottiene il relativo valore, tutti gli altri nodi devono confermare reciprocamente la correttezza del valore. Il primo miner che trova la soluzione e quindi riesce a minare il blocco lo annuncia alla rete. Dunque, la raccolta delle transazioni utilizzate per i calcoli viene approvata come risultato autenticato, che viene indicato da un nuovo blocco nella blockchain. Siccome sono molteplici i nodi che partecipano all'attività di mining può accadere che più di un nodo arrivi ad una soluzione e che questa venga accettata, generando così un fork di due blockchain. Nel protocollo PoW, in seguito la catena che diventa più lunga viene giudicata come quella autentica, cioè quella che la maggioranza dei minatori ha scelto come fidata e per questo ha continuato ad aggiungerci blocchi. La validità della blockchain quindi aumenta ogni qualvolta viene aggiunto un blocco, questo perché la modifica di un dato qualsiasi richiederebbe la sovrascrittura dell'intera catena, cosa computazionalmente sempre più complessa. La fiducia degli utenti si basa proprio su questo principio. [2]

[6]commissioni di transazioni, costo dell'utilizzo del servizio di rete

2.2.2 Proof of stake - *PoS*

L'algoritmo PoW necessita di un continuo processo di mining e quindi di un continuo consumo di elettricità, si pensi che il consumo di corrente elettrica di Bitcoin è dell'ordine dei terawattora. Proof of Stake rappresenta un'alternativa a risparmio energetico all'algoritmo PoW per il consenso. Questo algoritmo invece di chiedere ai miners di trovare un nonce[7] in uno spazio illimitato, richiede a quest'ultimi di bloccare nella rete una somma di valuta come fosse una "caparra". Il principio di selezione per aggiudicarsi il blocco da validare è scelto con due criteri: la quantità della valuta "bloccata" e per quanto tempo. Questo perché si è notato che utenti più ricchi sono meno propensi ad attaccare la rete, mentre con il parametro di assegnazione relativo al tempo si cerca di evitare lo scenario in cui i più ricchi vengano sempre scelti. L'algoritmo PoW presenta molte più applicazioni, soprattutto in sistemi di blockchain pubblici, però negli ultimi anni gli algoritmi PoS stanno prendendo sempre più piede sopratutto per le applicazioni in sistemi di blockchain privati (spesso implementati con Etherum il quale sta migrando proprio verso questo tipo di validazione), dove i membri della rete si conoscono tra loro e quindi possono utilizzare un consenso più leggero e veloce. [2][6]

2.2.3 Proof of authority - *PoA*

Proposto da Gavin Wood, co-fondatore di Ethereum, nel 2017, il PoA è l'algoritmo di consenso alla base delle bockchain consortili. Si basa proprio sullo sfruttare un numero ristretto di validatori, infatti all'interno della blockchain solo alcune utenze hanno il consenso a convalidare le transazioni e quindi di aggiornare il proprio registro più o meno distribuito. Quindi, solo alcuni nodi di convalida (*validatori*), i quali devono autenticare la propria firma ed identità, sono responsabili della generazione di ogni nuovo blocco di transazioni che sarà incluso nella Blockchain. Questo nuovo blocco può essere accettato direttamente senza verifica, o con il voto unanime, o semplicemente a maggioranza dei nodi responsabili, a seconda della configurazione scelta. La rete mantiene la capacità di aggiungere o eliminare eventuali validatori. La grande differenza con il PoW è l'assenza del mining e, dunque, assenza di concorrenza in fase di validazione, che comporta risparmi energetici e di risorse. Tutto questo porta ad una blockchain in grado di aggiornarsi più frequentemente, riducendo il tempo tra un blocco e l'altro (*Blocktime*) e di elaborare più transazioni (*Blocksize*) per le spese di elaborazione vicine allo zero.
Il PoA, però, basandosi su un algoritmo di questo tipo, non rispetta a pieno l'idea di decentralizzazione, caratteristica intrinseca della blockchian stessa, ma anzi

[7] campo dell'header del blocco settato dai miner affinché l'hash risultante rispetti i requisiti attuali della rete.

tende ad una centralizzazione seppur rimanendo un algoritmo molto efficiente nelle blockchain private e soprattutto consortili.

Nella sottostante Tabella 2.1 sono riportate schematicamente le principali differenze dei tre algoritmi di consenso [10] .

	Proof of Work (PoW)	**Proof of Stake (PoS)**	**Proof of Authority (PoA)**
`Partecipanti`	Chiamati minatori (*miners*); aperto a tutti i membri della rete	Chiamati fabbri (*forgers*); il creatore di un nuovo blocco viene scelto in base alla quota di partecipazione	Chiamati validatori; scelti dalla rete dopo eventuali verifiche e autenticazioni
`Requisiti`	Richiede il consumo di una risorsa esterna (mining hardware, alimentazione)	Richiede una grande caparra per essere identificato come validatore del blocco	Richiede il superamento dello standard di approvazione per diventare validatore
`Creazione di criptovalute`	Nuove monete digitali sono create ogni volta che la transazione viene validata;serve come ricompensa per il validatore del blocco	Ha una certa quantità di monete digitali in circolazione; le monete sono state pre-minate in anticipo	Tende ad una centralizzazione e quindi è poco sfruttato per le criptovalute
`Processo di convalida`	Tutti i miners competono tra di loro per risolvere il problema crittografico per validare la transazione	Un gruppo di validatori partecipa ad un algoritmo di consenso per votare il prossimo blocco da minare	Il blocco può essere convalidato direttamente senza verifica, a voto unanime o a maggioranza
`Incentivi`	Ricompensa per ogni blocco minato	Non c'è ricompensa per ogni blocco minato, ma il fabbro prende le fee delle transazioni del blocco	Non c'è ricompensa per ogni blocco minato, ma dei grossi vantaggi per l'efficienza e la scalabilità del sistema

Tabella 2.1. Principali differenze tra i tre algoritmi di consenso (PoW - PoS - PoA)

2.3 Tipi di blockchain

La tecnologia blockchain ha diverse aree di utilizzo. Può essere utilizzata in tutti gli scenari in cui è richiesta un'autorità centrale ma distribuita e decentralizzata. Proprio in base a come viene gestita quest'autorità ci sono diversi tipi di blockchain:

- Pubbliche;
- Private;
- Consortili.

La tabella seguente (Tabella 2.2) riassume alcune delle principali differenze tra i diversi tipi di blockchain. [12]
È importante sottolineare però come questa gestione di autorità che scaturisce la

	Pubblica	**Privata**	**Consorzio**
`Chi può leggere?`	Chiunque	Solo gli utenti invitati	Dipende
`Chi può scrivere?`	Chiunque	Partecipanti autorizzati	Partecipanti autorizzati
`Proprietà`	Nessuna	Singola entità	Più entità
`I partecipanti si conoscono?`	No	Si	Si
`Velocità di transazione`	Lenta	Veloce	Veloce

Tabella 2.2. Blockchain Pubblica vs Privata vs Consortile

divisione principale tra pubblico e privato è una visione legata strettamente alla fase di scrittura. Infatti quello di cui si parla veramente è chi è in grado di scrivere i dati su la blockchain. La gestione in fase di lettura invece va a creare due altre aree: blockchain chiusa e blockchain aperta. Generalmente quando si fa distinzione tra i diversi tipi di blockchain si fa riferimento solamente al pubblico e privato, ma non sarebbe così sbagliato vedere tutte le possibili soluzioni: pubbliche e aperte, pubbliche e chiuse, private e aperte, private e chiuse.
Le blockchain pubbliche e private offrono due soluzioni molte diverse, da un lato (pubblico) si ha una totale trasparenza e accessibilità, dall'altra (privata) bisogna conoscere gli utenti per autorizzarli a compiere transazioni o per visualizzare determinati dati e/o informazioni.

2.3.1 Blockchain pubblica

Spesso quando si parla di blockchain pubbliche ci si riferisce a loro anche con l'aggettivo "*permissionless*", senza permesso, perché non c'è bisogno che qualcuno conceda l'autorizzazione, dato che questi particolari tipi di catene di blocchi sono aperti a tutti. Le principali caratteristiche di una blockchain pubblica sono:

- Una struttura decentralizzata;
- Un'autorità decentralizzata;
- Una logica centralizzata.

Essendo una struttura decentralizzata nessuno ha il controllo sulla rete e chiunque può diventare un utente per partecipare alle attività principali. Ciò che è effettivamente pubblico non sono le informazioni identificative di un utente, ma sono visibili apertamente solo le informazioni relative alle transazioni tra gli utenti, come il numero del portafoglio utente, la data e l'importo. [11]
È importante sottolineare che una blockchain pubblica non è meno sicura degli altri tipi, infatti il livello di sicurezza è particolarmente elevato grazie all'autogestione che entra in gioco quando le informazioni vengono condivise con la rete globale.

2.3.2 Blockchain privata

Chiamata anche blockchain "*permissioned*" (autorizzata), entra in gioco quando alcune caratteristiche della blockchain pubblica non sono adatte al contesto specifico. Infatti in alcuni casi le organizzazioni e gli individui vogliono controllare chi ha accesso alle transazioni.
Questo tipo di sistema è identificato come "senza autorizzazione" in quanto permette alle aziende, o più in generale a qualche utente, di avere un'autorità centrale e concedere il permesso agli altri utenti della rete, aggiungendo restrizioni ed esercitando il pieno controllo sul sistema. Viene da sé che l'utente che governa il sistema ha pieni poteri su limitazioni e consensi, stabilendo facilmente chi può partecipare alla rete stessa e soprattutto a quali transazioni. Quindi solo gli utenti verificati possono leggere o scrivere nelle blockchain private.
Naturalmente, la stessa entità "centrale" decide quali sono le modalità di mining e può manipolare le voci del libro mastro della blockchain. Questo entra in contrasto con le basi di autenticità della blockchain. Infine, è importante sottolineare anche che in questi tipi di blockchain i dettagli delle transazioni possono essere totalmente privati e quindi non leggibili anche se i membri della rete si conoscono tra loro. Le blockchain private sono davvero ottime soluzioni in scenari in cui la protezione dell'anonimato e degli utenti è davvero importante o si vuole aggiungere valore alla soluzione. Mentre in uno scenario aziendale privato, è meglio conoscere l'identità dell'utente che ha fatto quella transazione, garantendo separazione tra tipi di informazioni e tipi di utenti. [12] [13]

2.3.3 Blockchain consortile

Questa tipologia di blockchain può essere considerata come un ibrido tra blockchain pubblica e privata. Il sistema è semi-pubblico e autorizzato dove alcuni nodi preselezionati lo controllano. Come le blockchain private, la rete è centralizzata, ma questo controllo è dato ad un gruppo di utenti certificati. Le blockchain consortili contengono alcune delle stesse caratteristiche crittografiche della loro controparte pubblica, ma consentono un controllo molto maggiore da una fonte centralizzata costituita da nodi specifici.
Quindi la differenza principale con le rispettive controparti è la modalità di consenso, né in mano ad un unico nodo, né totalmente distribuita sulla rete. Da qui, le regole di questo sistema sono flessibili: la visibilità della catena può essere limitata ai validatori, visualizzabile dai singoli autorizzati, o da tutti.
Questa tipologia di blockchain risulta essere vantaggiosa in un contesto in cui più organizzazioni operano nello stesso settore e richiedono un terreno comune su cui effettuare transazioni o trasmettere informazioni. Dal punto di vista di un'organizzazione risulta invece interessante farne parte per condividere informazioni con altri attori. [11] [12]

2.4 Smart contract

A partire dagli anni '90, il termine *smart contract* è stato usato per descrivere una grande varietà di cose diverse. La prima volta è stato introdotto dal ricercatore americano di crittografia Nick Szabo nel lontano 1994 [7], il quale coniò come definizione di smart contract: "un set di promesse, specificate in forma digitale" [4]. Con il passare degli anni la definizione di smart contract è cambiata, in particolare dopo il 2008 con l'invenzione del Bitcoin e ancora di più con l'avvento di Etherum ha assunto altri significati.
Un contratto intelligente è un programma informatico immutabile e sicuro che funziona in modo deterministico e rappresenta un accordo automaticamente eseguibile ed esecutivo. Per comprendere meglio questa definizione di smart contract:

- Programma informatico: gli smart contract sono semplicemente programmi per computer. In questo conteso la parola "contratto" non ha alcun significato legale
- Immutabile: una volta implementato e immesso nella rete, il codice di uno smart contract non può cambiare. Questa è la grande differenza con i software tradizionali, infatti l'unico modo per modificare uno smart contract è quello di implementarne una nuova istanza
- Sicuro: la sicurezza è una delle considerazioni più importanti quando si scrivono smart contract. Essendo spesso pubblici, dove ogni utente può interagirci,

diventa fondamentale un'ottima implementazione, infatti ogni vulnerabilità può essere sfruttata e le perdite sono quasi sempre impossibili da recuperare. È quindi fondamentale seguire le migliori pratiche e utilizzare modelli di progettazione come ad esempio la "programmazione difensiva", la quale prevede:

  - Minimalismo e semplicità: più è semplice e più è sicuro. La complessità è sinonimo di minor sicurezza;
  - Riutilizzo del codice: se esiste già una libreria o un contratto che fa la maggior parte del necessario, bisogna riutilizzarla;
  - Qualità del codice: evitare bug è fondamentale poiché una volta "lanciato" il codice, non si presentino eventuali problemi da risolvere;
  - Leggibilità del codice: il codice deve essere chiaro e semplice da comprendere;
  - Copertura dei test: testare tutto il codice possibile prima di renderlo eseguibile.

- Deterministico: dato lo stesso contesto di blockchain dove viene eseguita la transazione contenente l'esecuzione dello smart contract, il risultato ottenuto sarà sempre lo stesso per ogni utente che "lancia" il contratto

- Automaticamente eseguibile: soddisfare automaticamente i termini del contratto, riducendo al minimo la possibilità di azioni malevole.

Gli smart contract sono implementati come istruzioni per le transazioni che di solito sono attivate dagli eventi. Dopo che un utente invia una transazione all'indirizzo del contratto, questa viene eseguita da ogni nodo di consenso in modo da raggiungere un accordo sul suo esito. Lo stato del contratto viene aggiornato di conseguenza. Sulla base delle informazioni contenute nella transazione ricevuta, il contratto legge o scrive nella propria memoria privata, o addirittura può creare a sua volta un nuovo contratto. L'attivazione automatica è resa possibile dall'indirizzo dello smart contract, infatti risiedendo nella blockchain, ogni smart contract ha il proprio indirizzo univoco.
I contratti intelligenti racchiudono i termini degli accordi dei partecipanti per le attività che si svolgono in rete. Questi asset crittograficamente unici possono essere creati, scambiati e regolati in tempo reale dagli utenti. Al verificarsi delle condizioni di input, lo smart contract "risponde" eseguendo automaticamente qualsiasi tipo di obbligo o condizione: una coordinata GPS che indichi l'arrivo di un camion nel luogo corretto potrebbe automaticamente far scattare il pagamento al venditore delle merci trasportate da quel camion, oppure, una misurazione in fase di lavorazione di una temperatura su un prodotto può essere registrata come un'informazione essenziale per la qualità di quel prodotto.

Quindi si può dire che uno smart contract può essere visto come un'applicazione IFTTT [8] la quale produce gli effetti contenuti in una transazione al verificarsi di eventi specifici (Figura 2.3).

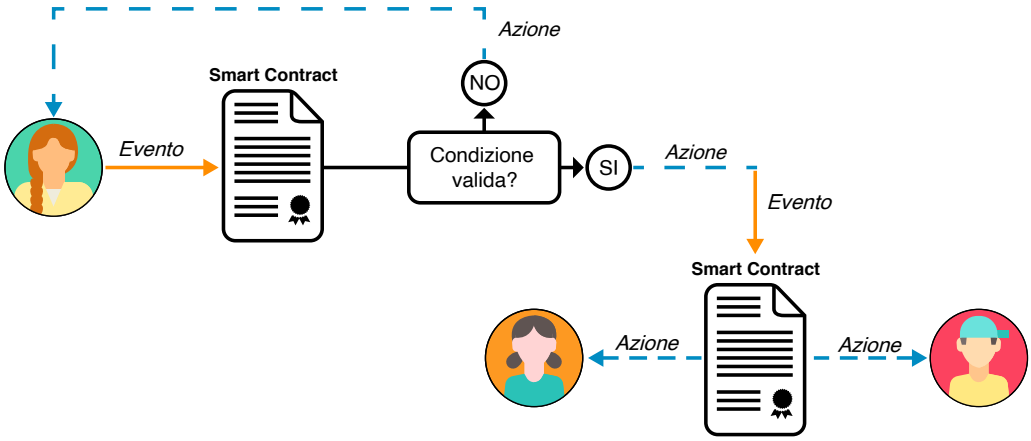

Figura 2.3. Applicazione IFTTT di uno smart contract

Negli ultimi anni gli smart contract hanno avuto larga diffusione grazie alla blockchain di Ethereum, la quale basa la propria funzionalità sulla EVM - Ethereum Virtual Machine - e gli smart contract stessi. Prima di spiegare brevemente cos'è la EVM, bisogna comprendere bene cosa sono questi smart contract in Ethereum e, soprattutto, come è possibile interagire con loro. In Ethereum uno smart contract rappresenta a tutti gli effetti una porzione di codice, o funzione, con la quale è possibile interagire direttamente o indirettamente. Quando avviene una transazione, o al verificarsi di alcune condizioni possono essere eseguite queste parti di codice. Però, quest'ultimo, il codice, per poter essere eseguito ha bisogno di un "interprete", ovvero, una traduzione dal linguaggio di programmazione al linguaggio macchina, in modo da poter essere compreso ed eseguito dalla macchina. La componente che crea questo livello di astrazione tra il codice in esecuzione e la macchina in esecuzione è la macchina virtuale, o meglio nota come Ethereum Virtual Machine - EVM. Questa macchina virtuale rappresenta, quindi, il vero e proprio motore di Ethereum, l'ambiente di runtime per lo sviluppo e l'esecuzione degli smart contract. L'interazione con gli smart contract, in linea con gli algoritmi di consenso adottati nella blockchain di Ethereum, necessitano del pagamento di alcune fee per incentivare e sostenere il meccanismo. Queste fee, in Ethereum, sono gestite sottoforma di

[8] If This Then That - "se accade questo, allora fai quello"

gas, ovvero, sono viste come se fosse della materia prima da utilizzare con un corrispettivo costo. In funzione di quanta materia viene utilizzata e il costo di questa, viene aggiunta una tassa al valore della transazione. Quindi per *gas* si intende il valore di prezzo, necessario per condurre con successo una transazione o eseguire un contratto sulla piattaforma della blockchain di Ethereum. Il gas è calcolato in base al codice da eseguire e il suo prezzo (*GasPrice*) è espresso in *gwei*[9], viene utilizzato per allocare le risorse della macchina virtuale (EVM) in modo che le applicazioni decentralizzate, come i contratti intelligenti, possano auto-eseguirsi in modo sicuro.

2.5 Applicazioni decentralizzate - dApp

Con la diffusione sempre più comune della blockchain, anche i paradigmi di programmazione di applicazioni e pagine web si stanno evolvendo, in particolare ci si sta muovendo sempre più verso la decentralizzazione delle risorse e quindi anche dei server che le gestiscono.
Queste applicazioni decentralizzate (Decentralized APPlication - dApp) sono delle soluzioni che sono in esecuzione su sistemi di calcolo distribuiti, come le tecnologie DLT - Distributed Ledger Technology - che sono la base dei sistemi blockchain. Quindi, le applicazioni decentralizzate sono memorizzate ed eseguite da un sistema blockchain, che spesso risulta essere proprio Ethereum con i suoi smart contract.

Le dApp, a differenza delle tipiche applicazioni in cui il codice back-end è eseguito su server centralizzati, hanno il loro codice back-end eseguito su una rete peer-to-peer decentralizzata. Il codice front-end per le interfacce utente, invece, può essere in qualsiasi linguaggio di programmazione che possa effettuare chiamate al suo backend, e può essere salvato sia in storage centralizzati che decentralizzati. Le Dapp, quindi, basandosi su sistemi distribuiti sono considerate più adattabili, trasparenti, e resilienti.
Un limite riscontrato, durante la diffusione delle dApp, ma più in generale con la sempre più ampia diffusione della blockchain è la mancata possibilità di sfruttare dati esterni al mondo blockchain e quindi off-chain, rimanendo circoscritti alle sole informazioni del mondo on-chain. Ad esempio, se si vuole realizzare una dApp per la gestione di scommesse si ha bisogno di un ente esterno che comunichi agli smart contract di riferimento della dApp i risultati esatti dei match affinché le scommesse vengano pagate correttamente. Proprio da questa esigenza di avere a disposizione negli smart contract i dati relativi al mondo off-chain che si è introdotto il concetto di oracolo, concetto discusso e approfondito nella Sezione 2.5.1.

[9] è un sottomultiplo degli ether, moneta della blackchain Ethereum, in particolare 1 gwei = 0.000000001 (10^{-9}) ether

2.5.1 Cos'è un Oracolo

Nell'antichità l'oracolo era l'uomo o più in generale l'entità attraverso la quale si ottenevano risposte ad ogni tipo di domanda, saggi consigli o profezie. Ripercorrendo questa definizione, anche l'*Oracolo* nell'ambito blockchain ha in un certo senso lo stesso significato. Infatti, rappresenta la connessione tra la rete blockchain, limitata alle sole informazioni salvate su di essa, e le restanti informazioni del mondo di Internet. Ad esempio, se si ha bisogno in blockchain di informazioni riguardanti le valute monetarie, attraverso un oracolo si possono avere in blockchain queste informazioni. Il problema principale dell'utilizzo dell'oracolo, in un certo senso, è la snaturalizzazione della blockchain stessa, andando in contrasto con il principio di decentralizzazione, in quanto ci si rivolge ad un unico "ente" per avere informazioni riguardanti un determinato settore. Proprio in linea con questi principi, un oracolo che opera in una blockchain deve avere delle caratteristiche ben precise:

- garantire la non manipolazione dei dati fino al loro inserimento in blockchain;
- essere il più trasparente possibile in modo da instaurare un rapporto di fiducia con gli utilizzatori;
- essere sicuro e protetto da attacchi, per garantire autenticità del dato.

Queste caratteristiche non sono così semplici da soddisfare, soprattutto perché in un'architettura del genere si rischia di far diventare proprio la connessione con l'oracolo la componente più debole ed esposta ad attacchi. Proprio per queste problematiche, molte aziende si stanno specializzando in servizi di questo tipo, in modo da offrire un servizio sicuro e performante, come ad esempio Provable o Chainlink. Entrambi queste due soluzioni in fase iniziale di sviluppo sono state considerate come validi strumenti per la realizzazione della soluzione, ma poi successivamente abbandonate per diversi motivi. Infatti, come deducibile dall'architettura della soluzione proposta, si è optato per uno sviluppo interno di server predisposti alla gestione dell'oracolo, per potersi distaccare da soluzione terze, non ancora del tutto affidabili o applicabili.

