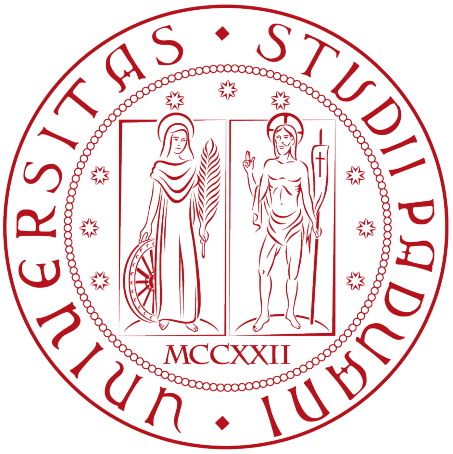
Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea in Informatica



Titolo della tesi

Tesi di laurea

Relatore

Prof. Tullio Vardanega

Laureando

Pietro Lauriola

Anno Accademico 2022-2023

Sommario

Il presente documento descrive il lavoro svolto durante il periodo di stage, della durata di trecentoventi (320) ore, dal laureando Pietro Lauriola presso l'azienda Sync Lab S.r.l. Gli obbiettivi da raggiungere erano i seguenti:
In primo luogo era richiesto la stesura di uno Studio di fattibilità circa la possibilità di utilizzare la Zero Knowledge Proof per sviluppare una piattaforma di voto verificabile ma anonima, ovvero che raccolga le votazioni degli utenti approvati senza che sia possibile risalire a cosa abbiano votato ma rendendo facile la verifica del fatto che abbiano effettivamente votato. In secondo luogo era richiesta l'implementazione di un Proof of Concept (PoC) per dimostrare la fattibilità del progetto.

"And yet I smile"
— Ezekiel

Ringraziamenti

Padova, Settembre 2023 Pietro Lauriola

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Contesto aziendale

In questo capitolo presento il contesto organizzativo e produttivo dell'azienda *SyncLab S.r.L.*. Viene fornita una descrizione di ciò che ho potuto osservare riguardo le tecnologie utilizzate, i processi interni dell'azienda, il tipo di clientela e la propensione dell'azienda per l'innovazione.

1.1 L'azienda

L'azienda ospitante è stata ***SyncLab S.r.L.***, nata nel 2002 a Napoli e attiva nel settore dell' *Information and Communication Technology* (ITC). Con il passare degli anni si è espansa aprendo in tutto 6 sedi in Italia, a Napoli, Roma, Milano, Padova, Verona e Como.

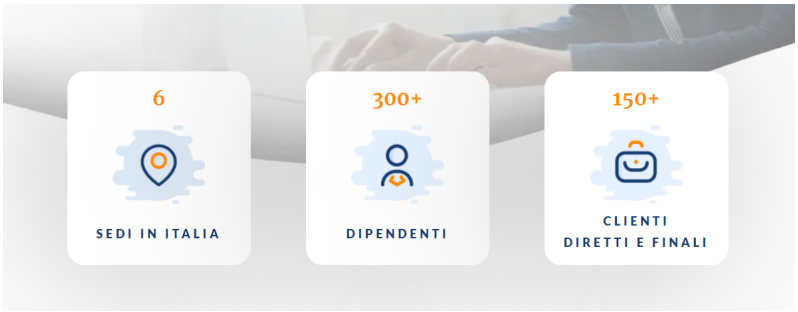


Figura 1.1: Dati relativi all'azienda
Fonte: synclab.it

Grazie a una struttura interna che favorisce la collaborazione, l'interazione non si limita ai colleghi della stessa sede, ma si estende globalmente in tutta l'azienda.

Lo scopo è quello di promuovere lo scambio di conoscenze all'interno dell'organizzazione e creare un ambiente in cui il progresso personale non sia il risultato esclusivo degli sforzi individuali, ma anche della collaborazione attiva tra i membri del *team*.

È rilevante sottolineare che ho notato che i dipendenti presenti, almeno nella sede di Padova, sono principalmente giovani.

*SyncLab S.r.L.*è identificabile come *System Integrator*, sebbene sia nata come una *Software House*. La differenza tra i due ambiti è rilevante per comprendere il modus operandi dell'azienda.

Software House: un'azienda che sviluppa internamente delle soluzioni software che soddisfino una certa opportunità di mercato, e offre i propri prodotti ai clienti interessati.

System Integrator: un'azienda che, contattata da aziende esterne, effettua manutenzione e evoluzione delle funzionalità di prodotti *software* già sviluppati e in uso.

Si tratta quindi di due approcci allo sviluppo ben diversi : mentre una *Software House* si concentra sulla creazione e sviluppo di soluzioni *software* innovative da zero, basandosi sulle esigenze e opportunità del mercato, un *System Integrator* si focalizza sull'ottimizzazione, l'integrazione e la manutenzione di software esistenti in base alle esigenze dei clienti che già utilizzano tali prodotti.

1.2 Settori di attività e progetti

*SyncLab S.r.L.*collabora con numerosi clienti, che operano in diversi ambiti, tra cui: *EHealt, Telco, Web and Mobile, Data Management, Blockchain, Maritime.*

Figura 1.2: Alcuni ambiti in cui l'azienda opera
Fonte: synclab.it

Dopo aver discusso degli attuali ambiti di operatività di *SyncLab*, è interessante fare un salto indietro e analizzare le radici dell'azienda.

Quando *SyncLab* operava come *Software House*, ha creato una serie di prodotti e soluzioni innovative che hanno contribuito a definire il suo prestigio nel settore *IT*. Prodotti e soluzioni che non solo hanno consolidato la sua posizione nel mercato, ma hanno anche gettato le basi per la sua evoluzione futura.