Provable

Provable[10] è un servizio di oracoli per smart contract e applicazioni blockchain, che gestisce richieste su diverse piattaforme come Ethereum, Rootstock, R3 Corda, Hyperledger Fabric ed EOS. Attraverso una prova di autenticità, calcolata con macchine virtuali verificabili o ambienti di esecuzione affidabili, il servizio provable riesce a fornire una soluzione affidabile e a dimostrare che i dati forniti sono autentici

[10]https://www.provable.xyz/

e non manomessi. Riproducendo internamente un modello logico "If This Then That" il motore di provable può essere sfruttato sia internamente che esternamente alla blockchain. Una richiesta valida di dati a Provable, fatta tramite l'integrazione nativa della blockchain o tramite l'API HTTP, riporta i seguenti argomenti:

- Un tipo di sorgente di dati
- Una domanda
- Un tipo di prova di autenticità (opzionale)

Il servizio di provable in un primo momento è stato considerato per essere integrato nella soluzione finale, ma dopo diverse analisi si è riscontrato un problema nella funzionalità. Infatti, il servizio risulta essere gratuito solo alla prima interrogazione, dalle successive si ha necessità di fare una transazione di ETH per ottenere una risposta. Il limite riscontrato nello sviluppo è stata l'impossibilità di sfruttare il servizio nella blockchain consortile, che unito al costo di interazione ha fatto sì che la scelta ricadesse su un'implementazione privata del servizio di oracolo.

Chainlink

Chainlink[11] si pone come obiettivo quello di risolvere ed evitare il problema della centralizzazione sull'oracolo. Infatti, Chainlink è una rete decentralizzata di oracoli che fornisce dati reali agli smart contract sulla blokchain. Questa soluzione si pone, quindi, l'obiettivo di connettere le due realtà ancora troppo distanti di mondo on-chain e mondo off-chain.
La rete si compone di sue principali componenti, la componente on-chain, la quale restituisce le risposte alle richieste di dati o di informazioni effettuate, e la componente off-chain, la quale è costituita da nodi Oracle collegati alla rete Ethereum. Questi nodi raccolgono autonomamente le risposte alle richieste fuori catena.
Il tutto è reso possibile grazie all'utilizzo dei token ERC20 LINK, sulla propria blockchain LINK. Questa soluzione è ancora in fase embrionale e attualmente utilizzabile solo nella mainnet di Ethereum o su una testnet proprietaria. Per questo è stato scelto di non adottarla nel progetto, seppure risulta essere idealmente una buona soluzione al problema di centralizzazione scatenato dall'uso di un oracolo.

2.6 Benefici e limitazioni

La blockchain racchiudendo dentro sé tutte le caratteristiche citate nei paragrafi precedenti garantisce con la sua applicazione diversi punti di forza e vantaggi.

[11] https://www.chain.link/

Tuttavia diversi aspetti di questa sua natura decentralizzata comporta anche delle limitazioni e svantaggi.

Si evidenziano quali sono i molteplici *benefici* che comporta la blockchain:

- Decentralizzazione: elimina la necessità di un intermediario o di un'autorità centrale, rappresenta il principale vantaggio della blockchain. Grazie ai meccanismi di consenso per concordare la validità delle transazioni tra gli utenti non è necessaria alcuna organizzazione di terzi che le regoli, ogni entità è libera di scambiare informazioni con altre. La dismissione degli intermediari offre, dunque, la possibilità di aumentare la velocità e di ridurre le inefficienze, riducendo parzialmente o eliminando completamente gli attriti nelle transazioni.
  Tutto questo può tradursi in una riduzione dei costi, in tempi più brevi e in una migliore scalabilità al mercato.

- Immutabilità: una volta che i dati sono stati registrati nel sistema blockchain, è estremamente complicato modificare le informazioni. Questo vantaggio rende la tecnologia blockchain estremamente resistente all'alterazione. Anche se altamente improbabile e complesso, la possibilità di poter modificare queste informazioni esiste. Infatti per operare una manomissione delle informazioni registrate sulla blockchain bisognerebbe poter accedere a tutti i nodi collegati nella rete prima che il blocco successivo venga registrato. Ciò significa che minore è il numero di nodi nella rete, maggiore è la possibilità di manomissione essendo la tecnologia più esposta all'attacco.

- Trasparenza e fiducia: il sistema è trasparente e di conseguenza riesce a creare una fiducia tra gli utenti grazie alla condivisione delle blockchain e la visibilità delle transazioni. Ogni membro della rete possiede una copia completa della blockchain e i dati non possono essere modificati o cancellati a meno che non venga stabilito un consenso diffuso in tutta la rete. Questo sistema garantisce la trasparenza, l'immutabilità e la fiducia della blockchain.
  La fiducia della blockchain si basa sulla fiducia di due o più partecipanti, che non si conoscono tra loro. Può essere aumentata e rafforzata al crescere dei processi e transazioni condivise tra gli utenti.

- Sicurezza: rispetto a un database centralizzato tradizionale con un unico punto di ingresso e quindi di possibile attacco informatico, la blockchain, essendo decentralizzata, crea potenzialmente l'opportunità di un sistema più resiliente fornendo una protezione più efficiente contro diversi tipi di cyber attacchi. Inoltre, dato che tutte le transazioni della blockchain sono crittograficamente protette, esse forniscono una maggiore sicurezza cibernetica. L'ingresso di ogni utente nella rete corrisponde ad una nuova identità univoca, che rende

la tecnologia blockchain altamente sicura e protetta.
Altro aspetto fondamentale della sicurezza, intrinseco nel sistema stesso, è la concatenazione degli hash crittografici dei blocchi. Per ogni nuovo blocco, è necessario calcolare il nuovo valore dell'hash, il quale includerà il valore dell'hash del blocco precedente.

Quindi, come sopra indicato questa tecnologia hai i propri vantaggi, ma non solo. Infatti presenta anche alcune *limitazioni* ed è giusto evidenziarle per poter comprendere a pieno la tecnologia:

- Consumo energetico elevato: il principale svantaggio della blockchain è l'elevato consumo di energia. Il mantenimento distribuito di un registro in tempo reale è uno dei motivi, poiché ogni volta che viene creato un nuovo nodo, questo comunica contemporaneamente con ogni altro nodo per garantire la trasparenza. I minatori della rete cercano di risolvere costantemente molte soluzioni al secondo nel tentativo di convalidare le transazioni ed aggiungere un nuovo blocco alla catena.
  Per farlo usano quantità importanti di potenza di calcolo, la quale richiede un continuo consumo di elettricità oltre che di tempo. Queste risorse sprecate contemporaneamente dai diversi nodi sono molto ingenti, considerando, inoltre, che solo il lavoro di uno di loro verrà "premiato" al raggiungimento del consenso. Dunque il principale motivo dell'elevato consumo di energia è proprio la verifica della firma delle transazioni e quindi la minazione dei blocchi, caratteristica principale del sistema stesso della blockchain, la quale giustifica la grande potenza di calcolo necessaria per questo processo.

- Scalabilità: soprattutto nelle blockchain che basano il proprio algoritmo di consenso sul Proof of Work, il costo di mantenimento della rete può essere molto elevato. Per cercare di mantenere bassi i livelli di consumo non dovranno essere raggiunte potenze di calcolo troppo elevate, influenzando in negativo la velocità di processamento delle transazioni. Bisognerà pagare *fee* sempre più elevante per far sì che la transazione risulti attraente per i miner e venga processata in un tempo ragionevole. L'aumento delle fee sarà sempre più elevato nel momento in cui sempre più utenti faranno parte della rete, rendendo il sistema non utilizzabile per il costo elevato e tempo di processamento di ogni singola transazione.

- Smart contract immutabili: una volta che lo smart contract viene aggiunto alla blockchain, diventa immutabile, in quanto non può essere cambiato. Se sono presenti anomalie nel codice, lo saranno anche durante tutto il ciclo di vita del codice. Ciò può creare scenari in cui una persona malintenzionata può sfruttare i difetti del codice per inviare il contenuto degli smart contract ai propri conti. Poiché la blockchain è immutabile, queste transazioni sono molto

difficili da annullare, il che significa che grandi quantità di valore possono restare bloccate o andar perse per sempre.

- Minacce alla sicurezza: sebbene la sicurezza sia considerata uno dei vantaggi della blockchain, la tecnologia può comunque essere attaccata dalle diverse minacce che si collegano ai protocolli PoW e PoS. I tre attacchi principali sono:
  - Attacco di maggioranza: la possibilità che esso si verifichi è molto remota, poiché un unico utente dovrebbe controllare almeno il 51%[12] dell'intera rete. Nel caso accadesse, avendo la maggior parte della rete a disposizione si potrebbero creare nuovi blocchi contraffatti e farli apparire nella rete come reali raggiungendo facilmente il consenso.
  - Doppia spesa: sfrutta le divisioni delle catene per spendere due volte la stessa moneta.
  - Attacco di Sybil: l'aggressore forza l'utente a comunicare solo con nodi contraffatti, in modo da raccogliere informazioni e controllare il registro dell'aggredito per truffarlo.
- Regolamentazione: questa limitazione della tecnologia riguarda soprattutto la parte delle criptovalute. Non esistendo, nella maggior parte degli stati mondiali, delle vere regole finanziare che ne regolano l'uso porta a sfruttarle per attività illegali come frodi e riciclo di denaro. Negli ultimi anni, però, molti stati stanno iniziando a imporre delle regolamentazioni per l'uso di questa tecnologia [14].

[12] in realtà il quorum è dato dal 50%+1

Capitolo 3

Food Chain: la blockchain nell'agroalimentare

Negli ultimi anni il settore agroalimentare è divenuto uno dei principali pilastri del sistema economico europeo. L'Europa, vanta la leadership di esportazioni mondiali in campo agroalimentare [16]. Anche in Italia, la situazione non è molto differente, infatti il settore agroalimentare è uno dei più importanti settori dell'economia del paese e rappresenta un vero potenziale di risorsa economica, grazie anche all'utilizzo delle tecnologie. Proprio sull'onda di questo grande potenziale economico, negli ultimi anni sono nate molte startup, le quali con l'ausilio delle nuove tecnologie come, ad esempio, la *Blockchain*, l'*Internet of Things* (IoT), i *Big Data* e l'*Intelligenza Artificiale* (AI) cercano di aggiungere valore ai prodotti e a tutelare cibi nazionali, regionali e locali.
Le principali rivoluzioni del *foodsystem*[1] sono sostenute dall'IoT e dalla blockchain. Quest'ultima si pone come la scoperta più rivoluzionaria di questi ultimi dieci anni, l'innovazione attraverso la quale diversi settori potranno compiere un'evoluzione tecnologica che porterà un miglioramento di tutto l'ecosistema economico e sociale. Pur essendo, la tecnologia, un mezzo attraverso il quale è possibile controllare e tutelare i prodotti agroalimentari nell'intero foodsystem, non può essere lo strumento chiave che riesce a dare una garanzia assoluta. Infatti possono esserci differenti idee di prodotto di qualità, come ad esempio la tutela dei lavoratori e la salvaguardia dell'ambiente. Quindi non è tutto controllabile e migliorabile solo con la tecnologia, però sicuramente se applicata in modo adeguato e con le giuste regole può essere un ottimo alleato per raggiungere l'obiettivo di offrire al cliente finale, ovvero il consumatore, un prodotto di qualità sotto tutti i punti di vista.

[1] sistema alimentare, comprende tutti i processi e le infrastrutture coinvolte nell'alimentazione, dalla coltivazione allo smaltimento

3.1 Food Value Chain

Prima di passare a vedere in dettaglio le diverse applicazioni della tecnologia nella filiera agroalimentare, è importante definire e chiarire bene l'intera "catena" produttiva, che va sotto il nome di *Food Value Chain* (FVC).
Una Food Vaue Chain - catena del valore alimentare - (FVC) è costituita da tutti gli stakeholder che partecipano alle attività di produzione e di creazione di valore aggiunto necessarie per la trasformazione della materia prima in prodotti alimentari [17]. Si riferisce a tutte le attività che garantiscono che il cibo segua una serie di processi e operazioni dalle fattorie alle tavole dei consumatori. La FVC è considerata la più complessa e frammentata di tutte le filiere, necessita di un insieme di accordi tra i vari stakeholder partecipanti con l'obiettivo comune di creare benefici per ogni attore del sistema e soddisfare al meglio le esigenze dei consumatori.
Le FVC possiedono un insieme di proprietà distintive che le distinguono dagli altri tipi di catena di approvvigionamento, o più generalmente note come *Supply Chain*. Alcune importanti caratteristiche peculiari sono elencate qui di seguito:

- Il breve ciclo di vita della maggior parte dei prodotti alimentari comporta la necessità di una lavorazione rapida e di brevi tempi di conservazione;
- Le merci deperibili richiedono specifiche condizioni di trasporto e di stoccaggio;
- Le operazioni di produzione hanno cicli di allestimento frequenti a causa della dipendenza dalla stagionalità dei prodotti;
- C'è un'elevata differenziazione dei prodotti all'interno della catena;
- Sono necessari rigorosi controlli di qualità e la conformità alle diverse legislazioni, regolamenti e direttive nazionali e internazionali in materia di sicurezza alimentare, poiché il consumo di alimenti ha effetti diretti sulla salute umana [18].

Nelle FVC il "valore" si riferisce ai guadagni di efficienza risultanti da uno stretto coordinamento tra i partner della supply chain, ai prezzi più elevati ottenuti con la commercializzazione differenziata di prodotti alimentari, e a un insieme di valori condivisi dai partecipanti alla catena che rispondono direttamente alle richieste e agli interessi dei consumatori [19].

Questi rapporti tra i partner hanno bisogno di coordinamento attraverso la comunicazione e sono caratterizzati da un forte impegno alla trasparenza, da collaborazione per la pianificazione aziendale e dallo scambio di know-how di mercato e di business.
L'industria alimentare è costituita da una rete globale di produttori, grossisti, distributori e rivenditori al dettaglio che servono la crescente domanda di cibo in

tutto il mondo. Ogni attore dell'industria alimentare ha un ruolo specifico da svolgere, con le proprie fonti di approvvigionamento e specifici clienti da servire. Ogni attore ha anche un impatto unico sulla domanda e sull'offerta in tutto il settore. I principali attori di una catena di approvvigionamento alimentare sono mostrati in Figura 3.1, ed analizzati di seguito:

Figura 3.1. Schema della Food Value Chain

- Produttori: sono il primo anello della catena alimentare, rappresentano l'inizio dell'intero processo. I produttori, che possono essere agricoltori o allevatori, sfruttando macchinari e prodotti chimici devono garantire la produzione della materia prima, in modo da soddisfare la domanda, per questo hanno diverse responsabilità. Infatti devono fornire prodotti alimentari che rispecchino le direttive governative, soddisfare le quantità richieste e mantenere dei prezzi accessibili, senza tralasciare la salvaguardia dell'ambiente. Le pratiche agricole e l'allevamento di animali varia notevolmente in funzione sia delle diverse regolamentazioni, sia delle differenti esigenze dei potenziali mercati e dei loro clienti.

- Trasformatori: le attività di trasformazione alimentare comprendono due categorie principali, operazioni primarie e secondarie. La lavorazione primaria è la conversione dei prodotti grezzi non commestibili in ingredienti alimentari, come ad esempio la pulizia, la sgusciatura, la classificazione e l'imballaggio. I prodotti della lavorazione primaria sono inviati al mercato per la vendita al dettaglio o alle fabbriche come ingredienti per la lavorazione secondaria. La lavorazione secondaria comprende le attività quotidiane di conversione degli ingredienti pronti per l'uso in alimenti commestibili, come ad esempio la macinazione del grano in farina, la spremitura del succo dalla frutta, la produzione di formaggio dal latte e la realizzazione di carne macinata.
  Una volta che il cibo viene lavorato, il compito più importante è quello di mantenerlo fresco. Qui entrano in gioco i confezionatori: il packaging deve mantenere il cibo fresco il più a lungo possibile, essere facilmente trasportabile e, soprattutto, attrarre i consumatori.

- Distributori: forniscono cibo e prodotti correlati agli operatori del settore della ristorazione. Prendono il cibo direttamente dai produttori e dai trasformatori consegnandolo a negozi di alimentari, ristoranti, ospedali e altri operatori del servizio alimentare. Il distributore è il punto di contatto diretto del produttore per i potenziali acquirenti di certi prodotti.

- Rivenditori: hanno il ruolo di vendere i prodotti direttamente ai consumatori. Possono essere aziende di dimensioni diverse, come i grandi supermercati e i piccoli commercianti indipendenti. Per realizzare un profitto cercano prodotti che coincidano con i loro obiettivi di business trovando i fornitori con i prezzi più competitivi. I rivenditori possono rifornirsi di prodotti provenienti da una qualsiasi delle tre fasi precedenti della FVC e rappresentano l'interfaccia primaria con il consumatore. Proprio per questo hanno un ruolo molto significativo per quanto riguarda la sensibilizzazione del consumatore ad una dieta sana e sostenibile, giustificando così i molteplici investimenti, in tecnologie come la blockchain, di diversi attori del settore.

- Consumatori: sono gli utenti finali nella catena di distribuzione, possono essere rappresentati semplicemente da persone comuni o altre entità economiche che acquistano e utilizzano il bene o il servizio. Ogni fase della catena del valore alimentare deve considerare le esigenze dei consumatori fin dall'inizio del processo di produzione del prodotto, al fine di soddisfare il più possibile la domanda dei consumatori.

Si può notare quindi come tutti i partecipanti della filiera sono influenzati dai consumatori finali, i quali negli ultimi due decenni hanno mostrato preoccupazioni e interessi sul sistema di produzione e sulla composizione degli alimenti. Tutto questo significa che, i consumatori, scelgono cosa acquistare in base alla qualità dei prodotti, alle tecniche utilizzate durante il processo produttivo, alla sicurezza alimentare e alla sostenibilità ambientale e sociale. Per rispondere a questa esigenza è necessario identificare gli alimenti e i loro ingredienti, effettuare controlli di qualità e le relative certificazioni, offrendo all'utente finale una visione completa di tutte queste informazioni con semplicità e trasparenza.

3.2 La tecnologia nell'agrifood

Per molte potenze mondiali il settore agroalimentare è sicuramente la base della propria economia, in particolare dell'Italia. Quest'ultima oltre a vantare la sua bellezza nell'arte, nella letteratura e nella storia, ha conquistato un ruolo importante nel mondo per le sue peculiarità agroalimentari e culinari. Con l'idea di preservare questi valori, nasce il binomio tra tecnologia e settore agroalimentare.

Le nuove applicazioni tecnologiche: IoT, Big Data, AI e Blockchain consentono di aggiornare non solo i prodotti, ma gli interi processi produttivi, andando a modificare le organizzazioni aziendali e le connessioni tra le imprese e i consumatori. Più in dettaglio si nota che gli obiettivi del "matrimonio" tra agricoltura e tecnologia porti i sui frutti in termini di:

- Efficienza: l'adozione di nuovi strumenti innovativi permette di produrre in maggiore quantità a prezzi più moderati;
- Efficacia: la nuova forza che nasce dalla fusione delle due, porta dei miglioramenti in termini di qualità del prodotto. L'efficacia è da intendersi oltre il semplice significato, in modo da garantire anche sicurezza alimentare e sostenibilità ambientale;
- Aiuto tangibile per il lavoro degli agricoltori e degli allevatori.

Tutti gli attori della catena FVC mostrano grande interesse verso la tecnologia e la sua applicazione nel campo agroalimentare. Negli ultimi anni il valore economico di questi investimenti è più che triplicato, coinvolgendo centinaia e centinaia di imprese, dalle più affermate alle startup [20] [22]. In particolare, gli agricoltori e allevatori mostrano grande interesse verso quelle tecnologie che li aiutino a gestire le esigenze dei consumatori, come l'aumento di richiesta e di qualità del prodotto, la trasparenza della filiera e la sicurezza, garantendo sempre dei costi adeguati.
In linea con le esigenze sopracitate, la tecnologia che meglio risponde a queste, è la blockchain. Infatti, la "catena di blocchi" riesce a fornire una risposta del tutto innovativa a proposito della realizzazione di una nuova connessione tra produttori e consumatori basata su un concetto di fiducia moderno e rivoluzionario. Una nuova visione che pone la blockchain come un servizio necessario alla supply chain per soddisfare le più recenti esigenze di fiducia, sicurezza e tracciabilità.

Le applicazioni della blockchain nel contesto dell'agrifood sono le più disparate:

- Favorire gli agricoltori su iter burocratici e assicurativi;
- Tracciare la provenienza delle materie, lungo tutta la filiera;
- Introdurre maggiore trasparenza nella filiera;
- Controllare e verificare informazioni sulla sostenibilità ambientale di progetti e prodotti;
- Tutelare enti pubblici da frodi (erogazione fondi e sussidi).

Quindi, l'utilizzo di questa tecnologia risulta essere una vera e propria rivoluzione e innovazione, consentendo ai produttori, ai trasformatori, ai distributori, ai venditori e a tutti i consumatori un'estrema autonomia per verificare il prodotto lungo

la complessa filiera. L'adozione di questa tecnologia, però, porta con sé una semplificazione in ogni fase dell'intero sistema, concedendo a tutti gli attori interessati un'unica sorgente informativa certificata da cui reperire le informazioni della FVC. La rivoluzione più grande sarà quella di poter tener traccia di ogni prodotto in tempo reale dall'azienda agricola alla tavola, garantendo miglioramenti economici agli attori coinvolti [21].

Come sopracitato, molte aziende e startup stanno investendo molto nella blockchain e la sua integrazione con il mondo dell'agroalimentare. Molti gruppi GDO[2] stanno lavorando e collaborando con grandi imprese per portare valore aggiungo a ciascun anello della filiera, aggiungendo informazioni sulla tracciabilità (date di lavorazioni, temperature di lavorazione e distribuzione, trattamenti, ...) del prodotto finale. Tra i vari gruppi GDO, Carrefour si è fatta pioniera di questa integrazione con le sue collaborazioni con IBM, la quale mette a disposizione il suo know-how attraverso IBM Food Trust[3], per fornire ai propri clienti informazioni sul lotto del prodotto che stanno consumando in modo trasparente ed efficace.
Nella Sezione 3.3 viene descritto l'attuale avanzamento delle ricerche della comunità scientifica e la loro visione su lo sfruttare la tecnologia, ma soprattutto la blockchain nella catena di approvvigionamento agroalimentare; mentre nella Sezione 3.4 sono analizzate in dettaglio alcune tra le diverse applicazioni, già esistenti sul mercato, della blockchain nel settore agrifood.