Vediamo alcuni dei progetti più rappresentativi e influenti realizzati da *SyncLab* in quella fase cruciale della sua storia.

- **SynClinic**: Una soluzione nel settore dell'*EHealth* progettata per centralizzare e facilitare la gestione sia clinica che amministrativa di ospedali, strutture sanitarie e residenze mediche.

  Il suo obiettivo principale è assistere il personale sanitario nell'identificazione e nella gestione del rischio clinico, garantendo al contempo un'ottima tracciabilità e organizzazione delle varie tappe del trattamento del paziente.

- **SeaStream**: Questa piattaforma è stata progettata per potenziare l'efficienza, la sicurezza e incoraggiare l'innovazione nel dominio marittimo.
  SeaStream presenta un *Fleet Operation Center* (FOC) che offre una sorveglianza avanzata delle flotte navali in operazione globalmente.
  Inoltre, mette a disposizione una *Harbor Operation Platform* (HOC), che fornisce una gamma completa di servizi destinati ai professionisti del settore portuale.
- **Fast Reservation**: Una piattaforma digitale ideata per la gestione delle prenotazioni, adattabile a diverse realtà come stabilimenti balneari, parchi e attività nel settore della ristorazione. L'obiettivo è rendere il processo di prenotazione fluido e intuitivo per gli utenti.
- **Sobereye**: Una soluzione basata sul *web* progettata per analizzare e monitorare lo stato psicofisico di una persona mediante l'osservazione della pupilla. Questa applicazione è particolarmente utile per identificare alterazioni potenzialmente causate da stanchezza eccessiva o assunzione di sostanze come alcool e droghe, contribuendo a ridurre potenziali rischi sul luogo di lavoro.

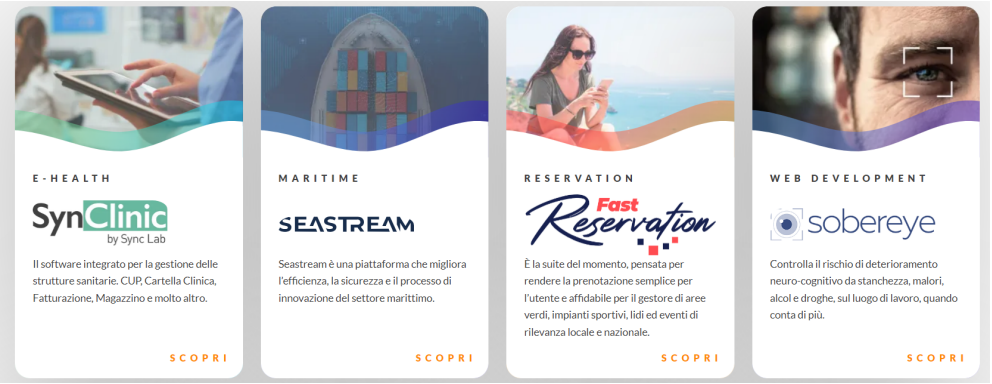


Figura 1.3: Alcuni progetti sviluppati dall'azienda
Fonte: synclab.it

1.3 Way of working

1.3.1 Gestione dello smart working

Durante il percorso di tirocinio, sebbene la sede dell'azienda fosse a Padova, ho svolto la maggior parte del lavoro da remoto. L'azienda adotta un metodo di lavoro che consiste nel trovarsi in sede circa una volta a settimana per confrontarsi sul lavoro svolto, sui progressi fatti e sulle difficoltà riscontrate.

Il restante del tempo lavorativo viene svolto in autonomia e, qualora ci si trovi in difficoltà, si possono utilizzare gli strumenti di comunicazione da remoto per risolvere dubbi o problemi.

1.3.2 Tecnologie interne

In questa sezione tratteremo alcune tecnologie di cui ho avuto esperienza diretta. Tuttavia, non procedo a fornire specifiche dettagliate riguardo al loro utilizzo interno

per la gestione del lavoro.

SyncLab utilizza un'ampia gamma di tecnologie, che includono linguaggi di programmazione e *framework* all'avanguardia nel settore dell'*Information and Communication Technology*.

L'azienda fa ampio uso di linguaggi di programmazione come **JavaScript, TypeScript, Java, Python, Solidity**.

Figura 1.4: Alcuni linguaggi di programmazione in uso da SyncLab

Solitamente questi linguaggi vengano affiancati da *framework*, che offrono un'infrastruttura predefinita per lo sviluppo di applicazioni. Questi *framework* facilitano la creazione di *software* efficiente e scalabile, fornendo librerie predefinite, strumenti di sviluppo e modelli architetturali. Grazie alla loro natura modulare e flessibile, i *framework* consentono ai programmatori di concentrarsi sull'implementazione delle funzionalità specifiche, migliorando la qualità del *software* sviluppato. Di seguito i principali *framework* utilizzati:

- **Angular**: *Framework* di sviluppo *front-end* basato su JavaScript. Offre una potente piattaforma per la creazione di applicazione *web* scalabili e reattive. Attualmente è una delle soluzioni più utilizzate nel settore.
- **Java Spring**: *Framework* di sviluppo *back-end* basato su Java. Fornisce una vasta gamma di moduli e funzionalità per la creazione di applicazioni Java robuste. Attualmente si è imposto come *standard de facto* per lo sviluppo di servizi *web* in Java.
- **Odoo**: *Framework open source* per lo sviluppo di applicazioni di gestione aziendale, basato in Python. Odoo è altamente personalizzabile e modulare grazie al vasto insieme di moduli offerti per la gestione delle vendite, degli acquisti, delle risorse umane, della contabilità e molti altri.