3.3 Stato dell'arte

La sicurezza e l'affidabilità degli alimenti è sempre più precaria, infatti secondo l'Organizzazione Mondiale della Sanità (OMS) nel mondo quasi 1 persona su 10 si ammala dopo aver mangiato cibo contaminato e proprio questo cibo non sicuro favorisce la creazione di un circolo vizioso di malattie e malnutrizione, che colpisce in particolare i neonati, i bambini piccoli, gli anziani e i malati [23] [24]. In Europa le molteplici regolamentazioni alimentari tendono a porre dei rimedi, come ad esempio il regolamento 1760/2000 della Commissione Europea per le carni bovine, il quale richiede un attento e preciso salvataggio di informazioni lungo tutta la filiera, dal processo di nascita del bovino fino al confezionamento finale del punto vendita, passando per lo smistamento e la macellazione [25]. Inoltre, sempre l'OMS, ha ribadito l'importanza di una buona collaborazione tra i diversi governi, tra produttori e consumatori, in modo da riuscire a garantire la sicurezza alimentare al di là degli innumerevoli attraversamenti di confini nazionali, e a volte continentali,

[2]Grande Distribuzione Organizzata - sistema di vendita al dettaglio

[3]Piattaforma di IBM che aiuta le imprese a sfruttare al meglio la blockchain

che gli alimenti possono compiere durante l'intero processo della catena di approvvigionamento [23].
Tornando all'esempio del regolamento 1760/2000 della Commissione Europea per i bovini, citato in precedenza, risulta essere, per quanto possa sembrare strano essendo un regolamento risalente a 20 anni fa, il sistema di tracciamento più avanzato nell'Unione Europea. Infatti, ha dei grossi difetti, soprattutto lungo la catena delle informazioni condivise, dove non è presente nessun meccanismo che garantisce la credibilità delle informazioni e in particolar modo tra l'agricoltore e il macellatore. Non sono da sottovalutare anche possibili errori umani nella trascrizione di informazioni o ancor peggio delle vere e proprie manipolazioni [26].

L'ultimo anello della catena FVC, il consumatore, negli ultimi anni sta modificando le proprie esigenze, scoprendo sempre più un forte interesse verso la conoscenza dell'intero processo e l'importanza stessa del conoscere il prodotto che sta consumando. Questi cambiamenti da parte degli utenti finali hanno portato gli altri anelli della catena a sentire l'esigenza di adeguarsi, per poter continuare a soddisfare la domanda. E' proprio su questa scia che si sono mossi i ricercatori, andando a rivisitare e rimodernizzare l'idea della supply chain in generale, ma più in particolare per le catene di approvvigionamento degli alimenti, integrando nuove tecnologie come IoT e blockchain che senza dubbio rappresentano le due innovazioni che più si prestano a risolvere questi problemi.

Essendo la blockchain una tecnologia molto recente, molti degli studi effettuati sono posteriori al 2015 [27], in particolare si è notato come l'uso della blockchain al servizio delle catene di approvvigionamento agroalimentari non è troppo diffusa e ancor meno nella filiera dei bovini [43] [44], a differenza della sua applicazione nelle supply chain in generale dove risultano esserci molti più studi e analisi [28]. L'idea di sfruttare la blockchain e l'IoT al servizio di un efficientamento nella produzione, e non solo per i servizi finanziari dove la blockchain ha preso maggiormente piede, è molto interessante e meritevole di uno studio [29] [30].

Prima di procedere ad un'analisi più dettagliata delle attuali integrazioni tra IoT e blockchain nel campo FVC, è opportuna riflettere sui benefici che quest'ultima può portare nella supply chain. Per poter comprendere a pieno i vantaggi che la blockchain può portare, si deve ribadire l'attuale limitazione della catena di approvvigionamento, dove i dati e le informazioni, se presenti, sono centralizzate nei singoli anelli della catena e gli altri non possono accedervi, ripercuotendosi totalmente sui consumatori finali ai quali non è permesso risalire alla fonte del prodotto che stanno acquistando. Una prima risoluzione a questo problema era stata presentata con il progetto *Futurmed*, il quale voleva rinnovare il sistema aggiungendo un unico database centralizzato in cui tutti potevano salvare le proprie informazioni di lavorazione e gli altri elementi avevano la possibilità di leggerli [31]. Con l'avvento

della blockchain naturalmente il concetto di centralizzazione è stato superato e sono state proposte diverse soluzione con l'idea di poter aggiungere oltre alla sicurezza delle informazioni, facilmente garantite dalla natura stessa della blockchain, anche vantaggi gestionali e di pratiche aziendali, come [27]:

- riduzione di tempi e quindi di costi per le transazioni di informazioni e documenti su piattaforme basate sulla blockchain e che quindi non richiedono l'intervento di terze parti;
- essendo presenti i registri aperti e decentralizzati, dove chiunque può accedere e controllare, la trasparenza d'informazione e la stessa visibilità lungo tutta la filiera è sicuramente migliore;
- le relazioni tra i partner commerciali si estendono da fisiche a digitali, migliorando l'intero flusso di informazioni del prodotto.

Per poter rendere l'intero sistema funzionante, l'integrazione e collaborazione tra IoT e blockchain è obbligatoria, in modo da svincolare anche le stesse informazioni da possibili errori umani. Il fattore principale che può rendere questa collaborazione un'opportunità di miglioramento e rivoluzione per l'intera catena di approvvigionamento è la relazione di identità fisica e virtuale del prodotto grazie a codici univoci ottenibili mediante sistemi di identificazione come RFID[4] NFC[5] WSN[6] GPS[7] [33]. La comunicazione tra i diversi sensori dispersi lungo tutto il processo e la comunicazione delle informazioni da loro raccolte è il principale problema nello studio e realizzazione di architetture resistenti e performanti nei diversi campi agroalimentari. Per quanto riguarda l'agricoltura smart, innovativa, ci sono molte proposte di nuovi modelli e sistemi architetturali che operano più orizzontalmente nella catena produttiva, sfruttando non solo tecnologie come la blockchain ma anche AI e Cloud Computing per efficientare l'allevamento e l'agricoltura, rispettando l'ambiente e risparmiando sui costi produttivi [34] [35] [36]. In particolare nell'articolo [40] gli autori hanno esaminato i concetti associati alla tecnologia ICT basati su blockchain ed hanno proposto un modello di sistema di e-agricoltura ICT con un'infrastruttura blockchain per l'uso su scala locale e regionale.

L'applicazione della blockchain a sostegno dell'IoT per realizzare nuovi sistemi efficienti è molto studiata in ambito accademico, ma soprattutto viene sfruttata per rendere l'intero sistema il più possibile decentralizzato. Nell'articolo [37], gli autori

[4]Radio-Frequency IDentification

[5]Near Field Communication

[6]Wireless Sensor Network

[7]Global Positioning System

hanno proposto una soluzione blockchain integrata per la rete server LoRaWAN per costruire un sistema aperto, affidabile, decentralizzato e a prova di manomissione, che fornisce il meccanismo per verificare che i dati di una transazione siano esistiti in un determinato momento nella rete. Sostengono che sia il primo lavoro che integra la tecnologia blockchain e la tecnologia LoRaWAN dei sistemi IoT, sfruttando i vantaggi di entrambi. Così come gli autori dell'articolo [38] hanno proposto una soluzione per consentire a sensori IoT a basso consumo di accedere a un'infrastruttura basata su blockchain. Per raggiungere questo obiettivo, hanno progettato un gateway IoT come un nodo blockchain e hanno proposto un meccanismo di messaggistica basato su eventi per dispositivi IoT a basso consumo. Una dimostrazione di un tale sistema è stata implementata usando nodi e gateway LoRa in una rete Ethereum privata. Nell'articolo [39] gli autori presentano un metodo che cerca di utilizzare i dispositivi e sensori IoT al posto della registrazione e della verifica manuale, il che riduce l'intervento umano al sistema in modo efficace. L'idea futura è che possano utilizzare la tecnologia degli smart contract per definire un insieme di avvisi automatici nel sistema, per aiutare gli operatori a trovare i problemi e ad elaborarli tempestivamente.

La tracciabilità è molto importante nella catena di approvvigionamento alimentare per garantire la sicurezza e la qualità alimentare ai consumatori. Con *sistemi di tracciabilità* si intende garantire la reperibilità e rintracciabilità dei prodotti lungo tutti i movimenti nella filiera del cibo, dalla produzione alla distribuzione. Bisogna, però, fare distinzione tra i due termini spesso usati come sinonimi ma che hanno accezioni differenti, infatti con il termine *tracciabilità* ci si riferisce al percorso dell'alimento, seguendone l'intero processo produttivo dal campo alla forchetta, mentre con *rintracciabilità* si intende il ripercorrere a ritroso il processo produttivo, partendo dall'etichetta finale risalire fino all'origine [32].
Quindi, essendo la tracciabilità il mezzo attraverso il quale è possibile controllare i diversi stadi di produzione, lavorazione e distribuzione del cibo, risultano essere diversi gli stati europei che, nonostante le discipline imposte dalla commissione europea, non hanno ancora sviluppato e adottato requisiti legali per la tracciabilità dei prodotti alimentari. A livello europeo, la tracciabilità è disciplinata su tre livelli: politiche della Commissione Europea, politiche nazionali, standard e certificazioni private volontarie. Per le politiche della Commissione Europea, dal 2005, esiste il Reg. CE 178/2002 [8] che impone la rintracciabilità obbligatoria per gli alimenti e tutti i suoi ingredienti, seppure non ci sono indicazioni per il produttore sui metodi e tecniche da adottare per garantirne la veridicità. Non solo a livello europeo, ma

[8]Regolamento del parlamento Europeo che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare

anche a livello internazionale sono stati introdotti degli standard per la gestione della sicurezza e della qualità alimentare, come:

- ISO 22005:2007 : introduce linee guida e requisiti a supporto delle aziende e delle filiere agroalimentari di tutte le dimensioni per la raccolta della documentazione nelle varie fasi del processo di raccolta, elaborazione e distribuzione, consentendo di risalire in qualsiasi momento alla localizzazione e alla provenienza del prodotto o dei suoi componenti tramite un codice identificativo.

- ISO 22005:2008 : in aggiunta alla certificazione precedente, si introducono requisiti per la rintracciabilità volontaria sia esterna tra gli operatori della filiera sia interna, vale a dire prevede il poter ricostruire il percorso seguito da ogni materia prima o sostanza all'interno del singolo stabilimento.

- ISO 9001:2008 : viene introdotto il concetto di identificazione del prodotto attraverso un codice univoco per mantenere traccia del prodotto e delle sue parti costituenti lungo tutto il processo, dall'origine delle materie prime alla distribuzione del prodotto finito.

Dal punto di vista tecnologico vi sono diversi efficienti strumenti per la rintracciabilità dei prodotti alimentari, ad esempio i dispositivi di identificazione a radiofrequenza (RFID) e sistemi a lettura ottica dei codici a barre (QR Code) sono tra i più diffusi ed efficienti per l'automazione nella raccolta elettronica dei dati. L'automazione garantisce precisione e affidabilità nell'identificazione dell'unità tracciata, aumentando anche il numero di controlli che possono essere condivisi su reti sicure. A riguardo sono stati definiti anche una serie di standard ISO per regolamentare la codifica dei dati e l'interoperabilità tra diversi dispositivi. Tramite controllo da database centralizzati, tali sistemi permettono l'autenticazione del prodotto in tempo reale tramite un proprio codice univoco, tuttavia presentano due principali limiti: presentano elevati costi di mantenimento del database ed è difficile garantire appropriati livelli di privacy.
Negli ultimi anni sono state proposte molte soluzioni a questi problemi, sfruttando diverse tecnologie, ma soprattutto la blockchain, per garantire decentralizzazione e sicurezza, migliorando la tracciabilità di animali, piante e prodotti alimentari, garantendone l'innovazione e l'attualità rispetto alle normative vigenti nei diversi Paesi. Come sopracitato, i sistemi di identificazioni sono molto utilizzati per proporre delle soluzioni al problema della tracciabilità, come l'esempio proposto da Tian dove propone un sistema di tracciabilità della filiera agroalimentare che sfrutta la tecnologia RFID e la tecnologia blockchain. Dapprima ha analizzato i vantaggi e gli svantaggi dell'utilizzo della tecnologia RFID e della tecnologia blockchain nella costruzione del sistema di tracciabilità della catena di approvvigionamento agroalimentare e ha mostrato un possibile processo di costruzione di questo sistema. Egli pensa di poter portare la tracciabilità con informazioni affidabili in tutta

l'offerta agroalimentare, il che garantirebbe in modo efficace la sicurezza alimentare, raccogliendo, trasferendo e condividendo dei dati autentici e connessi tra loro della produzione, della trasformazione, dell'immagazzinamento, della distribuzione e della vendita [33]. Ancora più interessante, ai fini di questo lavoro di tesi, è il lavoro presentato nell'articolo [41], dove gli autori hanno presentato il loro percorso di sperimentazione e realizzazione per un sistema IoT open source per il tracciamento delle mucche. Hanno proposto un'architettura LoRaWAN per il lungo raggio di pascolo, analizzando l'architettura di sistema di alto livello per la tracciabilità del bestiame e implementando un'applicazione web e un protocollo di comunicazione proprietario CowTrack. I diversi test sul campo condotti hanno riscontrato, oltre alla distanza massima di circa 6 km per comunicare, anche buone impressioni da parte degli allevatori, soprattutto per quanto riguarda il servizio di recinzione virtuale e gli allarmi sui capi del bestiame.

Proprio sulla tracciabilità del bestiame e il loro pascolo, fulcro di interesse per questo lavoro, uno dei più recenti lavori presentati dalla società scientifica, è presentato nell'articolo [42] dove gli autori esaminano l'uso di una nuova infrastruttura che è in linea con la spinta attuale di molte industrie per entrare nell'era dell'IoT, proponendo un sistema efficiente, sicuro, decentralizzato e distribuito che può modernizzare il funzionamento dell'industria del bestiame e i suoi ambienti prevalentemente rurali. Con il caso d'uso in Brasile, dove sono stati testati alcuni tag RFID per il bestiame, hanno analizzato l'uso di memorizzazione cloud e su blockchain per monitorare lo stato di salute dei bovini durante il loro ciclo di vita, ed inoltre, hanno proposto un sistema che può agevolare il trasferimento di bestiame da un proprietario ad un altro sfruttando la blockchain per semplificare le procedure di acquisto/vendita tra gli allevatori. L'architettura proposta si basa su una blockchain privata ed è composta da quattro principali attori: amministratore, utenti, servizi cloud e rete blockchain. Il caso studio analizzato in Brasile ha evidenziato l'ormai datata e rurale struttura dell'intero processo, facendo emergere la voglia e la necessità di investire nelle nuove tecnologie per migliorare lo stile di vita di tutti di attori coinvolti, e ponendo la blockchain come un interessante progresso che vale la pena di approfondire.

Commentando brevemente l'attuale situazione della ricerca scientifica riguardo al mondo blockchain e agrifood più in generale, si può dire che sicuramente sono diversi i progetti che stanno nascendo per affrontare gli ormai conosciuti problemi di questo settore. Il progetto di appartenenza di questo lavoro di tesi è stato strutturato e pensato per coprire e rinnovare l'intero processo produttivo legato al mondo dell'allevamento e della produzione degli alimenti derivati da esso. Attualmente non vi sono progetti di quest'ordine di grandezza in Italia, dove grazie allo studio di 4 casi dimostrativi si è cercato di coprire l'intero settore, analizzando e proponendo soluzioni innovative con l'utilizzo della blockchain a partire dal sostegno economico

per i pascoli fino ad arrivare ad applicazioni e servizi per il consumatore finale.
In particolare, in questo lavoro di tesi, oltre ai problemi derivanti dalle limitazioni attuali della tecnologia, vengono affrontati tutti i problemi legati alla burocrazia e all'erogazione di sussidi e fondi per l'allevamento e il pascolo. L'analisi e la verifica della corretta erogazione è senza dubbio il primo tassello per una filiera più controllata e trasparente, dove anche l'utente finale deve saper scegliere con sicurezza e piena libertà. Schematizzando brevemente le funzionalità di servizi attualmente presenti in letteratura con quelle di questo progetto di tesi si può notare (Tabella 3.1) come la parte più innovativa di questo lavoro è data dalla realizzazione di un sistema versatile lungo tutto il flusso di dati, sfruttando tutte le caratteristiche di una blockchain consortile, e garantendo così un prodotto di progetto versatile e attento all'utente finale fin dalle prime fasi della filiera.

I casi d'uso riportati in tabella sono solo alcuni dei sopracitati e analizzati per lo stato dell'arte, ma risultano essere i più esemplificativi.
Nel primo caso riportato [33] si vuole sottolineare l'esistenza di molti studi riguardanti la catena di approvvigionamento generale, i quali sorvolano sulle prime fasi della filiera e quindi sul pascolo. Nei secondi due, invece, si notano alcune caratteristiche principali dei lavori presenti in letteratura, i quali hanno come focus del lavoro il pascolo di bovini o ovini. Infatti, se nel caso del sistema greco [41] si fa un attento studio sulla parte proprio inerente al pascolo, non andando oltre e non analizzando le successive componenti della filiera; nel caso testano in Brasile [42] viene considerata tutta la filiera seppur mancando degli accorgimenti iniziali sul pascolo. Il lavoro di questa tesi, invece, pone la propria attenzione sia sulla prima parte, quindi il pascolo, ma progettando soluzioni con un'ottica attenta all'utenza finale, dovendosi rapportare con un progetto di più ampia scala che fornisce una nuova e innovativa soluzione a tutta l'intera filiera.

Quindi, a livello mondiale sono diversi gli studi in questo ambito, anche applicati proprio all'allevamento dei bovini e la loro tracciabilità. Molti degli studi riguardanti la blockchain provengono proprio dall'oriente dove vi è una forte predisposizione e molto interesse per le nuove tecnologie come IoT e blockchain. Però anche in Europa gli studi non mancano, soprattutto per quanto riguarda l'utilizzo della blockchain in ambito finanziario. Nella sezione che segue vengono presentate alcune realizzazioni commerciali in modo molto schematico e conciso, e nel Capitolo 4, successivo, viene presentato il caso d'uso analizzato nel seguente lavoro di tesi e il suo progetto di appartenenza, mettendo in risalto le nuove scelte tecnologiche e le attuali necessità, soprattutto della regione Piemonte, di mettere al sicuro ed in evidenza la qualità dei propri prodotti, evitando truffe economiche e contraffazione

[9]Funzionalità rientrante negli sviluppi futuri del progetto

	Caso studio sulla tracciabilità della supply chain in Cina [33]	**Caso studio sulla tracciabilità del bestiame a Pogoniani [41]**	**Caso studio infrastruttura sicura in Brasile [42]**	**Caso studio dimostrativo di tesi del progetto PININ**
Tracciabilità dei capi al pascolo	X	X	X	X
Tracciabilità dei prodotti bovini e caseari nella filiera successiva	X		X	X
Integrazione tra IoT e blockchain per tracciatura geolocalizzata dei capi		X		X
Tracciabilità e controllo dati biomedici del capo		X	X	X
Tracciabilità e controllo erogazione fondi e sussidi				X
Definizione di recinti virtuali per il pascolo		X		X[9]

Tabella 3.1. Confronto funzionalità tra progetti

di informazioni le quali possono scaturire un affrettato discernimento di altri Paesi.

3.4 Le applicazioni già esistenti

Nella prima parte della seguente sezione saranno analizzati alcuni progetti ed applicazioni già in commercio, per testimoniare l'impiego della tecnologia, e in particolare della blockchain, nel settore agroalimentare; per poi passare ad un'analisi più dettagliata delle realizzazioni nel settore dell'allevamento e il pascolo di bestiame. Le analisi e gli studi condotti sul connubio tra tecnologia e agricoltura si sono soffermate ed entrate più in dettaglio per la parte dell'allevamento e quindi dei pascoli, essendo queste oggetto del progetto più ampio (dettagli al Capitolo 4) di cui questo lavoro di tesi fa parte, in modo poi da avvicinarsi al caso di studio di questo lavoro.

Ormai è noto come la tecnologia stia assumendo un ruolo importante nell'intero settore agroalimentare, non tralasciando però il settore dell'allevamento e dei pascoli. Infatti molte applicazioni tecnologiche, sfruttando proprio l'IoT e la blockchain, stanno rivoluzionando questo settore. Inoltre va ribadito come molti enti e associazioni, negli ultimi tempi, stiano evidenziando sempre più la necessità di valorizzare i prodotti locali, esaltandone le qualità e certificandone la provenienza e il trattamento.
In particolare sono state analizzate due realtà del nord Italia, entrambe legate al pascolo dei bovini e alla loro lavorazione (prodotti caseari e macellati), ed intente a valorizzare tramite la tecnologia i propri prodotti locali. Da un lato, nella Sezione 3.4.5, si ha un'idea nata per dare garanzia di qualità del prodotto finale, fornendo ai consumatori finali la possibilità di tracciare e validare, attraverso la blockchain, tutte le informazioni della filiera; dall'altro, nella Sezione 3.4.6, invece, si può notare come l'utilizzo di sistemi innovativi, come sensori IoT, possano fornire un servizio sia all'allevatore stesso che al consumatore.

La strategia che si è adottata per ed analizzare le applicazioni commerciali già esistenti è molto schematica, infatti per cercare di semplificarne la comprensione si è creata una struttura con quattro domande essenziali:

- *Chi?*: in cui si ha una brevissima introduzione sull'azienda o progetto.
- *Cosa?*: domanda centrale per comprendere il core del progetto.
- *Come?*: fornisce una visione dettagliata dell'idea e della sua realizzazione.
- *Vantaggi?*: risponde alla più frequente delle domande di chi sta valutando delle opportunità, che vantaggi si hanno?

Molte delle esistenti applicazioni sono strettamente legate al concetto di tracciabilità del prodotto finale lungo l'intera filiera, però quelle che sono state analizzate sono realtà che vanno a interpretare in modo più ampio questa relazione tra tecnologia e food, cercando di creare dei veri e propri punti di contatto tra produttori e consumatori certificando e verificando i prodotti finali.

3.4.1 Trusty

- *Chi?*: Trusty è una soluzione tecnologica sviluppata da Apio, azienda italiana nata nel 2014 che vanta molteplici collaborazioni con realtà nazionali e internazionali. E' il primo progetto italiano che ha visto l'applicazione della piattaforma di IBM (IBM Food Trust) per il settore alimentare.

- *Cosa?*: è una piattaforma basata su blockchain, nata con l'obiettivo di dare non una semplice visione di tracciabilità al consumatore finale, ma una vera e propria opportunità per il produttore per raccontarsi, narrando la storia del proprio prodotto, esaltandone le qualità caratterizzanti e coinvolgendo emotivamente il consumatore in modo da creare con esso un legame.
  La piattaforma è stata sperimentata e testata con uno use case sul vino, in collaborazione con Cantine Marramiero, il quale ha mostrato come una soluzione di questo tipo rappresenti una nuova opportunità di comunicazione tra produttori e consumatori.

- *Come?*: divulgando al consumatore tutti i processi di produzione e trasformazione il produttore ha la possibilità di raccontare la storia del proprio prodotto o dello specifico lotto di appartenenza. Questo è reso possibile grazie allo spazio web messo a disposizione del produttore e facilmente raggiungibile dal consumatore attraverso il QR code stampato sulla stessa etichetta del prodotto. Lo spazio web può essere personalizzato con foto, video, e tutte le informazioni che si ritengono necessarie al fine di regalare al consumatore una storia dettagliata e appassionante, garantendo sempre la sicurezza e la trasparenza delle informazioni.
  Inoltre Trusty è conforme allo standard GS1[10], che garantisce la struttura dei processi di trasformazione e approvvigionamento del prodotto. Sfruttando l'integrazione con IBM Food Trust il sistema associa un link ad ogni lotto e aggiorna in tempo reale la pagina web con le nuove informazioni.

- *Vantaggi?*: in un mondo ormai iperconnesso, le nuove tecnologie stanno riscrivendo i paradigmi della customer experience, l'inserimento di un QR code

[10]Global Standard, associazione dedicata allo sviluppo di standard globali per migliorare l'efficienza della filiera domanda-offerta

nella propria etichetta è un simbolo di identità e trasparenza verso il cliente. Trusty è uno strumento "circolare", che porta dei vantaggi informativi ai consumatori, ma allo stesso tempo anche ai produttori. Infatti, con un'analisi dei dati ricavabili dal QR code il produttore potrà acquisire informazioni strategiche per il proprio business ed instaurare un rapporto di reciproca fiducia con il consumatore.

3.4.2 Foodchain

- *Chi?*: FoodChain è un'azienda con diverse sedi nel nord Italia nata dalla fusione di due grandi passioni, la cucina e la tecnologia.
- *Cosa?*: sfruttano la blockchain per tracciare il percorso lungo tutta la filiera alimentare del prodotto, dal produttore iniziale al consumatore finale, offrendo a ogni partecipante interfacce web e app. Offrono una soluzione facilmente adattabile su ogni tipo di filiera, affidando ad ogni prodotto un codice univoco.
- *Come?*: ogni attore della FVC può registrare direttamente sulla piattaforma di FoodChain le informazioni del prodotto. L'intero ciclo produttivo, dall'iniziale produzione al posizionamento sullo scaffale è riportato nell'app del consumatore. Ogni singola informazione, che può essere sotto forma di testo, immagine o video, è registrata con un timestamp nella blockchain, che permette di ricavare data e ora dell'operazione, oltre che a garantirne l'immutabilità. Per rendere tutto questo funzionante al meglio, la società mette a disposizione hardware dedicato al mining delle transazioni e degli smart contract con cui interagire, oltre a i codici univoci con i quali il consumatore può accedere alle informazioni.
- *Vantaggi?*: sono la prima azienda italiana che ha unito questi due settori (agroalimentare e blockchain), mettendo in piedi un servizio modulare ed efficiente.

3.4.3 Posti

- *Chi?*: progetto nato dalla collaborazione di tre diverse realtà come il cuoco Antonello Colonna, l'azienda FoodChain e la startup romana pOsti.
- *Cosa?*: cerca di garantire la qualità all'interno dei ristoranti, offrendo al cliente una certificazione della ricetta e dei prodotti.
- *Come?*: il cliente con la scansione del QR code fornito in "allegato" al piatto ordinato, riesce a conoscerne la storia della ricetta, e assicurarsi sulla qualità di ogni singolo ingrediente del piatto. Questo progetto mostra come la blockchain può arrivare non solo nei progetti più complessi, ma anche nei più

semplici. Infatti la prima ricetta certifica è stata la "panzanella romana" piatto fatto di pochi ingredienti e molto semplici come pane, pomodoro, basilico e olio.

- *Vantaggi?*: Avere anche nella ristorazione la possibilità di controllare l'intera filiera delle materie prime e l'autenticità nella modalità di preparazione dei piatti.

3.4.4 Demeter

- *Chi?*: Demeter.life è una startup nata in Italia nel 2016, che vuole collegare direttamente i coltivatori con i consumatori.
- *Cosa?*: attraverso l'affitto di un "micro-campo", il consumatore può sostenere il coltivatore nella produzione, il quale a fine stagione raccoglierà e spedirà i frutti del lavoro al consumatore. Creando così un rapporto diretto tra i due attori che mette in luce un moderno livello di agricoltura sostenibile grazie a una nuova applicazione della blockchain.
- *Come?*: l'idea principale è quella di creare una connessione diretta tra coltivatore e consumatore, per rendere ciò possibile, si mette a disposizione degli attori un hub dove poter "affittare" dei micro-campi scegliendone la dimensione e la località. il coltivatore lavorerà al campo "affittato" e quando i suoi frutti saranno pronti verranno o spediti direttamente a casa del consumatore, o quest'ultimo potrà recarsi direttamente in loco per ritirarli. Nascerà così una vera e propria comunità, con le proprie regole per certificare il cibo biologico. Tutto questo naturalmente è supportato dalla blockchain (Ethereum), infatti la piattaforma è basata su un token proprietario (DMT) grazie al quale è possibile compiere ogni tipo di azione sulla piattaforma. La blockchain e la sua cripto-valuta assicurano e certificano ogni passaggio e lavorazione, garantendo così la tracciabilità del prodotto finale.
- *Vantaggi?*: grazie alla connessione diretta che si viene a formare è possibile ottenere dei prodotti con una qualità superiore, migliorando così gli standard di alimentazione dei consumatori senza dover eccedere nelle spese. Non solo i consumatori possono giovare del sistema, infatti i coltivatori in questo modo potranno essere remunerati in modo adeguato, in sicurezza e trasparenza in modo da mantenere viva la community.

3.4.5 Progetto tracciabilità razza Rendena

- *Chi?*: Apt - Azienda per il Turismo Madonna di Campiglio Pinzolo Val Rendena in collaborazione con pOsti, una startup romana dedita alla valorizzazione delle ricette tradizionali regionali italiane

- *Cosa?*: il progetto nasce con l'idea di tracciare le mucche rigorosamente di razza Rendena, le quali sono un presidio Slow Food[11], e i loro formaggi in modo da garantirne la semplicità e l'auteticità.

- *Come?*: il consumatore attraverso un semplice QR code edibile, riesce ad avere a portata di smartphone tutte le informazioni salvate in blockchain riguardanti la forma di formaggio che hanno davanti. Le informazioni disponibili sono le più disparate, da quelle riguardanti la mucca di razza Rendena a quelle sul pascolo, passando per quelle territoriali della malga e il malgaro, fino ad arrivare ad informazioni di produzione della forma di formaggio.

- *Vantaggi?*: l'idea di dare al consumatore una visione dell'intera produzione e informazioni di dettaglio su di essa portano una grande aggiunta di valore al prodotto stesso.

3.4.6 iGral

- *Chi?*: iGRAL - *Innovative beef cattle Grazing systems for the Restoration of Abandoned Lands in the Alpine and Mediterranean mountains* - è uno dei tre progetti di "agricoltura di montagna" finanziati da AGER - *AGricoltura E Ricerca* - la quale con altri partner, come università di Torino, si è posta l'obiettivo di recuperare e valorizzare i territori trascurati e secondari.

- *Cosa?*: con l'obiettivo di ripristinare degli spazi verdi migliori e più redditizi, in armonia con l'ecosistema ambientale, vengono studiati nuovi sistemi innovativi di pascolo, in modo da rivalorizzare le carni bovine delle razze Highland. In particolare si sta sperimentando la tracciabilità dello spostamento tramite GPS e la definizione di nuovi recinti virtuali.

- *Come?*: ogni bovino della mandria in esame è dotato di un particolare collare con un ricevitore GPS, il quale, con cadenza temporale regolare, invia ad un'antenna centrale la posizione, geolocalizzando il bovino. Questa antenna comunica tramite rete GSM con i server dell'azienda fornitrice dell'infrastruttura. In questo modo, è possibile avere un quadro real time della mandria, avvisando gli allevatori in caso di allontanamento di un capo o il superamento dei recinti virtualmente definiti.

- *Vantaggi?*:un sistema di questo tipo fornisce all'allevatore un ottimo supporto, in quanto in fase di alpeggio sono molti i capi che si allontanano dalla mandria e dunque che vengono dispersi, rappresentando una vera e propria

[11]associazione che si impegna a restituire il giusto valore al cibo, rispettando chi produce oltre che l'ambiente

perdita economica per l'allevatore. Inoltre con le informazioni raccolte è anche facilmente dimostrabile al consumatore la qualità del prodotto, fornendo indicazioni precise sull'allevamento e il pascolo.

Capitolo 4

Il progetto PININ

Nel seguente capitolo si andranno a definire più in dettaglio il caso d'uso analizzato e tutto il progetto circostante di cui fa parte, definendo gli obiettivi prefissati e gli effetti attesi, contestualizzando la nascita stessa del progetto e la sua articolazione.

4.1 Il progetto

Il progetto PININ - PIemuNt chèINa - prende forma con lo scopo di migliorare la qualità e la consapevolezza della stessa dei prodotti agricoli di fascia alta del Piemonte. L'utilizzo delle nuove tecnologie è la chiave primaria per la tracciabilità, la certificazione, l'autenticazione, per i sistemi innovativi per la commercializzazione dei prodotti nella catena alimentare e l'individuazione di falsi, di contraffazione e di truffe in modo da proteggere la qualità e i diritti di proprietà dei diversi marchi agroalimentari piemontesi [47].

Sono molteplici le tecnologie innovative portanti del progetto, dalla Blockchain all'Intelligenza Artificiale, passando per l'IoT, i Big Data e la Realtà Aumentata, in poche parole quasi tutte le tecnologie più recenti e innovative. Proprio sfruttando queste è possibile creare, da un lato, un sistema innovativo di tracciatura dei prodotti alimentari lungo tutta la filiera, dalle materie prime al consumatore finale, e dall'altro, un sistema che garantisce nuovi servizi per i diversi attori della filiera, ma soprattutto per il consumatore. Tutto ciò è realizzato con un pensiero fisso a quella che è l'economia circolare[1], quindi evitando sprechi alimentari, promuovendo prodotti a KM0 con nuove piattaforme di e-commerce e vendita, e tutelando l'utilizzo dei pascoli alpini in modo da garantirne la conservazione, preservando la biodiversità e l'assetto idrogeologico del territorio.

[1]sistema economico ideato per potersi ricostituire e sostenere in modo autonomo, garantendo dunque la sua ecosostenibilità

Il progetto, che vede *Consoft Sistemi S.p.a* come capofila insieme ad altre realtà aziendali nazionali e regionali, si colloca in uno dei due pilastri della strategia regionale S3, in particolar modo nell'ambito del *Made in Piemonte*. La strategia regionale S3 nasce da la contestualizzazione per le proprie esigenze da parte della regione rispetto a la strategia di crescita decisa dalla comunità europea "*Smart Specialisation Strategy - S3*" per gli anni 2014-2020 [46]. La strategia regionale S3, come anticipato poco sopra, si basa su due principali pilastri, da un lato si ha la necessità di tutelare il benessere dei cittadini dovuto ai repentini cambi demografici regionali, dall'altro si ha come obiettivo quello di innovare uno dei settori di eccellenza della regione come il sistema produttivo e industriale, ed è proprio in quest'ultimo che ritroviamo la valorizzazione del prodotto autoctono e il "Made in" [45]. La comunità europea sostiene economicamente queste scelte di crescita regionali, se ritenute pertinenti alle linee guida decise. La strategia piemontese è stata approvata nel 2016 [45] e la regione ha deciso di investire parte dei soldi in un bando "*Piattaforma tecnologica Bioeconomia*" dedicato alle aziende per diversi settori, come: agroalimentare, chimica verde, economia circolare. È proprio a seguito di questo bando che il progetto PININ ha preso forma, andandosi a collocare nell'ambito agroalimentare con una particolare attenzione all'utilizzo sensato ed intelligente delle risorse biologiche, e quindi della bioeconomia, per ciò che riguarda lo spreco alimentare. Essendo molteplici le aziende coinvolte per il progetto, che spaziano dal settore ICT[2] ad aziende impegnate nel settore della produzione e distribuzione dei prodotti alimentari, si può definire come un approccio interdisciplinare, finalizzato ad uno sviluppo di tecnologia non solo settoriale ma come risultato della loro collaborazione e con lo scopo ultimo di creare ecosistemi produttivi circolari sul territorio regionale.

La competizione tra le aziende che si orientano verso una vendita di prodotti di qualità è sempre maggiore, a causa della crescita da parte della grande distribuzione di vendite di prodotti di fascia alta, dove la qualità è la parola chiave. In aggiunta a ciò, vi è il costante incremento delle preoccupazioni del consumatore riguardo l'origine e la provenienza dei prodotti. Tutto questo si traduce in una necessità di differenziazione per le aziende, diminuendo i costi di certificazione di qualità e tracciabilità per fornire servizi innovativi al consumatore, il tutto accompagnato dall'introduzione di nuove tecnologie.
Le normative per la raccolta e la gestione dei dati sono molteplici e a volte molto stringenti per le aziende, le quali spesso si affidano a sistemi di raccolta automatizzati soprattutto per quelle informazioni che riguardano tracciabilità del prodotto, rimanendo però circoscritti ad una tracciabilità interna della singola azienda e non

[2]Information and Communication Technologies

ad una di più ampia veduta lungo tutta la filiera. Il problema di riuscire a portare queste informazioni in modo condiviso e chiaro lunga tutta la filiera con le attuali tecnologie maggiormente adottate e per la natura stessa della tipologia dei dati trattati risulta essere molto complesso, infatti non è possibile garantire la scalabilità del sistema lungo tutto il processo essendo dei sistemi disomogenei e non uniformi. Questa molteplicità di applicazioni e tracciature interne differenti possono risultare un vero e proprio problema per il sistema intero, andando a penalizzare l'efficienza della filiera e l'esperienza dell'utente finale, soprattutto all'aumentare del numero di partecipanti al processo.
La sicurezza, l'accessibilità e la fruibilità dei sistemi sono ormai all'ordine del giorno, così come la necessità di accedere ad informazioni diffuse lungo tutto il sistema con immediatezza, semplicità e velocità. Quindi, la possibilità di accesso a banche dati diverse mediante il medesimo strumento permette l'interazione di diversi attori della filiera che, in tal modo, validano le informazioni degli altri stakeholders incrementando la fiducia ed il grado di sicurezza dei diversi utenti.

Il progetto PININ nasce con l'idea di realizzare, prima di tutto, un'infrastruttura distribuita e decentralizzata basata su blockchain, in modo da poter garantire una tracciabilità del prodotto a diversi livelli di dettaglio (singolo prodotto, collo, lotto, ...) e di conseguenza tipologie diverse di informazioni come: scadenza, materie prime utilizzate, modalità di produzione, certificazioni, dettagli su l'etica, la sostenibilità, requisiti legati al gruppo etnico e religioso, informazioni nutrizionali, composizione e presenza di allergeni, ma anche altre informazioni che possono essere utilizzate in strategie di marketing e per la lotta alla contraffazione. L'istituzione di questi archivi decentralizzati e distribuiti uniti alla scalabilità lungo l'intera filiera permette, in tutte le fasi di manipolazione delle informazioni dalla visione all'elaborazione e modifica dei dati, di operare in tutta sicurezza e rispettando sempre le regole prestabilite. La difesa della qualità dei prodotti non riguarda solo le diverse fasi della filiera dei prodotti e la loro commercializzazione ma affronta anche problemi come la contraffazione, la protezione dei marchi e il rispetto delle regole.
Il pilastro portante del progetto è quindi la blockchain, che ha come obiettivo primario quello di autenticare e certificare una sempre più ampia gamma di prodotti e produzioni, in modo da instaurare un legame di fiducia con il consumatore. Si può definire come un approccio "a priori" alla tutela della qualità dei prodotti agroalimentari piemontesi di fascia alta. A supporto di questo vi è un filone di ricerca e sviluppo su applicazioni tecnologiche finalizzato all'*Internet IPRs*[3] *Intelligence* e all'*Online IPRs Protection* che assicura che i prodotti agroalimentari piemontesi di qualità non siano diffusi in modo errato, evitando contraffazioni e abusi degli IPRs.

[3] *Intellectual Property Rights - Diritti di Proprietà Industriale ed Intellettuale*

Quest'altro filone può essere visto come un approccio "a posteriori" alla tutela della qualità dei prodotti agroalimentari piemontesi di fascia alta. L'applicazione di entrambi gli approcci tecnologici e metodologici citati, a priori e a posteriori, consentirebbe quindi di ottenere un'elevata garanzia di tracciabilità e autenticazione dei prodotti agroalimentari e, al contempo, l'individuazione sistematica di prodotti falsi o illeciti sotto il profilo dei diritti di Proprietà Intellettuale utilizzati.

Il progetto si compone di quattro diversi dimostratori, volti a validare gli svariati ambiti applicativi. PININ è sperimentato su:

- Tracciabilità del prodotto nella grande distribuzione della carne Piemontese, che vede come partner principali La Granda e Eataly, e che offre al consumatore finali dei nuovi servizi innovativi pensati e progettati dagli altri partner come UNITO, HSC, Enhancers.
- Tracciabilità dell'erogazione dei fondi europei per gli allevamenti di bovini al pascolo in alpeggio e che vede coinvolti diversi attori come IPLA, UNITO, Interlogic, CSI Piemonte dovendo innovare il sistema di comunicazione tra i partecipanti al flusso dei dati e un nuovo tracciamento dei bovini.
- Anticontraffazione dei prodotti imbottigliati come vini e alcolici, con ulteriore analisi dei dati raccolti dalle interazioni tra i brand e i consumatori, andando a coinvolgere società come Guale Closures e L'Istituto Superiore Mario Boella - ISMB.
- Protezione dei marchi agroalimentari piemontesi attraverso l'individuazione di marchi falsi e la verifica del rispetto delle regole, ponendo particolare attenzione a prodotti D.O.P come Barolo e Asti spumante, ma anche prodotti industriali del territorio piemontese come Lavazza e Ferrero.

È possibile ripercorrere l'intera narrativa del progetto tramite la Figura 4.1, la quale riassume e unifica il progetto PININ. Sfruttando tecnologie innovative, e allo stesso tempo dirompenti, come la blockchain, AI, IoT e AR è necessario rivedere l'intero modello di business del settore agroalimentare e non solo introdurre soluzioni innovativi nei sistemi IT. Per poter rispettare le innumerevoli normative presenti in un settore come quello agroalimentare è necessario fin da subito tenerne conto. Il progetto nella sua completezza copre l'intera filiera a partire dalle materie prime fino alla distribuzione al dettaglio e al consumatore finale. Il primo punto di ingresso, in questo progetto, sono i pascoli alpini piemontesi e il tracciamento dei movimenti del bestiame al pascolo, in modo da poter fin da subito avere un pieno rispetto delle regole vigenti, come ad esempio quelle necessarie per i fondi europei a sostegno del pascolo alpino. Per poter rendere il tutto valido si ha bisogno di dispositivi IoT dotati di GPS nei collari dei capi. I dati così raccolti sono trasmessi in blockchain, rendendoli immutabili, in modo da potere avere un riscontro con le

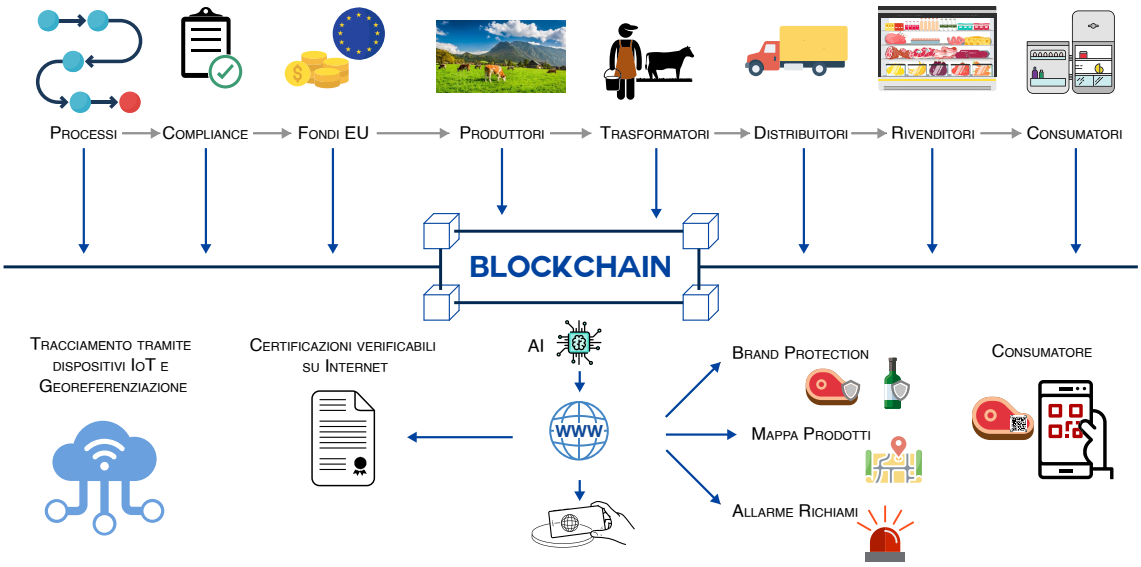

Figura 4.1. Narrativa del progetto PININ

mappe dei pascoli ottenibili dai diversi enti coinvolti per la richiesta ed erogazione dei contributi europei.
Il cammino lungo la filiera prosegue con l'analisi dei processi di trasformazione logistica e distribuzione della carne. In queste fasi ogni informazione ritenuta importante per dare una lettura di insieme all'intera filiera è salvata in blockchain. Quindi le informazioni sul lotto del prodotto e dei lotti delle materie prime o semilavorate utilizzate sono registrate.
Tutte queste informazioni riguardanti il lotto del prodotto sono liberamente accessibili dall'utente finale tramite un QR code allegato all'etichetta principale ed obbligatoria. Il QR code può essere quindi letto attraverso un'apposita applicazione per mobile o altri lettori dedicati, dando così accesso alle informazioni sul prodotto. Anche in fase di carico o scarico merci lungo il processo, sfruttando magari altri sistemi come RFID o NFC, è possibile registrare nuove informazioni importanti, come posizione del lotto in una mappa, temperature di trasporto e stoccaggio o info sulle scadenze. Naturalmente, il tutto facendo distinzione tra gli attori che compiono l'azione, infatti se oltre al rivenditore anche il consumatore riuscisse a dichiarare il possesso del prodotto di quel lotto, comunicazioni come ad esempio avvisi sul richiamo dei prodotti o le relative scadenze risulterebbero più efficienti ed efficaci. Infine, è importante sottolineare come non solo le informazioni contenute nella blockchain risulterebbero accessibili tramite QR code, ma anche tutte quelle

altre informazioni utili al consumatore, senza privarsi magari di nuove esperienze in realtà aumentata.