Figura 1.5: Alcuni framework in uso da SyncLab

Questa vasta gamma di tecnologie consentono di adattarsi alle esigenze specifiche dei clienti e offrire soluzioni *software* all'avanguardia che combinano efficienza, funzionalità e usabilità.

All'interno di un **gruppo di lavoro**, la normazione, regolamentazione e sincronizzazione delle attività sono fondamentali per garantire un flusso di lavoro efficiente ed efficace. A tal fine, l'utilizzo di *software* appositamente progettati volge un ruolo cruciale.

Di seguito alcuni *software* che svolgono questo ruolo:

- **Git**: Un **sistema di controllo di versione distribuito**, ampiamente adottato. Consente di tenere traccia delle modifiche apportate ai *file* e coordinare il lavoro

di più persone. Attraverso *Git*, i membri del gruppo possono collaborare in modo sincronizzato, gestire i conflitti, apportare modifiche senza sovrascrivere il lavoro degli altri e recuperare versioni precedenti dei *file*.

- **VS Code**: Un **ambiente di sviluppo integrato** (IDE) che offre un'interfaccia unificata per la scrittura del codice, la gestione dei *file* e la condivisione dei progetti. *VS Code* facilita la codifica collaborativa, fornendo strumenti per *debugging*, completamento del codice e integrazione con *Git*, agevolando la gestione e la tracciabilità delle modifiche al codice.

- **IntelliJ IDEA**: Un **ambiente di sviluppo integrato** (IDE) concepito primariamente per facilitare la programmazione in *Java*. Offre una vasta gamma di funzionalità destinate a assistere lo sviluppatore in ogni fase della codifica. Tra le caratteristiche più rilevanti, *IntelliJ IDEA* incorpora l'analisi statica del codice, permettendo di rilevare e segnalare errori sia logici che sintattici ancor prima dell'esecuzione del programma. Inoltre, si integra perfettamente con strumenti di versionamento esterni, come *Git*, agevolando la gestione e la tracciabilità delle modifiche al codice.

Figura 1.6: Alcuni software in uso da SyncLab

Nell'ambito della **comunicazione interna**, l'utilizzo di strumenti dedicati è essenziale per garantire una comunicazione efficace, per questo sono state individuate soluzioni come:

- **Discord**: Piattaforma di **comunicazione vocale e testuale**, ampiamente utilizzata e consente ai membri del gruppo di scambiare messaggi istantanei ed effettuare chiamate. *Discord* offre anche funzionalità aggiuntive, come la creazione di canali tematici per avere una comunicazione *topic based*.

- **Google Meet**: Piattaforma per **videoconferenze**, che permette di tenere riunioni *online*, condividendo schermi, documenti e presentazioni in tempo reale. Questo strumento è stato maggiormente usato durante e in seguito alla pandemia di SARS-CoV-2.

- **Google Calendar**: **Software gestionale** per la creazione di calendari privati e condivisi tra più utenti. Attraverso *Google Calendar* è possibile creare eventi, impostare promemoria e condividere le proprie disponibilità con gli altri membri. Viene anche utilizzato per organizzare l'alternanza tra *smart working* e lavoro in presenza.

- **Trello**: **Software gestionale** che adotta la filosofia Kanban, essendo ispirato alla metodologia della *Scrum board* tipica del modello agile. Permette di organizzare e tracciare il progresso dei lavori attraverso l'uso di schede specifiche, ciascuna associata a un determinato *task*. Questa strutturazione consente di avere una visione chiara e aggiornata dello stato dei progetti, e di facilitare la comunicazione e sincronizzazione tra i membri del *team* di sviluppo.

1.4 Dallo stack tecnologico ad applicativo

Nel vasto dominio dell'ingegneria del *software*, non si possono considerare le tecnologie in isolamento. Esse sono piuttosto dei pezzi che, messi insieme, costituiscono uno "*stack* tecnologico".
Questa integrazione ha particolare rilevanza quando ci si concentra sullo sviluppo di applicazioni *web*. Queste applicazioni, infatti, si articolano in due settori chiave: il *front-end*, focalizzato sull'esperienza e l'interfaccia utente, e il *back-end*, che gestisce la logica, la manipolazione dei dati e la loro persistenza.

Se dovessimo esemplificare utilizzando gli strumenti menzionati precedentemente:

- **Front-end**: La scelta potrebbe cadere su Angular come *framework*, concepito per creare interfacce *web* dinamiche. Questa scelta trascina con sé l'uso del linguaggio TypeScript e dell'HTML5. Sono tecnologie intrinsecamente collegate, funzionando in tandem per fornire l'esperienza desiderata.

- **Back-end**: In questo contesto, si potrebbe optare per Java Spring, ideale per elaborare logiche dati complesse, mentre la scelta del DBMS per la gestione dei dati potrebbe essere più flessibile e non direttamente vincolata dalla scelta del *framework*.

A queste tecnologie principali, si aggiungono strumenti che supportano il processo di sviluppo: IDE come IntelliJ IDEA per Java e VSCode per TypeScript; strumenti di versionamento come Git e soluzioni per la comunicazione e gestione di progetto, come Discord e Trello.

Questi *stack*, o insiemi di tecnologie, interagiscono tra loro, formando un mosaico tecnologico che costituisce lo scheletro di qualsiasi progetto.
L'immagine seguente offre una sintesi visuale delle tecnologie discusse, categorizzate per ambito di utilizzo.

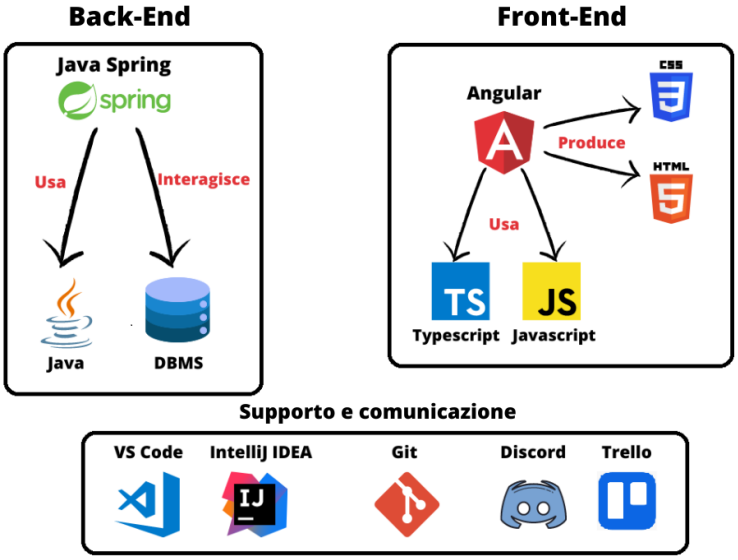


Figura 1.7: Esempio di *stack* tecnologico

Il punto cardine è che le tecnologie adottate da *SyncLab* (o qualsiasi *team* di sviluppo) devono essere viste come elementi di un ecosistema più ampio, con una visione orientata verso l'obiettivo finale piuttosto che sui dettagli specifici.

Vale la pena sottolineare che gli *stack* tecnologici proposti qui sono illustrativi. Sono modellati intorno alle tecnologie prevalenti in *SyncLab* e servono come esempi di come si potrebbero combinare diverse tecnologie. La scelta di uno *stack* non è prescrittiva; dipende da numerosi fattori e non è intenzione di questo lavoro prescrivere un approccio unico o limitante.

1.5 Propensione all'innovazione

L'azienda si distingue per la sua costante propensione all'innovazione, che costituisce uno dei pilastri fondamentali della sua filosofia aziendale.

L'arduo e persistente impegno di *SyncLab* nel perseguire l'innovazione è palpabile in ogni aspetto della sua attività. Questa dedizione si traduce in una incessante e meticolosa ricerca di metodologie all'avanguardia, tecnologie di ultima generazione e approcci rivoluzionari.

Vi è un dualismo, che emerge dalla filosofia di *SyncLab*:
Da un lato, vi è l'incessante impegno per affinare le dinamiche interne, dall'ottimizzazione della gestione dei progetti, al potenziamento delle relazioni con i clienti, dalla ricerca di una maggiore efficienza operativa alla dedizione nella formazione continua del suo *team*. Queste iniziative riflettono la passione dell'azienda per l'eccellenza in ogni aspetto della sua operatività.

Dall'altro lato, *SyncLab* non si limita a perfezionare l'infrastruttura interna. La sua visione trascende queste operazioni interne, rivolgendo lo sguardo verso il panorama esterno. L'obiettivo predominante è la creazione e proposizione di soluzioni di avanguardia, formulate per rispondere alle sfide crescenti e intricate del mercato attuale. Questi prodotti e servizi non sono semplicemente reattivi, ma anticipatori, mirando a generare un impatto significativo e a lungo termine nell'ecosistema tecnologico.

La visione pionieristica
Oltre a rispondere alle immediate necessità dei clienti, l'intento è di anticipare le tendenze future e posizionarsi come pionieri nel settore. La visione dell'azienda è chiara: migliorare costantemente sia l'infrastruttura interna sia le soluzioni offerte, assicurando che entrambe siano sempre all'avanguardia.

La mentalità aperta all'innovazione e la capacità di adattamento rappresentano quindi i *driver* fondamentali che guidano l'azienda nel suo percorso di crescita e successo nel panorama competitivo odierno.

Un esempio tangibile della visione avanguardista di *SyncLab* è la sua dedizione verso la tecnologia *blockchain*.

Questo impegno non si riflette solo in una mera scelta tecnologica, ma evidenzia un profondo desiderio dell'azienda di essere al passo con le innovazioni più pregnanti nel dominio *IT*.

La mia esperienza all'interno dell'azienda ha rivelato come *SyncLab* non solo riconosca l'importanza cardine della *blockchain*, allocando risorse significative per comprenderla in profondità, ma stia anche realizzando lavori concreti basati su questa tecnologia per conto di clienti che ne hanno riconosciuto il potenziale e ne hanno richiesto l'implementazione
Tali lavori, ancorati nella pratica e richiesti da clienti reali, mirano a sfruttare tutto il potenziale della *blockchain*.

L'obiettivo è doppio: da un lato, innovare e ottimizzare i processi esistenti, dall'altro, fornire nuove soluzioni che possano determinare una svolta nel panorama tecnologico attuale.

Questo approccio, che fonde analisi approfondita con applicazione diretta, dimostra la determinazione di *SyncLab* nel portare avanti l'innovazione.
L'azienda non si accontenta di stare al passo con le ultime tendenze, ma si posiziona attivamente come un agente di cambiamento, erogando servizi di alto valore ai suoi clienti.