4.1.1 Finalità del progetto

Nella fase di sviluppo e ideazione del progetto, rispettando le linee guida della strategia S3 della regione Piemonte, si sono formulati gli obiettivi e gli effetti attesi del progetto PININ.
Gli obiettivi che il progetto si pone risultano essere:

- Analisi dei processi per la tracciabilità dei prodotti alimentari nei diversi contesti applicativi.
- Sfruttando tecnologie innovative come la Blockchain, l'IoT, i Big Data e l'Intelligenza Artificiale si realizza un'infrastruttura informatica distribuita per la tracciabilità alimentare basata su queste.
- Sfruttando l'infrastruttura specificata al punto precedente, si forniscono nuovi servizi per il consumatore, magari anche arricchendoli con AR/VR.
- Realizzazione di una vera e propria rete del prodotto, partendo dalle informazioni in blockchain e corredarlo di altre complementari.
- Realizzazione di una piattaforma informatica dedicata alla tracciabilità del bestiame al pascolo in alpeggio, per fronteggiare le truffe nella ricezione dei fondi europei, sfruttando tecnologie come la blockchain e l'IoT.
- Sviluppo un sistema di anticontraffazione per i prodotti imbottigliati, sfruttando tecnologie come NFC, GPS, blockchain, in modo da poter strutturare anche una piattaforma IoT per la raccolta e l'analisi dei dati della filiera.
- Sviluppo di un sistema di ricerca di falsi prodotti alimentari con brand piemontese su siti di e-commerce.
- Analisi degli aspetti normativi con il supporto di nuove tecnologie.
- Sperimentazione dell'intera struttura sui quattro dimostratori proposti per la tracciabilità alimentare, la tracciabilità dell'erogazione dei fondi europei per i pascoli, l'anticontraffazione dei prodotti imbottigliati e l'individuazione di marchi falsi sui siti e-commerce.

Gli effetti attesi sul sistema produttivo e i suoi prodotti locali risultano essere:

- Miglioramento della qualità dei prodotti piemontesi sotto tutti gli aspetti analizzati, dalla tracciabilità alla contraffazione e il rispetto delle regole.

- Aumento di competitività nel proprio settore di appartenenza per le aziende che partecipano al progetto grazie ai nuovi servizi innovativi offerti ai consumatori.
- Riduzione degli sprechi monitorando i prodotti in scadenza e garantendone la freschezza.
- Maggiore efficienza nell'erogazione dei fondi europei per l'agricoltura e l'allevamento.
- Diminuzione dei prodotti contraffatti e con marchi falsi sul mercato.
- Creazione di una conoscenza base della relazione tra brand e consumatore, attraverso l'analisi dei dati per creare nuovi meccanismi di ingaggio, consapevolezza e fiducia.

4.2 Caso d'uso: *Tracciabilità dei fondi Europei per l'allevamento*

I quattro diversi dimostratori del progetto presentati brevemente nella Sezione 4.1 sfruttano metodologie di sviluppo e progettazione focalizzata sull'utente finale [4] e i suoi limiti e desideri sulle funzionalità del prodotto proposto, facendogli ricoprire un ruolo fondamentale in tutte le fasi di progettazione. Gli utenti saranno coinvolti dalle prime fasi delle indagini preliminari per individuare le problematiche, le esigenze e i requisiti degli utenti, in modo da fornire fin da subito soluzioni pratiche e facilmente integrabili; alla valutazione sul campo delle soluzioni proposte, in modo da poterle calibrare al meglio sui reali bisogni ed usi degli utenti. In questo tipo di progettazione le fasi di progetto, sviluppo, valutazione e riprogettazione sono molteplici, e talvolta anche partecipativa con utenti e stakeholder cosi da ottimizzare le soluzioni per i contesti di utilizzo specifico. Per l'intero progetto le soluzioni proposte sono:

- Sistema basato su blockchain per la tracciabilità della carne di Eataly "la Granda" e i relativi servizi per il consumatore che li consulta;
- Tracciabilità con sistemi IoT e Blockchain nell'erogazione dei fondi Europei per l'allevamento di bovini al pascolo in alpe;
- Sistema per l'anticontraffazione dei prodotti imbottigliati, con particolare attenzione al vino e agli alcolici tipici regionali;

[4] UCD - User Centered Design

- Protezione dei marchi di qualità per prodotti alimentari piemontesi e la relativa compliance regolativa;

La soluzione presentata per la tracciabilità dei fondi europei per l'allevamento è quella analizzata, approfondita e presa come caso d'uso per questo lavoro di tesi (Figura 4.2). Come ampiamente descritto nella Sezione 4.2.1 l'erogazione dei fondi

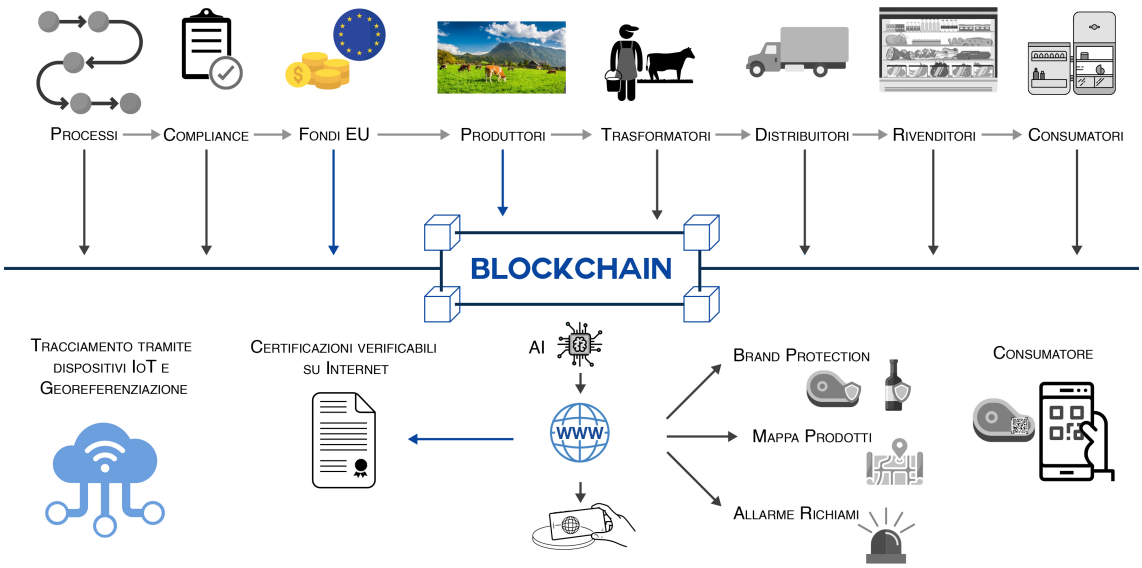

Figura 4.2. Narrativa del progetto PININ: Tracciabilità dei fondi Europei per l'allevamento

europei dedicati all'allevamento di bovini in alpeggio è protagonista di molteplici truffe ai danni delle diverse regioni italiane. Il pagamento del sostegno economico per gli allevatori deve avvenire sulla base di adeguati controlli che ad oggi risultano ancora molto difficili e articolati, proprio per evitare possibili frodi e truffe. Per la regione Piemonte l'organismo che si occupa dell'erogazione di questi contributi è l'ARPEA[5].
La criticità tecnica più grande per la realizzazione di questa soluzione è la corretta individuazione dei capi al pascolo con il proprio codice pascolo e la relativa associazione alla particella catastale afferente a quel codice. Tutto ciò nasce dalle esigenze di monitorare gli effettivi spostamenti dei bovini al pascolo, che ad oggi risultano essere solo informazioni proveniente da alcuni modelli auto-compilativi (Modello

[5]Agezia Regionale Piemontese per l'Erogazione in Agricoltura

IV e VII) depositati nella Banca Dati Nazionale, rispetto al reale uso delle superfici afferenti solo a quel pascolo. Altri problemi si hanno proprio con l'associazione tra codice pascolo relativo ai comprensori pascolivi e la loro riconduzione alle particelle catastali, informazioni spesso difficili da reperire sia in BDN che negli stessi comuni nei quali tali comprensori ricadono, facendo riflettere su l'effettiva corrispondenza e attendibilità che tali informazioni attualmente hanno, si riscontrano infatti grandi difficoltà nell'associare e far corrispondere ciò che viene dichiarato sui moduli e il reale dimensionamento delle particelle in loco.
Le aziende coinvolte sono più di 4000, e gli ettari delle superfici da monitorare risultano essere dell'ordine di centinaia di migliaia ($\sim$135'000 ha). Data la moltitudine di aziende coinvolte e l'ampia area geografica in cui operare, ad oggi, dove l'unico metro di verifica attuato sono delle puntuali indagini e controlli, i fondi e i sostegni economici vengono erogati sulla sola verifica di congruenza di dati tra le particelle dichiarate in BDN e quelle in Domanda Unica di pagamento. Quindi la situazione della mappatura di alpeggi in relazione alle particelle risulta essere disomogenea a livello dei diversi comuni e della regione stessa, ed è proprio da questo disallineamento che ARPEA, insieme a IPLA e CSI si sta muovendo per allineare ed aggiornare queste informazioni, in modo da rendere più attendibile l'ammissibilità e la correttezza dei pagamenti ai richiedenti.

Se da un lato, dunque, si ha il problema del disallineamento di informazione tra pascoli e particelle catastali, dall'altro si ha la necessità di verificare e certificare l'effettiva monticazione nelle zone indicate come pascoli ed legalmente assegnate. Questo sia per i motivi di riqualifica e sostentamento delle aree d'alpeggio, che garantiscono una rigenerazione e un sostentamento per la biodiversità e l'ecosistema nella sua interezza, ma anche per motivi veterinari. In tal senso non è pensabile al momento effettuare un controllo preciso e puntuale su tutti i capi o su tutte le mandrie sul territorio piemontese.

Proprio dall'unione di queste due problematiche che il caso d'uso prende forma, andando a sottolineare la necessità di nuovi sistemi sperimentali IoT per la tracciatura geolocalizzata di tutti i capi o parte di essi nelle mandrie, al fine di riuscire ad agevolare controlli anche a posteriori della movimentazione durante le fasi di alpeggio. Dalla necessità di tener traccia di queste informazioni per i futuri controlli, si fonde, insieme al sistema IoT, il sistema blockchain, il quale ne aumenta il valore di veridicità e autenticità delle informazioni, prevenendo manomissioni o altri inganni.
Tutto ciò è reso possibile dal sistema di tracciamento autonomo inserito all'interno dei collari dei bovini, senza possibilità di manomissione e che è in grado di restituire informazioni utili quali:

- registrare la posizione e gli spostamenti dei capi conservandoli in modo sicuro e

non manipolabile per un periodo abbastanza lungo da garantire la reperibilità delle informazioni,

- avere un sistema di alimentazione tale da garantire le funzioni per l'intero periodo di pascolo in alpeggio, senza necessità di sostituzioni o ricariche,
- trasmettere i dati ad un lettore in modo autonomo o su richiesta di un operatore.

Quindi il sistema in questione permette di risolvere i problemi sopra descritti, andando a fornire un sistema IoT per la tracciatura dei bovini legandoli ai pascoli di appartenenza e alle rispettive particelle catastali, ma in un'ottica più ampia, unendo le forze con il sistema blockchain, si crea un unico sistema che garantisce la tracciabilità del prodotto finale, partendo proprio dal pascolo del bovino fino ad arrivare alla tavola. Si può dire, dunque, che questo caso d'uso preso in analisi si inserisce nell'intera narrativa del progetto PININ come anello iniziale, risolvendo problematiche legate alle prime fasi della filiera ma con un'attenzione e un'applicazione di più ampia veduta, in modo da rispettare il paradigma UCD e tener sempre in mente le esigenze del consumatore finale.

La realizzazione del caso d'uso richiede una stretta collaborazione tra le diverse aziende ed enti che ne fanno parte. Dapprima bisogna infatti menzionare Consoft sistemi S.p.a, la quale fa da capofila del progetto, e grazie ai suoi molteplici ambiti applicativi riesce a fare da collante tra le diverse aziende. Consoft ha il compito di realizzare tutto il sistema relativo alla blockchain, supportata però dalle preziose informazioni fornite del CSI Piemonte e IPLA, i quali contribuiscono alla realizzazione provvedendo a tutta la parte relativa a normative a regolamentazioni agroalimentari e dell'allevamento. Queste informazioni sono altrettanto utili ad Interlogic, la quale si occupa della realizzazione del sistema IoT per i collari Smart per rendere il tutto funzionante.

4.2.1 Il problema dei fondi europei

Il FEASR - Fondo Europeo Agricolo per lo Sviluppo Rurale - è il fondo europeo nato per il sostentamento e lo sviluppo in scenari rurali e agricoli di aziende ed imprese operanti nell'intera comunità europea, rispettando le linee delle politiche rurali europee. In particolare dal 2014 al 2020 il FEASR ha come obiettivo quello di migliorare la competitività del sistema agricolo, porre attenzione alla produzione sostenibile e rispettosa per l'ambiente ed il clima, ed infine, aiutare a sviluppare in realtà rurali, economia e posti di lavoro. Proprio in linea con quest'ultimo obiettivo, l'unione europea, in accordo con le diverse regioni italiane retribuisce gli allevatori che si offrono di far pascolare i propri capi in alpeggio, migliorandone ed aiutandone il mantenimento biodiversificato. Infatti attraverso l'opera di monticatura i

territori riescono a trovare un equilibrio ed uno sviluppo maggiore in termini di biodiversità e sostenibilità idrogeologica ed ambientale.

Se però, da un lato possiamo dire che questi aiuti europei sono una grossa opportunità per gli allevatori onesti, dall'altro risultano essere altrettanto vantaggiosi per i "disonesti". Infatti la possibilità che gli allevatori approfittino di queste agevolazioni è concreta, e gli eventi accaduti in alcune regioni italiane ne sono la dimostrazione. Questi fondi europei nascono con l'idea di aiutare giovani agricoltori allo sviluppo delle proprie attività, ma non essendoci molti controlli, spesso si fa molta difficoltà a prevenire truffe e frodi, da parte degli allevatori stessi e spesso, in alcune regioni, anche dalla mafia.

Nella regione Piemonte la procedura per la richiesta è fin troppo semplice, soprattutto da eludere. Infatti, gli allevatori devono presentare un modulo dove spontaneamente dichiarano il codice e l'area di pascolo, dove e per quanto porteranno i capi al pascolo. Solo a fine stagione vi è un'altra presentazione di documenti, dove sempre gli allevatori confermano o modificano le informazioni precedentemente dichiarate, come ad esempio possibili nascite o decessi dei capi. Già a questo punto si può iniziare a capire come sia abbastanza semplice realizzare truffe, richiedendo sostentamenti maggiori di quelli che realmente spetterebbero. In aggiunta a tutto questo ci sono le impervie aree di pascolo, che sono difficilmente raggiungibili, sono allocate in aree sperdute e spesso distanti chilometri e chilometri l'una dall'altra. Gli operatori che si dovrebbero occupare di controllare e verificare si trovano a dover operare in scenari non molto favorevoli, e che spesso richiedono intere giornate per essere raggiunti. Da l'unione di tutto questo pascolo delle vere a proprie truffe ai danni dell'Europa, la quale ignara delle situazioni e convinta di sostenere l'agricoltura si ritrova purtroppo spesso a sostenere dei veri e propri illeciti.

Percorrendo l'intera Italia, regione dopo regione, sono presenti molteplici notizie, facilmente reperibili in rete[6], che documentano la dannosa gestione, e le innumerevoli frodi compiute in tutti questi anni. Banalmente se si cerca su un motore di ricerca "*fondi europei per l'allevamento*" i primi risultati parlano proprio di vere e proprie truffe. Risulta quindi più difficile trovare delle informazioni su questi fondi che non le notizie di truffe compiute. Bisogna ricordare però anche tutti gli allevatori onesti, che usufruiscono del sostegno rispettando le leggi e dichiarando il vero, per realizzare prodotti di altissima qualità e valore.

Il caso d'uso analizzato dunque nasce da un lato per proporre nuove regole per

[6]digitando su un motore di ricerca "fondi europei pascolo" i primi risultati sono notizie di riferimento a frodi o illeciti

l'assegnazione dei contributi, infatti sfruttando le più innovative tecnologie si vuole creare un sistema valido robusto e veritiero per tracciare gli spostamenti dei bovini, ma dall'altro anche per tutelare tutti gli allevatori onesti, in modo da offrire un supporto per continuare a produrre ottimi prodotti. Tutto ciò, dunque, resta perfettamente in linea con la strategia S3 regionale a sostegno del "Made in Piemonte", una delle finalità dell'intero progetto PININ.

4.2.2 Innovazioni perseguite

Come emerso nella Sezione 3.3, la comunità scientifica di tutto il mondo sta sempre più sperimentando le nuove tecnologie nei più disparati settori. In particolare, si può notare come i paesi extra UE stiano procedendo ad un'integrazione sempre più massiccia e valida di blockchain ed IoT in molti settori, soprattutto nelle supply chain. In Europa, invece, si sta mettendo in primo piano un uso della blockchain legato spesso al mondo della finanza, anche se non mancano alcuni esempi di applicazioni al mondo produttivo e agroalimentare.

In Italia, la sperimentazione e realizzazione di applicativi blockchain integrati all'IoT procede abbastanza bene, soprattutto nella regione Piemonte, la quale, sfruttando i diversi progetti di ricerca regionali ed europei sui sistemi blockchain, si dimostra essere uno dei centri principali di ricerca a livello italiano. Ed è proprio da questi punti di forza, unendo le diverse competenze sulla tecnologia, dalla blockchain all'IoT, dall'Intelligenza artificiale ai Big Data, delle diverse imprese del territorio che prende forma il progetto intero di PININ.

In un contesto come quello di questo progetto, dove tutti i diversi attori della filiera devono stabilire e mantenere un livello di collaborazione e condivisione di informazioni elevato lungo tutta la catena di creazione del valore, le principali caratteristiche della blockchain come il decentramento, la fiducia e la scalabilità, risultano essere fondamentali. Per realizzare tutto ciò, ottimizzando la gestione della catena di approvvigionamento e dei processi di business di tutte le imprese coinvolte, l'applicazione nella sua interezza proposta da PININ è necessaria per rendere più semplice la comunicazione tra i diversi processi attraverso delle API o un'integrazione personalizzata in modo da interfacciarsi al mondo reale e ai consumatori nel migliore dei modi.

Relativamente al caso d'uso, e quindi al tracciamento dei bovini al pascolo in alpeggio, per la duplice funzione di tracciabilità per il prodotto e controllo per i finanziamenti europei, l'integrazione delle due tecnologie IoT e blockchain risulta essere fondamentale, proponendo e sperimentando dal lato IoT RFID semi-passivi e NFC sicuri oltre che a nuovi collari per i capi e tutta la relativa infrastruttura di

comunicazione, dal lato blockchain l'utilizzo della stessa con la piattaforma Ethereum e i relativi smart contract per la gestione di registrazione e analisi dei dati raccolti.
L'impatto atteso per le aziende coinvolte nell'intero progetto, ma soprattutto in questa parte, ricade sullo sviluppo di una soluzione innovativa per la tracciabilità alimentare, lungo tutta la filiera andando a gestire i processi iniziali e la burocrazia circostante, per poi proseguire in un vero e proprio attestato di qualità lungo la filiera, in modo da arrivare al consumatore ed essere facilmente compresa, verificata e giudicata da esso. Tutta questa innovazione nel sistema produttivo, inoltre, favorisce la competitività delle imprese partecipanti, ma più in generale, per il tessuto sociale rappresenta una vera e propria opportunità di rinnovamento, andando a migliorare la qualità dei prodotti agroalimentari attraverso la tracciabilità e la protezione dai falsi e imitazioni, facendo diminuire gli sprechi con un monitoraggio più attivo e preciso, aumentando la soddisfazione del consumatore migliorandone le relazioni con il produttore, raccogliendo dati importanti che se analizzati possono rinnovare e modificare il processo abbattendo costi e migliorando ancora di più la qualità del prodotto secondo le abitudini di consumo, e infine, strettamente legato al caso d'uso, si ha un miglioramento e un aumento di controllo sull'utilizzo dei terreni adibiti al pascolo al fine di ottenere una maggiore efficienza nella distribuzione dei fondi europei per l'agricoltura e l'allevamento.

Quindi, la piattaforma proposta nella sua interezza mette a disposizione un sistema di anticontraffazione, tracciamento, e promozione innovativa attraverso la blockchain e IoT (NFC - RFID). In particolar modo il caso d'uso analizzato vuole offrire un punto di ingresso all'intero sistema, andando a risolvere un grande problema come quello delle truffe per il pascolo realizzando un innovativo sistema di tracciamento per i bovini incorruttibile e sicuro. I sistemi di tracciamento avanzati hanno il potenziale di influire su ogni fase della catena del valore, il quale si traduce in un importante vantaggio competitivo strategico.

Capitolo 5

Progettazione

La fase di progettazione per questo lavoro di tesi è stata articolata e complessa, in quanto risulta essere un caso d'uso molto dettagliato e ricco di particolarità tecniche del settore agroalimentare e, in particolare, dell'allevamento. Per poter comprendere fin da subito di cosa si sta parlando e di come le diverse informazioni sono correlate fra di loro, bisogna avere in mente, quanto meno, un quadro generico del funzionamento e dell'ambito di applicazione. Prima di tutto, dunque, bisogna ricordare che in questo progetto, che come ormai è chiaro, fa parte del progetto PININ, la chiave innovativa del funzionamento è data dall'uso della Blockchain insieme ad elementi di IoT per tracciare lo spostamento durante il periodo di pascolo dei bovini in alpe, in modo da garantire e certificare tutte quelle informazioni necessarie ad una corretta erogazione dei fondi europei. Dopodiché, bisogna ricordare le diverse problematiche e limitazioni nei controlli legate all'erogazione stessa dei fondi, dove la fraudolenza prende fin troppo spesso piede, a discapito di tutti gli allevatori onesti che necessitano di sostegni.
Proprio partendo dall'unione di queste due punti centrali si è andato ad operare sul progetto, quindi, dopo una ricostruzione dettagliata dell'attuale flusso di informazioni si è aggiunto e ipotizzato un'integrazione con il nuovo sistema blockchain, pensato e sviluppato per l'intero progetto.