Capitolo 2

Lo stage

2.1 Strategia aziendale

2.1.1 Offerte aziendali

SyncLab ha costruito una rete solida con istituti di istruzione. Queste collaborazioni si manifestano in diversi modi: oltre a partecipare attivamente a progetti proposti all'interno di specifici corsi di laurea, *SyncLab* è regolarmente presente e attiva in eventi accademici, come StageIT, sottolineando la sua dedizione nell'interazione diretta con la comunità accademica e gli studenti.

Figura 2.1: Partner accademici di Synclab
Fonte: synclab.it

Ma, in particolare, attraverso programmi di stage ben strutturati, l'azienda ha potuto trarre vantaggio dal flusso costante di nuove idee, conoscenze e competenze.

Sulla base della mia interazione diretta con l'azienda, ho identificato un aspetto saliente relativo alle loro offerte di stage: queste non sono unicamente intese come strumenti per la formazione e l'orientamento di potenziali professionisti. Invece, rappresentano anche un mezzo attraverso il quale l'azienda stessa mira ad acquisire nuove competenze e ad approfondire aree inesplorate del settore.

Questo approccio dimostra la visione olistica dell'azienda riguardo all'apprendimento e all'innovazione: un ciclo continuo in cui l'azienda impara dagli stagisti tanto

quanto gli stagisti imparano dall'azienda.

I programmi di stage offerti da *SyncLab* riflettono chiaramente la strategia aziendale di rimanere all'avanguardia nel panorama *IT*. Essi sono strutturati in base alle esigenze attuali dell'azienda e alle tendenze emergenti nel settore:

- **Sviluppo e Integrazione**: In questo ambito, gli stagisti hanno la responsabilità di perfezionare *software* preesistenti, lavorando su specifiche funzionalità atomiche. Sebbene queste funzionalità non siano destinate alla produzione finale, rappresentano, in alcuni casi, soluzioni alternative che l'azienda aveva precedentemente considerato.
  Gli stagisti, attraverso questo approccio, hanno l'opportunità di esplorare e sviluppare questi concetti, contribuendo a una comprensione più ampia delle potenzialità e delle alternative del *software* in questione.
- **Ricerca e Innovazione**: Questo percorso si focalizza sull'approfondimento teorico di tecnologie emergenti e concetti in evoluzione nel settore *IT*.
  Gli stagisti sono incaricati di condurre studi specifici, mirati a esplorare aspetti particolari e dettagliati delle nuove tecnologie, sempre in linea con le esigenze e gli obiettivi precisi dell'azienda.
  Questa immersione teorica fornisce una solida base per comprendere le nuove tendenze, valutare il loro potenziale e considerare possibili applicazioni pratiche nel contesto aziendale.
- **Analisi e Ottimizzazione**: Questa area si concentra sulla valutazione dettagliata delle soluzioni *software* correntemente in uso all'interno dell'azienda.
  Gli stagisti sono incaricati di esaminare questi sistemi, identificare possibili inefficienze o aree di miglioramento e proporre soluzioni ottimizzate.
  La chiave di questa fase è un approccio critico e analitico, che mira a garantire che il *software* dell'azienda funzioni al suo massimo potenziale, sfruttando al meglio le risorse disponibili e rispondendo in modo efficiente alle esigenze degli utenti.

2.1.2 Stage in azienda

Gli *stage* presso *SyncLab* sono quindi visti non solo come un'opportunità per identificare e formare futuri professionisti, ma anche come un canale per iniettare innovazione e nuove idee nel tessuto dell'organizzazione.

Questa visione dualistica sottolinea l'importanza strategica che l'azienda attribuisce all'integrazione di giovani nel suo ecosistema.

La partecipazione attiva degli stagisti ai progetti aziendali è centrale in questa prospettiva. L'azienda li coinvolge in attività che hanno un impatto diretto sugli esiti dei progetti, garantendo che le loro competenze e visioni vengano valorizzate e utilizzate per raggiungere gli obiettivi dell'organizzazione.

Inoltre, è da notare come l'esperienza di stage presso *SyncLab* spesso funga da trampolino di lancio per una carriera a lungo termine all'interno dell'organizzazione. Molti stagisti, avendo dimostrato valore e impegno, vengono poi assunti come membri effettivi del team, evidenziando la profondità e l'efficacia del programma di stage proposto.

Infine, è degno di nota come *SyncLab* non solo valorizzi individualmente ogni stagista, ma promuova anche l'interazione tra di loro.

Quando più stagisti lavorano su tematiche o aspetti correlati, l'azienda li mette attivamente in contatto, favorendo un ambiente collaborativo.

Questa strategia permette agli stagisti di condividere le proprie competenze, di aiutarsi reciprocamente e di arricchire ulteriormente la loro esperienza formativa.

Metti un'immagine tra i paragrafi!

2.1.3 Ruolo del tutor

Un aspetto fondamentale dell'esperienza di stage presso *SyncLab* è la presenza di un *tutor* personale che accompagna lo stagista lungo tutto il percorso. Questo *tutor* non è mai scelto a caso, ma è una figura esperta nel settore specifico in cui lo stagista opererà. La sua presenza è cruciale per guidare, consigliare e offrire *feedback* costruttivi basati sulla sua vasta esperienza.

Questa strategia dell'azienda assicura che ogni stagista sia supportato e guidato in maniera ottimale.

Nel mio caso specifico, a seguito della mia scelta specifica di stage, è stato assegnato *Matteo Galvagni* come mio *tutor*, proprio perché la sua esperienza era particolarmente in linea con il settore in cui avrei lavorato, ossia la *blockchain*.

Il *tutor*, oltre a fornirmi indicazioni e strumenti utili per velocizzare la comprensione e assimilazione delle conoscenze necessarie, ha giocato un ruolo fondamentale anche nella fornitura di *feedback*.

Un elemento distintivo dell'esperienza degli stagisti è proprio la frequenza e la qualità del *feedback* ricevuto. *SyncLab* si impegna a fornire valutazioni regolari e dettagliate, garantendo agli stagisti opportunità di crescita e sviluppo professionale coerenti con le esigenze aziendali.

2.2 Progetto proposto

2.2.1 Introduzione

Nell'era digitale, la ricerca di sistemi di votazione sicuri, trasparenti e al contempo garantisti della *privacy* è divenuta una priorità.
Il progetto intrapreso ha come scopo primario lo sviluppo di una piattaforma di votazione online che affronta **due sfide fondamentali**:

- Garantire l'anonimato totale degli elettori
- Garantire l'integrità inalterabile delle votazioni.

Per quanto riguarda la **prima sfida**, il sistema deve essere progettato per rendere il voto online completamente anonimo. Gli elettori devono poter partecipare alle votazioni senza rivelare la propria identità, garantendo così la massima *privacy*. Ciò si è supposto fosse possibile attraverso l'utilizzo di tecnologie di crittografia, in particolare la *Zero Knowledge Proof (ZKP)*. La *ZKP* può consentire agli elettori di dimostrare che hanno il diritto di votare senza rivelare chi sono o cosa hanno votato.

Per quanto riguarda la **seconda sfida**, la *blockchain* svolge un ruolo cruciale nel garantire l'integrità delle votazioni. La *blockchain* è una tecnologia distribuita che consente di registrare le votazioni in modo permanente e immutabile. Una volta che dei dati, nel nostro caso i voti, vengono registrati sulla *blockchain*, diventa impossibile modificarli o cancellarli senza lasciare traccia. Questo livello di sicurezza è fondamentale per garantire che le votazioni siano affidabili e immuni da frodi o manipolazioni.

Lo *stage* è finalizzato non solo a valutare la fattibilità di tale sistema ma anche a sviluppare un *Proof of Concept (PoC)* funzionante. Il *PoC* servirà a dimostrare concretamente che il sistema può essere implementato e che è in grado di garantire l'anonimato degli elettori e l'integrità delle votazioni.
In sintesi, il progetto mira a rivoluzionare il modo in cui il voto online è condotto, garantendo una maggiore *privacy* agli elettori e una maggiore sicurezza alle votazioni stesse attraverso l'uso combinato della *Zero Knowledge Proof* e della *blockchain*. La fase di sviluppo del *Proof of Concept* sarà cruciale per dimostrare l'efficacia di questo approccio innovativo e per gettare le basi per futuri sviluppi nel campo delle votazioni online.

2.2.2 Definizione Zero knowledge proof

Nell'ambito di questo progetto, la *Zero Knowledge Proof (ZKP)* svolge un ruolo di primaria importanza. Essa consente a una delle parti coinvolte, chiamata "*prover*," di dimostrare la veridicità di un'affermazione senza dover rivelare alcuna informazione specifica all'altra parte, nota come "*verifier*." Questa capacità di coniugare autenticità e riservatezza riveste un'importanza cruciale in contesti quali le transazioni *blockchain* e i sistemi di voto elettronico.

Per effettuare questa dimostrazione, viene generata una "prova" utilizzando complesse funzioni di crittografia. Questa "prova," che rappresenta il fulcro del concetto in una *ZKP*, è una rappresentazione crittograficamente robusta che il *prover* fornisce al *verifier* per dimostrare la veridicità di una determinata affermazione. La sua ge-

nerazione avviene in modo tale da risultare convincente, ma senza mai rivelare dati specifici.

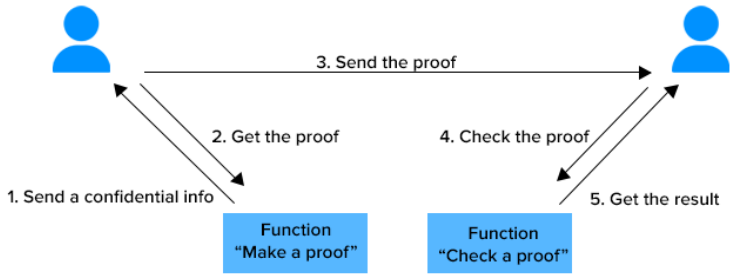


Figura 2.2: Generazione e controllo prova
Fonte: Medium

Per esempio, nel contesto delle elezioni elettroniche, un elettore (*prover*) può dimostrare che il proprio voto è stato registrato correttamente senza dover rivelare il contenuto effettivo del voto. Questa "prova" rappresenta l'evidenza crittografica che il voto è legittimo e corretto, ma non rivela cosa sia stato votato. Il sistema di verifica (*verifier*) può quindi confermare la validità del voto senza conoscere il suo contenuto, proteggendo così l'anonimato degli elettori e l'integrità dei risultati elettorali.

Oltre alle applicazioni nelle votazioni, la *ZKP* gioca un ruolo determinante nella protezione della *privacy* in transazioni *blockchain*. Ad esempio, gli utenti possono dimostrare la disponibilità di fondi sufficienti per una transazione senza dover specificare l'ammontare esatto dei loro averi. Questa "prova" crittografica consente agli utenti di effettuare transazioni in modo sicuro senza rivelare informazioni sensibili.

In conclusione, la *Zero Knowledge Proof* offre una soluzione avanzata per garantire sia la sicurezza che la *privacy* nelle transazioni digitali e nei processi di voto, grazie all'uso di "prove" crittografiche che dimostrano la veridicità senza la necessità di rivelare dati specifici.