Nelle prime fasi di studio è risultato complicato inquadrare al meglio le problematiche da risolvere e le esigenze dei vari utenti della filiera coinvolti. Una volta inquadrate le principali problematiche dell'attuale situazione nel settore dell'erogazione dei fondi europei per il pascolo in alpe, riconducibili a due principali criticità, quali:

- estrema necessità di verificare e certificare l'effettiva monticazione nelle zone indicate per garantire rigenerazione e sostentamento della biodiversità;
- associazione tra pascolo di appartenenza di un determinato bovino e la relativa particella catastale;

è stato possibile effettuare e stimare due elementi fondamentali nella fase di progettazione come il *Use Case Diagram* (Figura 5) e il *Sequence Diagram*. Lo sviluppo del progetto applicativo, dunque, prende forma a partire da questi elementi, i quali permettono sia di avere un quadro più chiaro d'insieme e quindi di poter affrontare in modo schematico ogni singolo problema dell'intero flusso, ma anche di fornire una solida base di partenza per l'elaborazione della parte progettuale implementativa vera e propria e più di dettaglio. Infatti, grazie alle informazioni contenute da questi documenti, è stato possibile individuare in modo più chiaro e sicuro le analogie tra i vari flussi di informazioni e le relative criticità.

Attraverso i sopracitati strumenti progettuali, è stato possibile avere un quadro più dettagliato dell'intero flusso di informazioni del caso d'uso. Infatti, si può notare come gli attori coinvolti lungo tutto il flusso di informazioni è di numero pari a undici, ognuno con le proprie relazioni informative e ambiti applicativi, anche se generalizzando le applicazioni è possibile descrivere il flusso con i soli cinque attori presenti nell'*Use Case Diagram*, in quanto ricoprono i ruoli di maggiore interesse per l'intero processo.

Per poter capire meglio il flusso di informazioni, si deve avere a mente chi possono essere gli attori coinvolti nell'intero flusso di informazioni. Più in dettaglio:

- Allevatore/CAA - Centri di Assistenza Agricola o gli stessi allevatori, che si occupano di gestire tutta la parte di registrazione di anagrafe;
- Veterinario - attore che ricopre il compito di gestire tutta la parte di verifica delle informazioni di anagrafe richieste dall'allevatore o dal CAA, e nel seguente caso d'uso è anche il garante della corretta installazione dei collari;
- Sindaco - è stato riportato il sindaco, ma non sempre ne risponde lui in prima persona ma delega la mansione a qualche funzionario comunale. Ha il compito di verificare e accettare le richieste effettuate dagli allevatori tramite il Modello 7 per l'autorizzazione a pascolare;
- Interlogic - attore che si occupa della gestione delle informazioni riguardante i dati provenienti dai collari smart;
- IPLA - attore strettamente necessario, in quanto è l'attuale risoluzione al problema dell'associazione tra pascoli e particelle catastali, sta generando una correlazione dettagliata di queste due informazioni connesse tra loro da una relazione *N a N*;
- CSI - principale attore del flusso, esegue molte delle attività necessarie alla registrazione delle informazioni in blockchain, da quelle strettamente legate all'anagrafe e quindi nascita e morte a quelle delle richieste dei finanziamenti, passando per informazioni riguardanti i pascoli e le relative autorizzazioni;

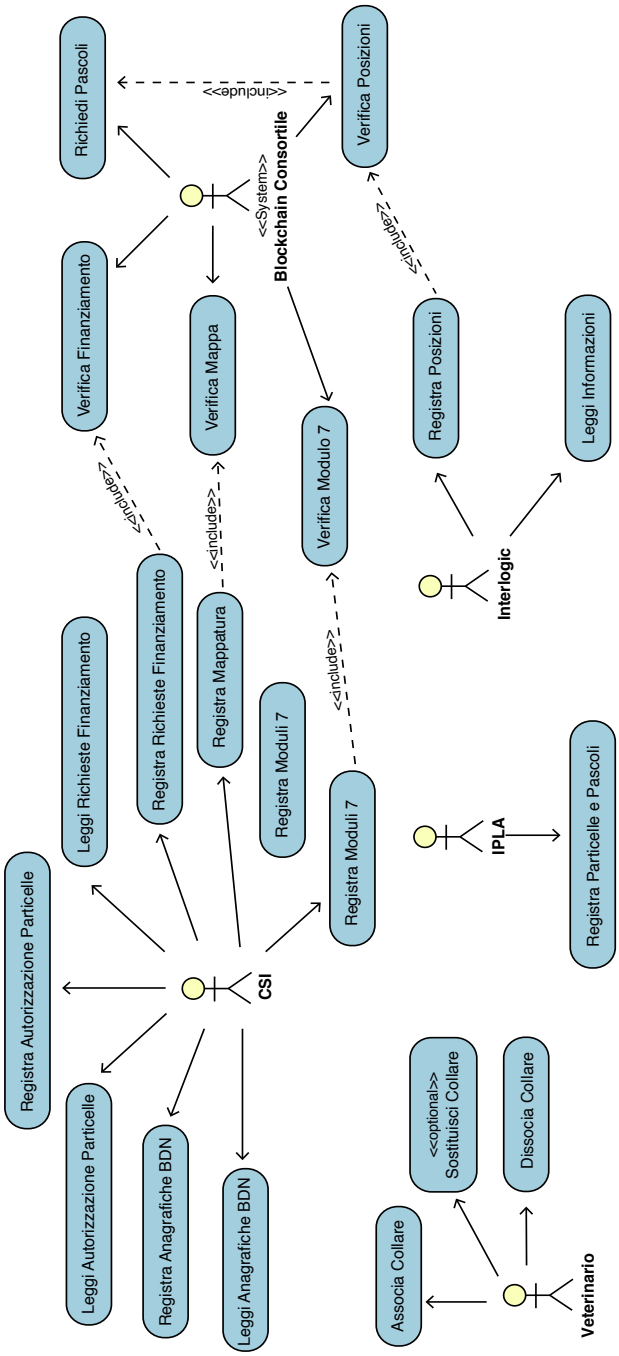

Figura 5.1. *Use Case Diagram* dei fondi europei per il pascolo

- Anagrafe agricola - attore che si occupa di gestire le informazioni riguardanti le autorizzazioni a pascolare sulle particelle catastali, proveniente dalle richieste della domanda grafica effettuata dagli allevatori;

- BDN - è la Banca Dati Nazionale, in questo processo è l'attore che contiene molte delle informazioni attualmente esistenti nel mondo agroalimentare e della loro anagrafe;

- Arvet - attore che si occupa di gestire le richieste di pascolo presentato tramite modulo 7;

- DEMETRA - attore che si occupa di gestire le richieste di finanziamento presentate dagli allevatori;

- Blockchain Consortile - attore chiave del processo, principale innovazione del flusso e il detentore di tutte le informazioni immutabili necessarie ad un corretto funzionamento della soluzione.

Il flusso di informazioni ha come origine la nascita di un bovino, la quale necessita di una registrazione nell'apposita anagrafe bovina nazionale entro un determinato numero di giorni, cosi come in caso di decesso o di cambio di proprietario. Queste informazioni una volta generate sono raccolte nella Banca Dati Nazionale (BDN). Durante l'intero flusso di informazioni, principalmente, solo tre attori partecipano alla scrittura di informazioni in blockchain, e sono IPLA, CSI e Interlogic. Tutte quelle informazioni recuperabili dalla BDN e dall'anagrafe agricola regionale o relative alle autorizzazioni a pascolare vengono aggiunte in blockchain dal CSI. Le informazioni riconducibili alla relazione tra pascoli e particelle catastali, cosi come quelle relative ai moduli presentati dagli allevatori per la richiesta dei fondi vengono salvate da IPLA; mentre le informazioni relative ai collari smart, sono riconducibili ad Interlogic, essendo il partner di progetto che ne sta curando lo sviluppo e progettazione.
Da un attenta analisi e riflessione effettuata sul *Sequence Diagram* si è notato che in modo generico le interazioni eseguite con la blockchain sono sempre le stesse, cambiano le informazioni da salvare, e quindi presumibilmente le strutture dati necessarie per farlo, ma le azioni compiute sono simili lungo tutto il caso d'uso. Le interazioni maggiormente eseguite sono:

- registrazione in blockchain di informazioni;

- possibile verifica delle informazioni registrate, anche a posteriori, o comunque in modo disgiunto con la registrazione;

- richiesta di accedere a tali informazioni salvate in blockchain.

Proprio partendo da queste tre diverse tipologie di interazioni, si è arrivati alla conclusione di concentrarsi su una sola parte del flusso di dati, quello che maggiormente ricoprisse le tre tipologie e nel modo più complesso e articolato. A tal proposito, la scelta effettuata ricade sulla parte del flusso di dati relativa ai collari smart e il salvataggio delle informazioni ricavate da essi. Come visibile nella Figura 5.2 si è voluto analizzare la registrazione delle informazioni ricavate dai collari e la loro verifica, in quanto, a differenza delle altre verifiche necessita di un "*Oracolo*", e quindi si è ritenuto più interessante ai fini della tesi e ai fini progettuali analizzare in dettaglio questo preciso punto del flusso di informazioni. Prima di procede con la descrizione dell'architettura adottata per la soluzione proposta, relativa al salvataggio dei dati dei collari e la loro verifica, si vuole inquadrare l'uso della blockchain, motivandone le diverse scelte progettuali effettuate che hanno quindi poi portato alla realizzazione dell'architettura progettuale stessa.

Come anticipato all'inizio di questa sezione, l'utilizzo della blockchain è la chiave innovativa dell'intero progetto PININ. Sfruttando tutte le caratteristiche descritte nel Capitolo 2, intrinsecamente la blockchain riesce a garantire autenticità, trasparenza e immutabilità alle informazioni salvate su di essa. Questi tre aspetti sono fondamentali per la realizzazione del progetto e la risoluzione delle problematiche che afferiscono all'assegnazione dei fondi europei per il pascolo.
Essendoci diverse tipi di blockchain, private pubbliche o consortili, sono state analizzate i pro e i contro delle diverse tipologie prima di arrivare a sceglierne una da adottare nel progetto. Se sicuramente da un lato la blockchain pubblica è quella che a tutti gli effetti riesce a mantenere un alto livello di decentralizzazione, dall'altro non sempre risulta essere la soluzione migliore, soprattutto in termini economici, essendo spesso le transazioni da effettuare un numero molto elevato. Per questo caso d'uso, infatti, si è strutturato un sistema consortile, dove quindi i diversi nodi selezionati hanno il controllo della rete che non viene lasciata in mano ad un singolo ente come nella privata ma non risulta essere nemmeno totalmente decentralizzata. Si è scelta questa tipologia di blockchain in quanto risulta essere un'ottima scelta nei settori dove gli attori partecipanti appartengono allo stesso settore, hanno diverse informazioni da doversi scambiare l'un l'altro, sia dal punto di vista di funzionalità del prodotto finale sia dal punto di vista di conoscenza extra-aziendale per offrire un servizio migliore. Dunque, la totalità delle informazioni che vengono immagazzinate sono salvate in una blockchain consortile, basata su Ethereum e che quindi attraverso l'invocazione di diversi smart contract permette il salvataggio delle informazioni. Come appena citato, la blockchain consortile adottata è una blockchain basata su Ethereum, dove non solo gli utenti di questo flusso di dati hanno accesso, ma anche tutti gli altri utenti degli altri casi dimostrativi del progetto, essendo quindi questa una blockchain consortile a livello progettuale.
Per questo specifico caso d'uso, non si è sentita l'esigenza di aggiungere, oltre alla

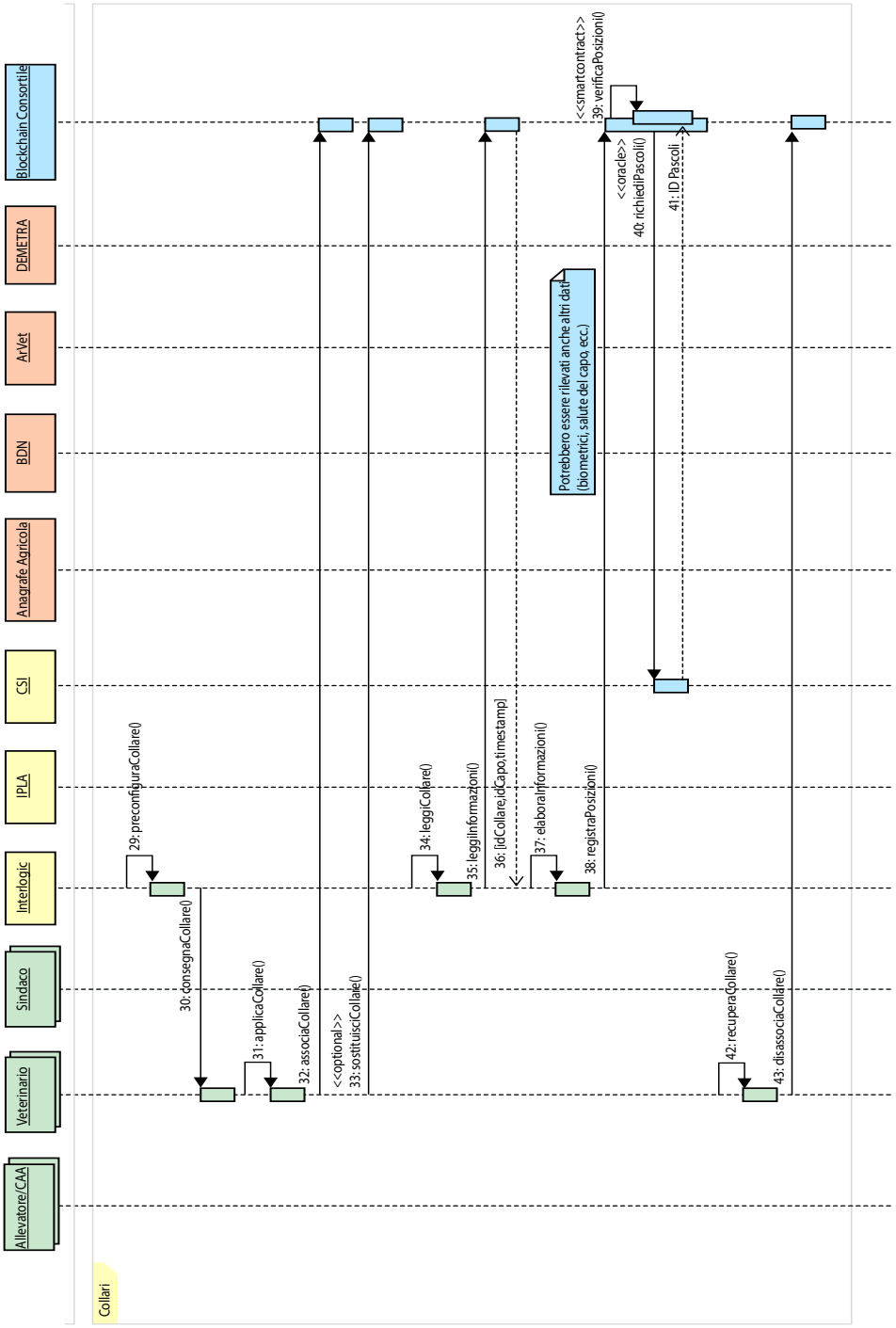

Figura 5.2. Frammento *Sequence Diagram* relativo ai dati dei collari

blockchain consortile, anche delle interazioni con una blockchain pubblica, a differenza di altri casi d'uso, come ad esempio, il sistema basato su blockchain per la tracciabilità della carne di Eataly "la Granda" e i relativi servizi per il consumatore che li consulta, in cui è previsto il salvataggio di alcune informazioni riguardanti ordini e consegne in blockchain pubblica.

5.1 Architettura progettuale

In generale, il concetto dell'architettura progettuale è molto vario e dinamico, essendo composto dalla moltitudine di scelte effettuate lungo tutta la durata del processo progettuale, in cui il progettista fa delle scelte spesso invisibili all'utente finale ma che ne influenzano e spesso ne determinano il funzionamento.

In questo progetto, che come sopracitato, si va ad inserire all'interno del caso d'uso del tracciamento dei fondi europei, che a sua volta fa parte di un progetto più ampio di nome PININ, l'architettura implementata è stata frutto di molteplici e diverse analisi. Si è partito dapprima con lo studio e l'analisi del flusso delle informazioni per arrivare a capire in dettaglio quali dati fossero realmente condivisi, trasmessi e necessari alla realizzazione del progetto, in modo da riuscire a creare fin dall'inizio delle strutture dati ben precise negli smart constract, i quali rappresentano il fulcro centrale del progetto. Proprio mettendo gli smart contract al centro della progettazione dell'architettura che si è strutturato il lavoro poi adottato. Infatti, la soluzione finale adottata è stata modificata più volte, proprio per riuscire a creare una soluzione il più possibile scalabile e soprattutto sensata per il lavoro che si stava svolgendo. Inizialmente la struttura era composta da due nuclei, uno legato alla blockchain e quindi agli smart contract, e un'altra legata strettamente all'interfaccia con la relativa distinzione tra front-end e back-end. L'insieme di smart contract sviluppati erano 4, di cui due per la registrazione di informazioni, uno per la verifica e uno per la gestione dell'oracolo, in modo da tenere anche in fase progettuale distinzione dei ruoli di ogni smart contract, facilitandone eventuali revisioni e future implementazioni e applicazioni. Dopo un'attenta analisi delle tecnologie utilizzabili per realizzare l'oracolo, si è scelto di modificare la struttura, eliminando lo smart contract dell'oracolo e facendo gestire quest'ultimo direttamente allo smart contract che si occupava della verifica delle informazioni. Dunque, dopo questa rivisitazione e modifica di sviluppo, dettata dalla necessità di adozione di altre tipologie di tecnologie rispetto a quelle considerate inizialmente, si è arrivati alla soluzione finale adottata. Quest'ultima prevede una suddivisione dell'architettura in tre differenti nuclei, uno in più rispetto alla prima soluzione pensata. Il cuore centrale del progetto restano gli smart contract, i quali progettati in modo separato l'uno dall'altro per garantire scalabilità e replicazione lungo tutto il flusso e progetto. Questi tre differenti smart contract si occupano di gestire la registrazione e la verifica delle

informazioni provenienti dai collari. I tre smart contract, oltre a condividere informazioni tra di loro, hanno anche dei collegamenti con il mondo *off-chain*. Da un lato i due smart contract di registrazione delle informazioni interagiscono con quella che è la parte di front-end del progetto, mentre lo smart contract di verifica delle informazioni, oltre a interagire con i due smart contract di registrazione delle informazioni, interagisce con un ulteriore server esterno alla blockchain, che ha il ruolo di *Oracolo* (vedi Sezione 2.5.1). Questo server esterno a sua volta interagisce con quello che più propriamente è considerabile l'oracolo vero e proprio, ovvero un servizio REST[1] che ricevuti determinati parametri restituisce dei valori, che concretamente sono latitudine e longitudine della posizione del bovino ottenute dal collare grazie alle quali poi si ricava il codice pascolo di appartenenza. Infine, per avere un quadro più preciso dell'architettura, lo smart contract di verifica ha anche delle relazioni con il back-end dell'interfaccia, che rende l'uso dell'applicativo più semplice e user friendly. Uno schema riassuntivo ed esemplificativo dell'architettura finale adottata è visibile in Figura 5.3, mentre i dettagli implementativi sono rimandati al Capitolo 6.

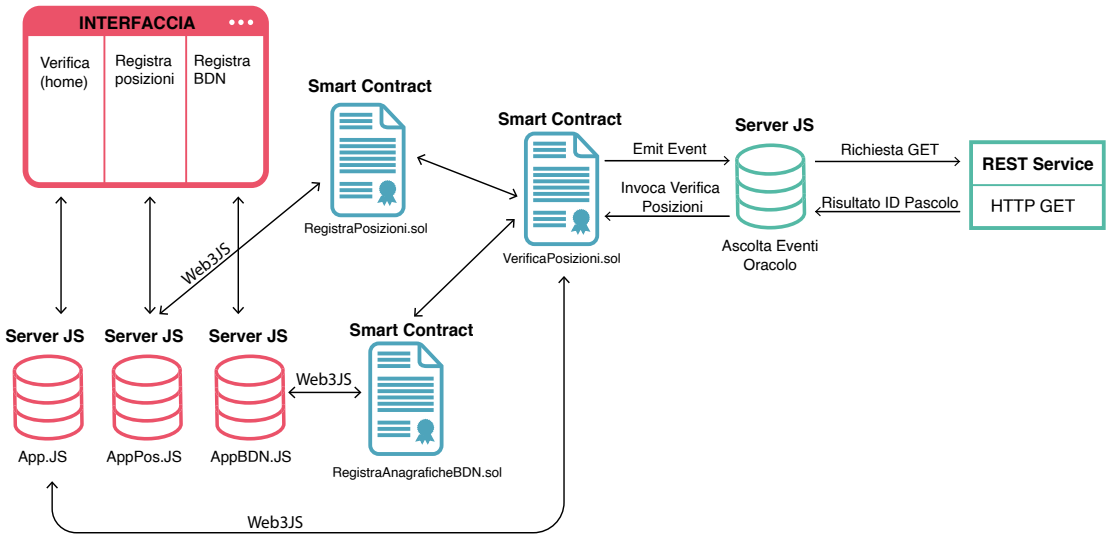

Figura 5.3. Architettura del progetto

Questa tipologia di struttura, che mette al centro i tre smart contract e da un lato

[1]REpresentational State Transfer - modello architetturale per la comunicazione tra dispositivi remoti connessi ad Internet

la parte di interfaccia e dall'altro la gestione dell'oracolo, è stata ottenuta e voluta per cercare di mantenere soprattutto in fase implementativa separazione e netta distinzione tra gli elementi e i propri ruoli nell'intero sistema. Questa divisione degli smart contract è, inoltre, dettata da limiti di sviluppo legati al consumo di gas nelle transazioni e durante l'interazione con essi. Proprio con un occhio di riguardo al consumo di gas, e quindi al costo ipotetico che ogni interazione con esso scatenasse, si sono implementati i diversi smart contract. Uno dei principali obiettivi in fase di sviluppo è stato proprio l'ottimizzazione in termini di consumi per gli smart contract, infatti si sono analizzati singolarmente tutti i dati da salvare e minimizzati gli spazi per memorizzarli. Questa tipologia di programmazione degli smart contract, orientata all'ottimizzazione del consumo di risorse è la base dello sviluppo stesso degli smart contract, infatti essendo un codice potenzialmente eseguibile da tutti, essendo pubblicato in blockchain, anche un millesimo di consumo in meno può risultare vincente sull'adozione da parte di altri utenti.

Capitolo 6

Dettagli implementativi

Nelle seguenti sezioni sono descritte, in modo dettagliato, tutte le componenti sviluppate durante il lavoro di tesi presso Consoft Sistemi s.p.a.
Per poter descrivere nel migliore dei modi tutti i dettagli si è scelto di strutturare l'intero Capitolo in tre macro sezioni, ognuna delle quali corrispondente a uno dei tre nuclei dell'architettura precedentemente presentata nel Capitolo 5. Infatti nella prima parte saranno descritti i tre smart contract sviluppati, motore dell'intero studio e progettazione. Successivamente, saranno analizzate le due componenti afferenti al sistema dell'Oracolo e, infine, sarà data una panoramica di come è stata strutturata la dApp[1] e la sua relativa interfaccia.