2.3 Obiettivi

Nel contesto di qualsiasi progetto, definire obiettivi chiari rappresenta una fase cruciale. Senza obiettivi ben definiti, un progetto rischia di perdersi nell'incertezza, di deviare dalla sua finalità e di non produrre risultati concreti. Pertanto, nella realizzazione di questo progetto la determinazione di obiettivi ben definiti è stata un imperativo.
Di seguito, gli obiettivi specifici del progetto sono lo **studio di fattibilità e lo sviluppo del *Proof of Concept***, come di seguito:

Studio di Fattibilità: Condurre uno studio dettagliato sulla fattibilità dell'utilizzo della *Zero Knowledge Proof (ZKP)* per garantire la *privacy* nelle votazioni elettroniche. Questa analisi ha un focus particolare su due componenti fondamentali: la tecnologia *blockchain* e la *ZKP*.

Per quanto riguarda la tecnologia *blockchain*, si esaminano le diverse piattaforme e protocolli disponibili per determinare quale sia più adatta al contesto delle votazioni elettroniche. Questo include l'analisi di varie *blockchain*, nonché considerazioni sulla scalabilità e sulla sicurezza.

Per quanto riguarda la *Zero Knowledge Proof (ZKP)*, vengono esplorate le diverse varianti e implementazioni di questa tecnologia crittografica. Inoltre, vengono valutate le loro applicazioni potenziali nel contesto delle votazioni elettroniche, identificando le loro capacità e le eventuali limitazioni.

Lo studio di fattibilità ha quindi l'obiettivo di fornire una panoramica chiara delle strade possibili per l'implementazione della *ZKP* nelle votazioni elettroniche. Così da concentrarci sulle soluzioni tecniche più promettenti e identificare le sfide chiave da affrontare durante lo sviluppo del *Proof of Concept (PoC)*.

Sviluppo di un *Proof of Concept (PoC)*: Il *Proof of Concept (PoC)* è un'implementazione pratica e limitata della *Zero Knowledge Proof (ZKP)* all'interno della piattaforma di voto elettronico. Il suo scopo principale è dimostrare che la *ZKP* può essere applicata con successo per garantire l'anonimato degli elettori e la sicurezza delle votazioni elettroniche.

In questa fase, ci concentriamo sull'implementazione dei concetti teorici relativi alla *ZKP* in un ambiente controllato. Il *PoC* funge da prototipo iniziale e dimostra come un elettore può votare in modo anonimo e come il sistema può verificare l'autenticità dei voti senza rivelare i dettagli specifici del voto.

I risultati del *PoC* influenzeranno le eventuali fasi successive del progetto, guidando le decisioni riguardo all'implementazione su larga scala della piattaforma di voto basata sulla *ZKP*.

2.4 Vincoli

Nel contesto di qualsiasi progetto, è fondamentale considerare attentamente i vincoli che possono influenzare la sua realizzazione. I vincoli definiscono le restrizioni e le limitazioni che devono essere prese in considerazione per garantire il successo del progetto. Nel caso specifico della piattaforma di voto, sono presenti diversi vincoli che devono essere affrontati per garantire la riservatezza, l'integrità e la verificabilità del processo di voto.

- **Vincolo di riservatezza**
  Il sistema deve garantire che, sebbene ogni voto possa essere verificato come legittimo, l'identità dell'elettore e la sua scelta specifica rimangano completamente anonime. In altre parole, è fondamentale che sia impossibile determinare cosa ha votato un singolo utente

- **Vincolo di unicità del voto**
  Ogni indirizzo utilizzato per votare è considerato come un'entità unica nel sistema. Pertanto, è essenziale che un utente non possa esprimere più di un voto utilizzando lo stesso indirizzo.

- **Vincolo di integrità del voto**
  La *blockchain*, per sua natura, è una struttura dati immutabile. Questo vincolo è fondamentale per garantire l'integrità del sistema di votazione. Non deve essere possibile, in nessun caso, modificare i voti una volta che questi sono stati registrati. Questo assicura che non sia possibile alterare il voto di altri utenti, garantendo che ogni voto conteggiato sia effettivamente quello espresso dall'elettore.

- **Vincolo di verificabilità**
  Chiunque deve poter verificare che i voti siano validi e il conteggio corretto. La piattaforma di voto deve fornire un meccanismo di verifica che consenta agli utenti di accedere ai risultati del voto in modo trasparente e affidabile. Questo viene realizzato attraverso l'utilizzo della *blockchain*, che permette la registrazione pubblica e immutabile dei voti, e l'utilizzo di algoritmi crittografici per garantire l'integrità dei dati.

Affrontare questi vincoli è fondamentale per creare una piattaforma di voto sicura, affidabile e trasparente. La considerazione di questi vincoli durante tutto il processo di sviluppo e implementazione del progetto garantisce che la piattaforma soddisfi le esigenze di *privacy* degli elettori, l'integrità del processo di voto e la verificabilità dei risultati.

2.5 Motivazione della scelta

Ho conosciuto l'azienda tramite l'evento STAGE-IT 2023, un'iniziativa promossa da Confindustria Veneto Est in collaborazione con i Dipartimenti di Matematica e Scienze Statistiche dell'Università di Padova, a cui ha partecipato anche il Dipartimento di Ingegneria Informatica. Durante l'evento, ho avuto l'opportunità di entrare in contatto con diverse aziende che proponevano progetti innovativi nel campo dell'*IT*. Sebbene vi fossero molteplici opportunità offerte da diverse aziende, la proposta di *Synclab* ha suscitato un interesse particolare in me.

Oltre alla mia conoscenza dell'azienda tramite STAGE-IT, ci sono state altre ragioni che mi hanno spinto a scegliere questo progetto, che possiamo riassumere nei seguenti punti:

- **Acquisire Competenze in *Blockchain***: ho visto questa opportunità come un modo per acquisire competenze specifiche nel campo della *blockchain*. La tecnologia *blockchain* è in continua crescita e sta diventando sempre più rilevante in diversi settori.
  L'opportunità di lavorare direttamente con questa tecnologia e di comprendere i suoi meccanismi interni rappresentava una proposta troppo allettante per essere ignorata.

- **Acquisire Competenze in *Smart Contracts***: Ancorato al mondo della *blockchain*, lo sviluppo e l'implementazione di *smart contracts* rappresenta una delle aree di maggiore crescita e innovazione. Gli *smart contract* sono programmi autonomi che eseguono automaticamente le condizioni stabilite al loro interno.
  Acquisire competenze in questo settore non solo avrebbe arricchito il mio bagaglio tecnico, ma avrebbe anche fornito uno sguardo sul futuro della tecnologia.

- **Osservare Direttamente il Lavoro in Azienda**: La teoria e la pratica sono due facce della stessa medaglia. L'opportunità di osservare e partecipare

attivamente alla vita quotidiana di un'azienda *software* avrebbe garantito una visione pratica e applicata delle mie conoscenze teoriche. È stata un'opportunità per imparare da professionisti del settore e per sviluppare competenze trasversali, come la gestione del tempo, la collaborazione e la comunicazione efficace

- **Possibilità di Proseguire il Lavoro in Azienda**: Al di là dell'esperienza immediata dello *stage*, la prospettiva di una possibile continuazione professionale con *Synclab* rappresentava un ulteriore incentivo. Lavorare su un progetto significativo con la possibilità di una futura collaborazione a lungo termine è stata un'ottima opportunità .

In conclusione, ho scelto di lavorare su questo progetto presso questa azienda perché mi ha colpito fin dal primo incontro durante STAGE-IT. Le opportunità di acquisire competenze *blockchain* e *smart contract*, l'esperienza diretta nel contesto aziendale e la possibilità di proseguire il lavoro in azienda sono state le principali motivazioni che mi hanno spinto a fare questa scelta.

Capitolo 3

Il progetto: Svolgimento

Breve introduzione al capitolo, se sarà ritenuta necessaria.

3.1 Pianificazione

Pianificazione del lavoro, gestione delle ore, con rappresentazione grafica.

3.1.1 Interazione tutor

Come abbiamo iniziato; Frequenza degli incontri, come venivano svolti; Revisioni e feedback intermedie, finali.

3.2 Analisi dei requisiti

Breve paragrafo che tratta il come è stata effettuata l'AdR con il Tutor. Alcuni requisiti sono stati definiti a priori dal tutor, altri sono stati ottenuti a seguito di discussioni tra me e il tutor.

3.2.1 Tracciamento requisiti

Quali sono stati i requisiti, obbligatori e non, funzionali e non e come sono stati tracciati.

3.2.2 Verifica requisiti

In che modo si è pianificato di verificare i requisiti sopra elencati.

3.3 Ricerca e studio tecnologie

Ho dedicato un tot di tempo alla ricerca delle tecnologie da utilizzare e il loro studio. Descrizione di alcune importanti tecnologie scelte.

3.3.1 Scelte tecnologiche e progettuali

Spiegazione di alcune scelte effettuate, ad esempio perché ho utilizzato alcune librerie piuttosto che altre, per la ZKP. Descrizione di alcune idee progettuali avute, e perché sono state scartate a favore di altre, ad esempio riguardanti il cercare di evitare, o meno, che qualche utente possa utilizzare più account per effettuare votazioni.

Potrebbero essere aperte altre sottosezioni, se il contenuto di questa sarà particolarmente ampio e/o complesso.

3.4 Sviluppo in Solidity

Come è stato effettuato lo sviluppo in Solidity, definizione del contratto e sue caratteristiche, come è stato caricato su blockchain. Vi saranno eventuali sottosezioni per separare gli argomenti, se il contenuti di essi sarà particolarmente ampio.
Un esempio, con titoli simbolici : "Creazione del contratto", "Caratteristiche del contratto", "Caricamento del contratto"

3.5 Sviluppo in Angular

Come è stato effettuato lo sviluppo in Angular.

3.6 Sviluppo e pianificazione a confronto

Diagramma di Gantt e confronto tra la pianificazione iniziale e l'andamento reale del progetto.

3.7 Testing

Descrizione di quali test sono stati realizzati e in che modo.

3.7.1 Risultati

Risultati ottenuti, con screenshot e/o grafici

3.8 Conclusioni

Capitolo 4

Conclusioni

4.1 Copertura obiettivi

Quali obiettivi sono stati raggiunti e quali non.
Causa del perché alcuni non sono stati raggiunti.

4.2 Importanza delle tecnologie blockchain e zero knowledge proof per la votazione elettronica

Riflessioni riguardanti l'uso della Blockchain e ZKP per lo svolgimento di una votazione elettronica. Pro e contro.

Considerazioni sia personali che oggettive, riguardo le tecnologie Blockchain e ZKP. Sia utilizzate insieme, che prese singolarmente.

4.3 Conoscenze acquisite

Quali conoscenze considero acquisite.

4.4 Valutazione personale

Appendice A

Appendice A

Citazione

Autore della citazione

Bibliografia