Prima di procedere all'analisi e descrizione di dettaglio delle differenti caratteristiche implementative, si vuole dare una panoramica d'insieme dei dettagli. Nella prima parte sviluppata, quella degli smart contract è stato utilizzato il linguaggio di programmazione Solidity, linguaggio di alto livello e orientato agli oggetti per l'implementazione di smart contract che vengono eseguiti nella EVM[2]. Il suo sviluppo è stato influenzato da linguaggi come C++, Python e JavaScript.
Nella seconda parte, invece si è sviluppato sfruttando JavaScript e Java, grazie ai quali è stato possibile realizzare server e servizi REST[3]. Durante tutto lo sviluppo, in parallelo, si è anche portata avanti una piccola dApp, dove grazie alla sua interfaccia è possibile interagire con gli smart contract in maniera più semplice e user friendly. La dApp è stata progettata sfruttando, appunto, gli smart contract connessi a server JavaScript per il back-end dell'applicazione e del linguaggio JavaScript e HTML con la libreria Bootstrap per il front-end.

---

[1] APPlicazione Decentralizzata

[2] Ethereum Virtual Machine

[3] REpresentational State Transfer - modello architetturale per la comunicazione tra dispositivi remoti connessi ad Internet

La domanda che sicuramente può insorgere a questo punto, avendo un quadro generico di come sono stati sviluppate le tre parti architetturali è: *Come è possibile far comunicare degli smart contract sviluppati con Solidity con dei server off-chain sviluppati in JavaScript?* La risposta è molto semplice, sfruttando la libreria *web3.js*. Questa collezione di librerie permette di interagire con un nodo di Ethereum locale o remoto utilizzando connessioni HTTP, IPC o WebSocket. Quindi a tutti gli effetti è un API che permette questa connessione tra i due mondi, on-chain e off-chain, tra smart contract e i server esterni in JavaScript. Alla base del funzionamento di queste API vi è un oggetto JSON, che va sotto il nome di interfaccia JSON, che descrive l'Application Binary Interface (ABI) per uno smart contract di Ethereum. Utilizzando questa interfaccia JSON, la libreria *web3.js* è in grado di creare un oggetto JavaScript che rappresenta lo smart contract stesso, ed interagire con i suoi metodi ed eventi utilizzando l'oggetto *web3.eth.Contract*.

Il sistema Blockchain è stato realizzato con degli strumenti di supporto quali Truffle, Ganache e MetaMask. Il primo è stato sfruttato per poter avere un buon ambiente di svilluppo, supportato da framework di test per realizzare più facilmente la dApp, mentre con il secondo, Ganache, si è costituita la rete blockchain di test, basata su EVM e con caratteristiche molto simili al sistema di riferimento per il progetto, che risulta essere una blockchain consortile regionale ancora in fase di lavorazione. Le principali caratteristiche della Blockchain di test del lavoro sono:

- Punto di accesso alla Blockchain locale (127.0.0.1:7545);
- Automining, quindi all'arrivo di ogni transazione viene subito minata;
- *Gas Limit* settato a 6721975;
- *Gas Price* settato a 20000000000 wei[4];
- Nella rete ci sono 10 account con un balance di circa 80 ETH ciascuno.

MetaMask, infine è stato sfruttato per la gestione del wallet dell'utente e delle API Ethereum web3 che esso introduce nel contesto JavaScript di ogni sito web, in modo che applicazioni distribuite possano leggere dalla blockchain. Tenendo in mente tutto questo preambolo sulle caratteristiche dei differenti nuclei di sviluppo e la modalità di connessione tra di loro, si può procedere a vedere più in dettaglio e singolarmente le differenti componenti.

[4] 1 wei = $0.000000000000000001 (10^{-18})$ ether

6.1 Smart Contract

La fase di sviluppo implementativa, come quella progettuale, è partita proprio da questo nucleo. Lo sviluppo di smart contract è sicuramente la parte centrale di tutto il progetto, essendo questi gli elementi più innovativi.

Gli smart contract sviluppati, come già menzionato in precedenza, sono tre, due relativi alla registrazione di informazioni in blockchain e uno per la verifica delle posizioni dei bovini al pascolo. Il caso d'uso di dettaglio analizzato è la registrazione e la verifica delle posizioni rilevate attraverso i collari dei bovini, ma per poter eseguire le verifiche si doveva predisporre di altre informazioni relative ai capi e pascoli provenienti dalla BDN. Per questo è stato anche implementato lo smart contract che gestisce la registrazione di queste informazioni.

Di seguito sono riportati i dettagli implementativi di ogni singolo smart contract.

6.1.1 Registra Posizioni Bovini

Questo contratto è quello relativo alla registrazione in blockchain delle informazioni ricavate dai collari, che Interlogic, o chi per loro invocherà ogni qual volta si voglia salvare in blockchain nuove informazioni su un capo e la sua posizione di pascolo.

Il contratto è strutturato con un costruttore, una funzione per il salvataggio, e differenti funzioni per interrogare ed ottenere i dati dalla blockchain.
Il costruttore, il quale viene eseguito solo al momento del deploy[5] del contratto in blockchain, inizializza l'account proprietario, il quale, in modo esclusivo, avrà accesso alla scrittura di nuove informazioni in blockchain mediante questo contratto.
Per poter salvare le informazioni è stata implementata una mappa di strutture appositamente definite avente per chiave il codice id del capo. La struttura dati sfruttata è composta da:

- una stringa che rappresenta l'id collare;
- una stringa che rappresenta l'id capo;
- un intero senza segno basato su 128 bit per la latitudine del posizionamento del capo, il quale valore è adattato da decimale ad intero;
- un intero senza segno basato su 128 bit per la longitudine del posizionamento del capo, il quale valore è adattato da decimale ad intero;

[5] rilascio del software utilizzabile

- un intero senza segno basato su 256 bit per il timestamp dei dati ricevuti da parte del collare, importante non confonderlo con il timestamp della transazione di quando tali informazioni sono registrate in blockchain;
- un booleano che rappresenta l'esistenza o meno di informazioni in blockchain di un determinato capo.

Le differenze dei bit tra le diverse variabili della struttura è stata frutto di un'attenta analisi del tipo di informazione da salvare, e del relativo consumo di gas. Ogni qual volta si invoca la funzione appositamente implementata per il salvataggio delle posizioni del capo, tutte le variabili della struttura vengono ricevute come parametri della funzione stessa e aggiunte alla mappa. Inoltre all'esecuzione di questa funzione viene scatenato un evento che segnala l'avvenuta nuova registrazione e che serve alla dApp per aggiornare la propria interfaccia.
Come anticipato prima, le altre funzioni all'interno del contratto sono delle *Get-functions* e quindi implementate per restituire dei dati alla loro invocazione.

6.1.2 Regista Anagrafiche BDN

Rappresenta lo smart contract di supporto allo specifico caso d'uso analizzato, attraverso il quale si possono salvare in blockchain molte delle informazioni contenute nella BDN. Anche in questo caso, come nel precedente, il contratto prevede un costruttore, una funzione per il salvataggio dei dati e altre funzioni ausiliarie per ottenere i valori salvati.

Il costruttore, ha lo stesso ruolo del costruttore dello smart contract di registrazione delle posizioni, ovvero quello di inizializzare l'account proprietario, in modo da evitare scritture e salvataggi da parte di terzi in modo anomalo e inatteso.
Il principio di funzionamento della funzione di salvataggio è molto simile a quella precedente, quindi, attraverso una mappa si tiene traccia dell'insieme di dati utili. La mappa ha come chiave il codice id del capo e come valore la struttura dati ad essa associata. Quest'ultima è naturalmente differente dalla precedente, infatti è più articolata e composta da diversi elementi, quali:

- una stringa che rappresenta l'id capo;
- una stringa che rappresenta il tag dell'auricolare attualmente utilizzato per segnare i bovini;
- un intero senza segno basato su 64 bit per la data di nascita del bovino adattata in una successione di otto numeri dove i primi quattro rappresentano l'anno i due successivi il mese e infine il giorno;
- una stringa che rappresenta la razza del bovino;

- un intero senza segno basato su 32 bit per salvare il codice del proprietario del bovino che risulta essere totalmente numerico;
- una stringa che identifica il codice alfanumerico dell'azienda detentrice del capo;
- una stringa che rappresenta l'id pascolo;
- un intero senza segno basato su 64 bit per salvare la data di ingresso al pascolo del bovino, secondo la stessa logica della data di nascita;
- un intero senza segno basato su 64 bit per salvare la data di rientro dal pascolo del bovino, secondo la stessa logica della data di nascita;
- un booleano che rappresenta l'esistenza o meno di informazioni in blockchain di un determinato capo.

Per sviluppare questa articolata struttura dati si sono dovute fare delle scelte molto stringenti in termini di spazio di memoria, in quanto essendo un gran numero di elementi era molto facile superare i limiti di gas in fase di salvataggio. Per questo motivo le date sono state mantenute nell'ordine di anno-mese-giorno e non trasformate in timestamp, più facilmente gestibili dal calcolatore.
Anche in questo caso, la funzione di salvataggio riceve come parametri tutti gli elementi della struttura dati associata e dopo il controllo di esistenza e abilitazione aggiunge alla mappa le nuove informazioni. Viene scatenato un evento di segnalazione per l'avvenuta invocazione della funzione in modo da poter, anche in questo caso, segnalare alla dApp gli aggiornamenti.
Le altre funzioni presenti nello smart contract hanno il ruolo di restituire di dati salvati sotto forma di singole strutture della mappa stessa o solo alcuni elementi di esse.

6.1.3 Verifica Posizione e Pascolo

Questo è il contratto che si occupa di fare le opportune verifiche delle informazioni salvate in blockchain e la loro relativa congruenza. Nasce principalmente con lo scopo di dare la possibilità a un utente finale o chi di dovere di verificare l'effettivo pascolo dei capi nelle zone autorizzate, per poter certificare ed erogare i fondi nel migliore dei modi possibili, evitando frodi e truffe.
La struttura di questo smart contract è differente dagli altri due precedenti (sezioni 6.1.1 e 6.1.2), infatti non dovendo registrare dati ma bensì verificarne, ha la necessità di connessioni e risorse di informazioni esterne, proprio dagli altri due smart contract di registrazione. Gli indirizzi dei due smart contract di registrazione sono necessari per creare degli oggetti che permettano di interagire con le funzioni contenute in essi. Per questo sono state implementate due funzioni distinte, una per ogni

address, le quali ricevono come parametro l'indirizzo del contratto di registrazione specifico ed inizializzano l'apposita variabile.
Una volta settati gli indirizzi e quindi creati gli oggetti è possibile interagire con gli altri smart contract ed accedere alle mappe con i dati in essi salvati. La funzione di verifica che può essere invocata dall'utente dunque recupera le informazioni necessarie per ottenere l'id Pascolo di appartenenza di quel bovino specifico. Dunque, una volta ricevuto il codice id capo del bovino da verificare, vengono recuperate la latitudine e la longitudine del capo dal primo contratto descritto, e queste informazioni sono passate come parametri per l'invocazione dell'oracolo attraverso l'emissione di un evento, come visibile qui sotto nella parte di codice riporta

```
function verifica(string memory _idCapo) public{
    uint128 latitudine;
    uint128 longitudine;
    RegistraPosizione p = RegistraPosizione(adrRegistraPosizione);
    latitudine = p.getLat(_idCapo);
    longitudine = p.getLong(_idCapo);
    emit oracleEvent(latitudine,longitudine,_idCapo);
    }
```

L'evento viene gestito da un server esterno alla blockchain che una volta calcolato il risultato invoca una nuova funzione (*analizzaRisultatoOracolo*) implementata in questo smart contract che a tutti gli effetti compara i due risultati ottenuti, come si può notare nel seguente codice.

```
function analizzaRisultatoOracolo(string memory idPascoloOracolo,
   string memory _idCapo) public{
    require(server == msg.sender, "Non e' il server ad aver
       invocato la funzione!");
    idPascolo = idPascoloOracolo;
    certifica = compareStrings(idPascoloOracolo,callAnagraficheBDN(
       _idCapo));
    if(certifica){
    mappaEsiti[_idCapo]=2; //2=true
    } else {
     mappaEsiti[_idCapo]=1; //1=false
     }
    emit NewVerificaPosizioni(certifica);
    }
```

Se i risultati ottenuti dall'oracolo coincidono con il risultato salvato nella mappa del contratto della BDN allora un booleano viene inizializzato a *true*, viene aggiornata la mappa che tiene traccia dei vari esiti delle verifiche e viene emesso un ulteriore evento per l'aggiornamento della dApp.
Ricapitolando si può vedere questo smart contract suddiviso in 4 differenti aree di funzioni:

- funzioni per settare gli indirizzi dei contratti di registrazione;

- funzioni per interagire con gli smart contract esterni;
- funzioni per interrogare l'oracolo e gestirne i risultati;
- funzioni di visualizzazione e restituzione di dati salvati nella blockchain attraverso il contratto in questione.

Le due funzioni che servono, rispettivamente, a interrogare l'oracolo e gestirne i risultati emettono entrambe un evento. Il primo per invocare l'oracolo e passare i parametri di latitudine e longitudine al server esterno, la seconda funzione invece emette l'evento per aggiornare la dApp e visualizzare l'esito della verifica.

6.2 Oracolo

In un'ottica più generale del problema affrontato nel caso d'uso, questa parte implementativa non è sempre presente, in quanto solo il caso di dettaglio della registrazione dei collari necessita di un oracolo esterno per poter ricavare, a partire dalle informazioni di latitudine e longitudine, il relativo codice id pascolo necessario ad identificare la validità della richiesta di sostegno economico.
Nel caso analizzato in questo lavoro di tesi, e portato come dimostrativo di effettiva possibilità di realizzazione, il ruolo che questo ricopre è fondamentale, in quanto rappresenta l'entità che riesce a congiungere le informazioni della blockchain con algoritmi esterni per la georeferenziazione dei pascoli.

Questo nucleo di sviluppo è composto da due componenti:

- un server d'ascolto su eventi scatenati dallo smart contract di verifica;
- un servizio web REST che ricevendo i parametri dalle chiamate GET HTTP ne restituisce il risultato.

Le due componenti comunicato tra di loro per arrivare ad ottenere il codice pascolo, in modo da poter restituire al contratto che ha invocato l'oracolo il risultato nel minor tempo possibile e con la massima sicurezza.

6.2.1 Server

Tra le due componenti che fanno parte del nucleo architetturale dell'oracolo, sicuramente questa è quella più vicina al mondo blockchain, in quanto sfruttando le librerie di *web3.js* riesce a rimanere in ascolto sul solo evento scatenato dallo smart contract di verifica, in modo da poter garantire il corretto funzionamento e a sua volta comunicare con il servizio REST annesso.
Il server in questione, è un semplice server sviluppato in JavaScript, che attraverso la libreria *web3.js* e le ABI del contratto riesce a generarsi l'oggetto JavaScript dello

smart contract sul quale poi operare per invocare le funzioni e rimanere in ascolto sugli eventi generati da esso. Per poter creare l'oggetto JavaScript del contratto oltre alle ABI di quest'ultimo, necessita dell'inizializzazione dell'indirizzo del contratto in blockchain e dell'indirizzo dell'account con cui eseguire le transazioni per interagire con il contratto, come è possibile vedere nel frammento di codice riportato di seguito.

```
1  const XMLHttpRequest = require("xmlhttprequest").XMLHttpRequest;
2  const Web3 = require('web3');
3  const web3 = new Web3('ws://127.0.0.1:7545');
4  const abi =[...];
5
6  const address = '0x4dF4B562C8302514a366d4aa257A5bB0B2583054'; //
       address dello smc VerificaPosizioni deployato
7  const contract = new web3.eth.Contract(abi, address); //istanza del
       contratto
8  const account = '0xf79684856bC4d7Bd7e3a1316b6f2D086dea63B0f'; //
       account per eseguire le transazioni delle chiamate a funzioni
9  const adattaVirgola = 100000; // numero costante per adattare lat e
       long da float a interi e viceversa
```

La funzione principale sviluppata è composta dall'implementazione dell'attesa dell'evento, dal quale, una volta ricevuto, si estraggono i parametri di latitudine e longitudine per creare la richiesta HTTP da inoltrare al servizio REST. I parametri di latitudine e longitudine ricevuti devono essere adattati e resi dati reali, in quanto potendo registrare in blockchain solo numeri interi in fase di salvataggio viene eliminata la virgola, ma in fase di elaborazione da parte del servizio REST il dato è ripristinato secondo la forma decimale, in modo da rendere ed operare con valori reali di coordinate.

```
1  main();
2
3  function main(){
4    listen();
5  }
6
7  function listen(){
8    console.log('-----------------------------------------------');
9    console.log('Server in ascolto...');
10   contract.events.oracleEvent().on('data', (event) => {
11     var latitudine=event.returnValues[0]/adattaVirgola;
12     var longitudine=event.returnValues[1]/adattaVirgola;
13     console.log("lat e long: "+latitudine+" n"+longitudine);
14     var url='http://localhost:8080/Oracolo?lat='+latitudine+'&long=
         '+longitudine;
15     console.log("richiesta Oraclo: "+url);
16     //GET
```

```
17      var client = new HttpClient();
18      client.get(url, function(response) {
19        console.log(response);
20        var results=JSON.parse(response);
21        console.log(account);
22        console.log(event.returnValues[2]);
23        contract.methods.analizzaRisultatoOracolo(results.idPascolo,
              event.returnValues[2]).send({from: account, gas:3000000})
24        .then(function(res){});
25        console.log('-----------------------------------------');
26        console.log('Server in ascolto...');
27      });
28      }).on('error', console.error);
29  }
```

Una volta inviata la richiesta di elaborazione e ricevuta la relativa risposta la medesima funzione provvede a invocare una nuova funzione dello smart contract di verifica, la quale si occuperà di confrontare e verificare l'uguaglianza tra i due risultati ottenuti dall'oracolo e dalle informazioni di blockchain attraverso la comparazione delle due diverse stringhe ricevute.

6.2.2 Servizio REST

Questa componente del nucleo dell'oracolo, è quella più legata all'algoritmo di elaborazione e calcolo del codice pascolo a partire dalle coordinate di posizione. Lo sviluppo in dettaglio di particolari algoritmi è rimandato a altri enti partecipanti al progetto PININ, per questo lavoro di tesi però si è ritenuto necessario ipotizzare una possibile connessione tra blockchain e algoritmi, in particolare i possibili risultati ottenibili sono stati simulati e salvati in apposite mappe del sistema REST, come visibile nella porzione di codice di seguito riportata.

```
1  public class OraclePosition {
2
3    private final double latitudine;
4    private final double longitudine;
5    private final String idPascolo;
6
7    public OraclePosition(double latitudine, double longitudine) {
8      this.latitudine = latitudine;
9      this.longitudine = longitudine;
10     this.idPascolo = CalcolaParticella(this.latitudine,this.
           longitudine);
11   }
```

Attualmente, il servizio ricevuti i parametri di latitudine e longitudine, attraverso un algoritmo di ricerca in una mappa, verifica l'appartenenza ad un pascolo piuttosto che ad un altro verificando prima il range della latitudine e poi verificandone anche la longitudine. Solo dopo il soddisfacimento di entrambe, viene assegnato un

codice pascolo alla coppia di coordinate analizzate, come riportato nel frammento sottostante.

```
1 private String CalcolaParticella(double latitudine, double
    longitudine) {
2     for (String key : mappaParticelle.keySet()) {
3       double[] value = mappaParticelle.get(key);
4       if(latitudine>=value[0] && latitudine<=value[1] &&
            longitudine>=value[2] && longitudine<=value[3])
5         return key;
6   }
7   return "fuori Pascolo";
8 }
```

I dati utilizzati per simulare le aree di pascolo sono stati ottenuti dividendo l'intera area della regione Piemonte in sub-aree e assegnando ad ognuna di essa un codice pascolo differente. Questa strategia è una chiara semplificazione di algoritmi necessari alla gestione reale del caso, dove le aree di pascolo sono identificate da un codice pascolo ma le autorizzazioni a pascolare vengono richieste sulla scala delle particelle catastali, creando così una relazione tra codice pascoli e particelle catastali di N *a* N non sempre facilmente gestibile.

Il sistema REST è stato implementato sfruttando il framework *Spring*, così da avere un template ben strutturato su cui lavorare e poter sfruttare librerie ed API ben sviluppate, veloci e sicure.

6.3 dApp

La diffusione delle dApp, come ampiamente descritto nel Capitolo 2, è particolarmente cresciuta con l'espansione della Blockchain.
In questo lavoro di tesi, questo elemento ricopre un ruolo secondario, in quanto frutto di una volontà di semplificazione per l'esposizione del lavoro e per renderlo più piacevole e semplice.

Nelle Sezioni che seguono si presenterà in particolare la componente front-end dell'applicazione e verrà fatto un breve rimando a quello che, invece, in questa dApp ricopre il ruolo di back-end.

6.3.1 Front-end

La parte visibile all'utente dell'applicazione sviluppata si presenta articolata e suddivisa in tre sezioni, rispettivamente riconducibili ai tre smart contract presentati in precedenza.

Il cuore centrale, che è possibile definire come *Home* dell'applicazione, è rappresentata dall'interfaccia che permette di verificare se le aree di pascolo rilevate di un determinato capo sono riconducibili a le aree concesse a quell'allevatore. La pagina si presenta divisa in due aree principali. La prima, più in alto presenta una tabella dove vengono visualizzati i risultati ottenuti dalla richiesta di verifica relativa a: idCapo, idPascolo[6], idPascoloBDN[7]. Inoltre è presente un'area di testo con un bottone dove è possibile inserire il codice del capo di cui si vuole effettuare la richiesta. L'esito della richiesta oltre a popolare la tabella mostra a video un elemento grafico con la descrizione dell'esito stesso. Infine, in questa prima parte è presente l'indirizzo dell'account con cui si stanno eseguendo le transazioni in blockchain. La seconda parte della pagina, più in basso, è riconducibile invece a delle operazioni preliminare da effettuare sullo smart contract di verifica. Come descritto nella Sezione 6.1.3, questo smart contract, che fa da back-end per questa pagina, necessita di interazioni con gli altri due presenti nella blockchain. Quindi con questi elementi presenti nella seconda parte della pagina è possibile interagire con lo smart contract e le sue funzioni per settare gli address di riferimento degli smart contract di registrazione. Ogni smart contract ha una propria area di testo con il rispettivo bottone per convalidare l'interazione. In Figura 6.1 è possibile vedere la schermata "*Home*" descritta. Importante è sottolineare come la fase di verifica segua, in base al numero di volte che si effettua un controllo su un determinato capo, due flussi differenti, facendo distinzione tra una prima verifica o una ripetizione di controllo su un capo già precedentemente verificato. Questa distinzione è utile nel momento in cui si vuole verificare ad esempio un capo al pascolo dell'anno precedente, o comunque una situazione non in linea con lo stato attuale della mappatura conosciuta dall'oracolo a cui si fa richiesta. Infatti, se il capo non è mai stato verificato, il flusso di istruzioni convoglia le informazioni necessarie per inoltrare la richiesta all'oracolo, il quale risponderà invocando lo smart contract, come descritto nella Sezione 6.2.1. Altrimenti, se l'*idCapo* che si vuole controllare è già stato verificato, attraverso un'interazione con una mappa salvata nello smart contract di verifica, la quale tiene traccia delle verifiche già effettuate, viene restituito l'esito precedentemente ottenuto, andando così a risolvere eventuali problemi di confusione all'interno dell'oracolo. In questo modo, inoltre, è possibile evitare l'aggiunta di database esterni che tengano traccia di queste informazioni e delle varie transazioni e interazioni avute con lo smart contract, così da lasciare invariata l'architettura progettuale.
Oltre alla pagina di "*Home*" sono presenti altre due pagine, *Regista Posizioni* e

[6]codice id ricavato dall'Oracolo

[7]codice id di riferimento salvato in BDN

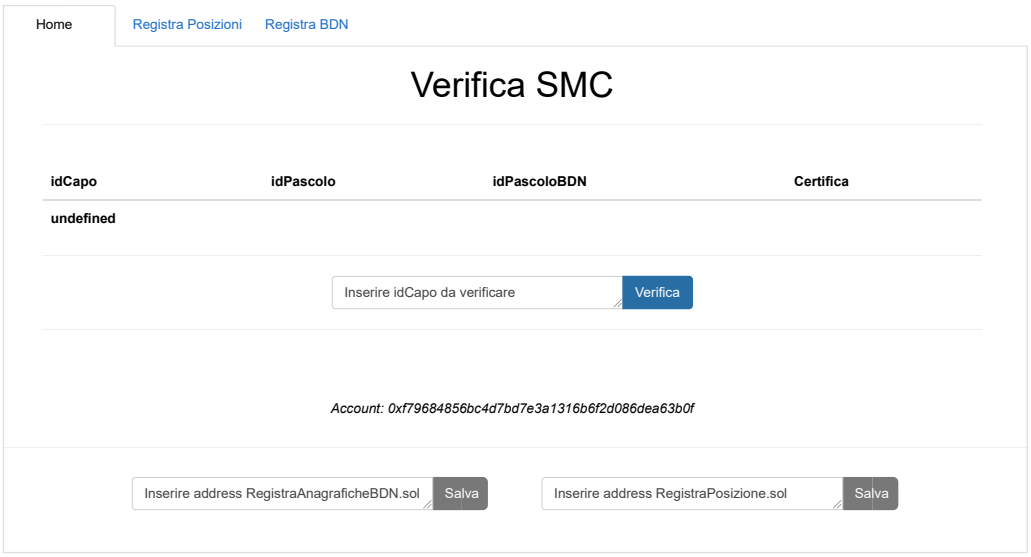

Figura 6.1. Schermata *Home* della dApp

Regista BDN, designate rispettivamente per la simulazione del salvataggio dei dati di posizione e le altre informazioni della BDN nella blockchain di riferimento. Entrambe le pagine hanno una struttura simile, sono composte da una tabella che mostra tutti gli elementi salvati nelle mappe dei rispettivi smart contract di riferimento, un'area dove è presente un bottone per la simulazione di ricezione dati e un'area di input, dove, attraverso la selezione di file, è possibile inoltrare le richieste di transazione per popolare gli smart contract. In particolare queste richieste, se effettuate attraverso un unico file con più informazioni da salvare vengono scatenate in successione, poichè il salvataggio è gestito in modo da provocare n transazioni per salvare le informazioni di n capi. Il pulsante per la simulazione presente nell'interfaccia, se premuto, avvia a tutti gli effetti una riproduzione di come il sistema front-end si comporterebbe alla ricezione di nuove informazioni provenienti in automatico dai collari e salvate in Blockchain. Con questa simulazione, quindi, si vuole evidenziare e riprodurre il flusso di interazioni e di dati che si genera all'arrivo di nuove informazioni, in modo da ricreare un funzionamento il più possibile veritiero e simile alla ricezione automatica dei dati, che in questa fase implementativa non è ancora stata analizzata in dettaglio.

6.3.2 Back-end

Il back-end dell'applicazione realizzata è rappresentato dall'insieme di smart contract e servizi circostanti presentati nelle Sezioni precedenti (Sez.6.1 e Sez.6.2).

L'interazione tra le due componenti dell'applicazione, il front-end e il back-end è reso possibile dalla libreria *web3.js*, la quale consente di elaborare le diverse richieste dell'untente ricevute dal front-end dell'applicazione. Le diverse componenti, descritte nella Sezione 6.3.1 precedente, interagiscono ognuna con uno smart contract, in modo da mantenere a livello architetturale netta separazione tra esse.
Come si può notare nel frammento di codice sottostante, la connessione tra front-end e back-end necessitano della definizione e inizializzazione di oggetti JavaScript che rappresentino lo smart contract di riferimento.

```
1  initWeb3: function() {
2    if (typeof web3 !== 'undefined') {
3      // Se l'istanza e'  gia' fornita da MetaMask
4      App.web3Provider = web3.currentProvider;
5      web3 = new Web3(web3.currentProvider);
6    } else {
7      // Specifica l'istanza di default se non viene fornita alcuna
           istanza web3
8      App.web3Provider = new Web3.providers.HttpProvider('http://
         localhost:7545');
9      web3 = new Web3(App.web3Provider);
10   }
11   return App.initContract();
12 },
13
14 initContract: function() {
15   $.getJSON("VerificaPosizioni.json", function(verPos) {
16     // Istanzia un nuovo contratto di Truffle
17     App.contracts.VerificaPosizioni = TruffleContract(verPos);
18     // Collega il provider per interagire con il contratto
19     App.contracts.VerificaPosizioni.setProvider(App.web3Provider)
         ;
20     return App.render();
21   });
22 }
```

Nell'esempio è riportata la creazione dell'oggetto JavaScript dello smart contract per la verifica. Quindi, si può notare come sfruttando la libreria *web3.js* è possibile creare, in modo semplice e diretto, connessione tra front-end e back-end dell'applicazione.

Capitolo 7

Conclusioni

In quest'ultimo capitolo si vogliono dare delle risposte alle domande della ricerca, mettere in evidenza i risultati ottenuti e le implicazioni generate durante l'intero processo di ricerca. Alla fine del capitolo saranno presentati anche i potenziali sviluppi futuri.

Nelle prime fasi è stata condotta un'estesa ricerca su una tecnologia relativamente nuova per comprendere a pieno le funzionalità e le potenzialità della Blockchain. Il campo di interesse è partito dalla Blockchain come tecnologia rivoluzionaria in molti settori, per arrivare poi alla FVC e ai relativi sistemi IoT necessari, in modo da poter fondere il tutto in un'unica soluzione trasversale lungo tutta la filiera alimentare, come previsto dal progetto di appartenenza PININ. Ci si è quindi concentrati sulla parte iniziale di quest'ultima, andando a proporre una soluzione per la tracciabilità e l'erogazione dei fondi europei destinati all'allevamento, non dimenticando, però, in fase progettuale, di proporre una soluzione orientata alla scalabilità.
Concentrarsi su tecnologie come IoT e Blockchain e come possano coesistere ed interagire contribuisce ad approfondire la conoscenza delle stesse e può favorire ciò che questa soluzione innovativa può fornire per migliorare e garantire qualità dei prodotti e sicurezza lungo la filiera.

Questo lavoro di tesi nasce, come già ampiamente descritto precedentemente, dalla necessità di dare forma e implementazione ad uno dei quattro casi dimostrativi del progetto PININ.
In tal senso, il caso d'uso analizzato, la tracciabilità dei fondi europei per il pascolo di bestiame, ha permesso di mettere in luce la fattibilità implementativa di una soluzione al grande problema delle frodi legate all'erogazione dei fondi Europei. La soluzione trovata per il particolare dettaglio di caso d'uso, come la registrazione e la verifica delle informazioni provenienti dai collari dei capi al pascolo, è risultata essere innovativa, adattabile a tutto il dimostratore e integrabile nella soluzione proposta per l'intero progetto PININ. L'architettura pensata, dove si è

voluta mantenere una netta separazione tra le varie componenti, ha mostrato come in un secondo momento e con l'aggiunta di un livello astrattivo sia facilmente adattabile e scalabile a tutto il flusso dei dati del caso d'uso. Con il sistema così pensato e con le molteplici relazioni tra le informazioni di tracciatura dei capi, dei pascoli e delle particelle di monticazione, è possibile effettuare controlli sia in un'ottica di verifica delle contribuzioni sia in merito all'uso della tracciabilità dei prodotti bovini e caseari nella filiera successiva. In questo specifico lavoro sono state considerate solo la tracciabilità e la verifica delle contribuzioni.
Gli smart contract realizzati, sono frutto di un'attenta riflessione sui consumi di gas generati con la loro interazione. I servizi esterni che svolgono il ruolo di oracolo, hanno una struttura del tutto in linea con quelle che sono le caratteristiche intrinseche della tecnologia adottata. L'applicazione decentralizzata sfruttando la libreria *web3.js*, infine, facilita l'interazione con gli smart contract, semplificando e riducendo il tutto ad una verifica di informazioni comune.
Inoltre, è importante sottolineare come questa soluzione proposta, per la tracciabilità dei fondi, sia del tutto innovativa nel settore, in quanto la verifica e la tracciabilità del prodotto stesso parte da una trasparenza e un'onestà aziendale che ne aumentano il valore.

7.1 Sviluppi futuri

Gli sviluppi futuri relativi al caso presentato possono essere molteplici. Partendo dallo stato attuale dell'applicazione in primo luogo bisogna delineare con precisione le interazioni con i diversi dati e stabilirne le funzioni e le modalità di funzionamento, per poi inoltrarsi in uno sviluppo di più ampie vedute e prospettive per l'intero progetto. Proprio in quest'ottica, il più importante è quello di portare il sistema progettato lungo tutto il flusso dati del caso di riferimento, per poi avere una soluzione che può integrarsi a tutti gli effetti con il progetto PININ di riferimento, dove la tracciabilità del prodotto è la chiave di volta. Questo processo è avvantaggiato dall'architettura pensata.
Un ulteriore sviluppo futuro, strettamente legato alle fasi di progetto sarà l'implementazione di un'unica soluzione per l'intero progetto PININ, andando ad unire i differenti casi dimostrativi sperimentati singolarmente.
Molto interessante può essere anche l'ampliamento di questa soluzione con l'introduzione dei *token*. L'inserimento nel sistema di quest'ultimi può risultare molto interessante soprattutto proprio per la gestione stessa dell'erogazione dei fondi, dove il richiedente con questo gettone può più facilmente dimostrare autenticità e onestà aziendale. La possibile erogazione potrebbe avvenire in base ad un eventuale graduatoria stipulata proprio in base al possesso dei token ricevuti e in relazione all'onestà dimostrata negli anni precedenti.

Lo studio della Blockchain è in continua evoluzione, il che implica la necessità di seguire con estrema attenzione le nuove scoperte che possono essere adatte in materia di tracciabilità lungo la catena alimentare e nell'erogazione dei fondi legati alle prime fasi di produzione.

Bibliografia

[1] Satoshi Nagamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf, 2008.

[2] T. Laurence, *Blockchain for Dummies*, John Wiley & Sons, May 2017, ISBN 978-1119365594.

[3] R. Wu, X. Zhang, M. Wang, L. Wang, *A High-Performance Parallel Hardware Architecture of SHA-256 Hash in ASIC*, IEEE, 2020 22nd International Conference on Advanced Communication Technology (ICACT), 2020, pp. 1242–1247.

[4] A.M. Antonopoulos, G. Wood, *Mastering ethereum: building smart contracts and dapps*, O'reilly Media, ISBN 978-1491971949, 2018.

[5] A.M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchains*, O'reilly Media, ISBN 978-1491954386, 2017.

[6] I. Bashir, *Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks*, Packt, ISBN 978-1787125445, 2017.

[7] I. Bashir, *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition*, Packt, ISBN 978-1788839044, 2018.

[8] J . Kothari, *Cryptography and its Types*, GeeksforGeeks, https://www.geeksforgeeks.org/cryptography-and-its-types/

[9] F. Provenzani, *Cos'è il Proof Of Work (PoW) e Proof Of Stake (PoS)?*, https://www.money.it/Cos-e-la-Proof-Of-Work-PoW-e-Proof-of-Stake, 2019.

[10] F. Provenzani, *Proof of Work vs. Proof of Stake*, https://blog.xsolus.com/proof-of-work-vs-proof-of-stake, 2018.

[11] M. Thibodeau, *3 Types of Blockchain Explained*, https://hedgetrade.com/3-types-of-blockchain-explained/, 2019.

[12] *Private, Public, and Consortium Blockchains - What's the Difference?*, https://www.binance.vision/blockchain/private-public-and-consortium-blockchains-whats-the-difference.

[13] D. Massessi, *Public Vs Private Blockchain In A Nutshell*, https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f, 2018.

[14] G. Mikhelidze, *La regolamentazione crypto nei Paesi post-sovietici*, https://cryptonomist.ch/2020/04/25/la-regolamentazione-crypto-paesi-sovietici/, 2020.

[15] G. Chiap, J. Ranalli, R. Bianchi, *Blockchain. Tecnologia e applicazioni per il business: tutto ciò che serve per entrare nella nuova rivoluzione digitale*, Hoepli, ISBN 978-8820390075, 2019.

[16] Comunicato stampa CE, *L'Unione europea è al primo posto del commercio agroalimentare mondiale*, Commissione Europea, https://ec.europa.eu/commission/presscorner/detail/it/ip_19_5527, 2019.

[17] D. Neven, *Developing Sustainable Food Value Chains: Guiding Principles*, Food and Agriculture Organization of the United Nations (FAO), E-ISBN 978-9251084823, 2014.

[18] H. Nguyen, L. Do, *The adoption of blockchain in food retail supply chain*, Lathi University of Applied Science, 2018.

[19] A. Diamond, D. Tropp, J. Barham, M.F. Muldoon, S. Kiraly, *Food Value Chains: Creating Shared Value To Enhance Marketing Success*, United States Department Of Agriculture, Agricultural Marketing Service, http://dx.doi.org/10.9752/MS141.05-2014, 2014.

[20] M. Pavesi, *Smart Agrifood: Boom dell'agricoltura 4.0*, Osservatori.net, https://www.osservatori.net/it_it/osservatori/comunicati-stampa/smart-agrifood-boom-agricoltura-4.0, 2019.

[21] A. Giordano, *Blockchain per l'agrifood. Scenari, applicazioni, impatti*, I quaderni di RuralHack, Societing4.0-Accademia di Management Mediterraneo, http://www.ruralhack.org/wp-content/uploads/2019/05/Blockchain-per-lagrifood..pdf, 2019.

[22] M. Pavesi, *L'agroalimentare è sempre più digitale: l'agricoltura 4.0 vale 450 mln di euro (+22%)*, Osservatori.net, https://www.osservatori.net/it_it/osservatori/comunicati-stampa/agricoltura-4-0-valore-crescita-tecnologie-startup, 2020.

[23] World Health Organization, *Food Safety*, WHO-Newsroom, https://www.who.int/news-room/fact-sheets/detail/food-safety#: :text=An%20estimated%20600%20million%20%E2%80%93%20almost,healthy%20life%20years%20(DALYs)., 2020.

[24] J. Duan, C. Zhang, Y. Gong, S. Brown, Z. Li, *A content-analysis based literature review in blockchain adoption within food supply chain*, International Journal of Environmental Research and Public Health, https://doi.org/10.3390/ijerph17051784, 2020.

[25] Commissione Europea, *Reg. (CE) n. 1760/2000 del 17 luglio 2000*, Regolamento del Parlamento europeo e del Consiglio, http://www.pianidisettore.it/flex/cm/pages/ServeAttachment.php/L/IT/D/

e%252Fa%252Ff%252FD.ac351e8ba44cd14a34e4/P/BLOB%3AID%3D617, 2000.

[26] F. Sander, J. Semeijn, D. Mahr, *The acceptance of blockchain technology in meat traceability and transparency*, British Food Journal, Vol.120, No. 9, pp. 2066-2079, https://doi.org/10.1108/BFJ-07-2017-0365, 2018.

[27] C. De Angelis, G.C. Elmo, R. Fondacaro, M. Risso, *L'impiego della tecnologia blockchain nella filiera agroalimentare: opportunità e sfide*, IDENTITÀ, INNOVAZIONE E IMPATTO DELL'AZIENDALISMO ITALIANO. Dentro l'economia digitale - Atti del XXXIX convegno nazionale accademia italiana di economia aziendale, pp. 749-757, https://www.collane.unito.it/oa/items/show/34#?c=0&m=0&s=0&cv=0, 2019.

[28] H. Treiblmaier, *The impact of the blockchain on the supply chain: a theory-based research framework and a call for action*, Supply Chain Management, Vol. 23 No. 6, pp. 545-559., https://doi.org/10.1108/SCM-01-2018-0029, 2018.

[29] B. Tan, J. Yan, S. Chen, X. Liu, *The Impact of Blockchain on Food Supply Chain: The Case of Walmart*, Springer Cham, Qiu M. (eds) Smart Blockchain. SmartBlock 2018. Lecture Notes in Computer Science, Vol. 11373, https://doi.org/10.1007/978-3-030-05764-0_18, 2018.

[30] A. Hughes, A. Park, J. Kietzman, C. Brown, *Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms*, Business Horizons, Vol. 62, Issue 3, pp. 273-281, https://doi.org/10.1016/j.bushor.2019.01.002, 2019.

[31] R. Accorsi, S. Cholette, R. Manzini, A. Tufano, *A hierarchical data architecture for sustainable food supply chain management and planning*, Journal of Cleaner Production, Vol. 203, pp. 1039-1054, https://doi.org/10.1016/j.jclepro.2018.08.275, 2018.

[32] A. Bechini, M.G.C.A. Cimino. F. Marcelloni, A. Tomasi, *Patterns and technologies for enabling supply chain traceability through collaborative e-business*, Information and Software Technology, Vol. 50, Issue 4, pp. 342-359, https://doi.org/10.1016/j.infsof.2007.02.017, 2008.

[33] F. Tian, *An agri-food supply chain traceability system for China based on RFID blockchain technology*, 13th International Conference on Service Systems and Service Management (ICSSSM), pp. 1-6, https://doi.org/10.1109/ICSSSM.2016.7538424, 2016.

[34] X. Gu, Y. Chai, Y. Liu, J. Shen, Y. Huang, Y. Nan, *A MCIN-based architecture of smart agriculture*, International Journal of Crowd Science 1, pp. 237-248, https://doi.org/10.1108/IJCS-08-2017-0017, 2017.

[35] K. Karandeep, *The Agriculture Internet of Things: A review of the concepts and implications of implementation*, International Journal of

Recent Trends in Engineering & Research (IJRTER), pp. 237-248, https://doi.org/10.1108/IJCS-08-2017-0017, 2016.

[36] S.M. Mahammad, P. Viswanathan *A Survey: Smart agriculture IoT with cloud computing*, IEEE, 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), https://doi.org/10.1109/ICMDCS.2017.8211551, 2017.

[37] J. Lin, Z. Shen, C. Miao, S. Liu, *Using blockchain to build trusted LoRaWAN sharing server*, Emerald Publishing Limited, International Journal of Crowd Science, Vol. 1, No. 3, pp. 270-280. https://doi.org/10.1108/IJCS-08-2017-0010, 2017.

[38] R.Ö. Kazım, Y. Arda, *Work-in-Progress: Integrating Low-Power IoT devices to a Blockchain-Based Infrastructure*, EMSOFT'17 Companion, https://doi.org/10.1145/3125503.3125628, 2017.

[39] J. Lin, Z. Shen, A. Zhang, Y. Chai, *Blockchain and IoT based Food Traceability for Smart Agriculture*, ICCSE'18: Proceedings of the 3rd International Conference on Crowd Science and Engineering, No. 3, pp. 1-6. https://doi.org/10.1145/3265689.3265692, 2018.

[40] Y. Lin, J. R. Petway, J. Anthony, H. Mukhtar, S. Liao, C. Chou Orcid, Y Ho, *Blockchain: The Evolutionary Next Step for ICT E-Agriculture*, ICCSE'18: Proceedings of the 3rd International Conference on Crowd Science and Engineering, Vol. 4, Issue 3, https://doi.org/10.3390/environments4030050, 2017.

[41] N. Zinas, S. Kontogiannis, G. Kokkonis, S. Valsamidis, I. Kazanidis, *Proposed open source architecture for Long Range monitoring. The case study of cattle tracking at Pogoniani*,Association for Computing Machinery, PCI 2017: Proceedings of the 21st Pan-Hellenic Conference on Informatics, No. 57, pp. 1-6, https://doi.org/10.1145/3139367.3139437, 2017.

[42] L. Leme, A. Medeiros, G. Srivastava, J. Crichigno, R. Filho, *Secure Cattle Stock Infrastructure for the Internet of Things using Blockchain*, 43rd International Conference on Telecommunications and Signal Processing (TSP 2020), http://ce.sc.edu/cyberinfra/docs/publications/Cattle_Blockchain_Paper[9763].pdf, 2020.

[43] A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, *A decentralized privacy-preserving healthcare blockchain for IoT*, Sensors, Vol. 19, No. 2, pp. 326, https://doi.org/10.3390/s19020326, 2019.

[44] G. Srivastava, A. D. Dwivedi, R. Singh, *Crypto-democracy: A decentralized voting scheme using blockchain technology*, Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018), Vol. 2, pp. 508-513, https://doi.org/10.5220/0006881906740679, 2018.

[45] Regione Piemonte, *S3 Strategia di specializzazione intelligente*, https://www.regione.piemonte.it/web/temi/sviluppo/sistema-ricerca-innovazione/s3-strategia-specializzazione-intelligente,

2016.

[46] Commissione Europea, *Smart Specialization Platform*, https://s3platform.jrc.ec.europa.eu, 2014.

[47] F. Cena, G. Boella, A. Cordero, A. Guffanti, A. Rapp, C. Schifanella, S. Ambrosini, P. Gay, C. Tortia, P. Barge, L. Comba, A. Biglia, *Blockchain and Artificial Intelligence for quality food protection and advanced consumer services*, I-cities 2019, 5th Italian Conference on ICT for Smart Cities And Communities, http://hdl.handle.net/2318/1727957, 2019.

Ringraziamenti