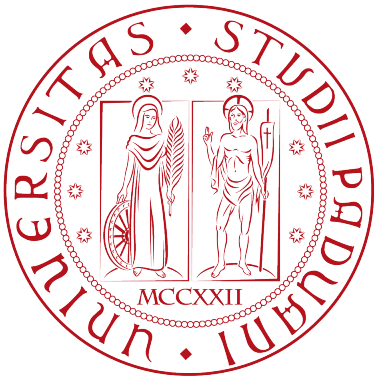
UNIVERSITÀ DEGLI STUDI DI PADOVA



DIPARTIMENTO MATEMATICA

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

SCUOLA DI SCIENZE

CORSO DI LAUREA IN INFORMATICA

Piano di lavoro

Studente:

Gabriel ROVESTI - 2009088

Azienda:

Sync Lab S.r.l

Contatti

Studente: Gabriel Rovesti, gabriel.rovesti@studenti.unipd.it, + 39 346 68 89 789

Tutor aziendale: Fabio Pallaro, f.pallaro@synclab.it, + 39 333 13 68 8500

Azienda: Sync Lab S.r.l, Galleria Spagna, 28, Padova (PD), https://www.synclab.it/

Scopo dello stage

Lo scopo di questo progetto di tirocinio è studiare da un punto di vista teorico i concetti di base delle tecnologie blockchain (concentrandosi sul funzionamento, tipologie di consenso legate, concetto di smart contract, linguaggio Solidity e vulnerabilità), al fine di esaminare il funzionamento delle transazioni e del mining dei blocchi ad essi legati. Successivamente si studierà la self-sovereign identity (detta anche SSI, identità autonoma senza doversi affidare a terze parti), implementandola mediante blockchain, i casi d'uso e i consorzi internazionali che stanno lavorando in questo ambito, anche in relazione ai finanziamenti europei. Infine, verrà esaminato il concetto di Zero Knowledge Proof e come questa tecnologia potrebbe essere utilizzata per la SSI, allo scopo di definire possibili scenari futuri di applicabilità. In particolare, si studieranno le vulnerabilità principali in Solidity e come affrontarle.

Lo studente avrà il compito di studiare le tecnologie indicate, acquisendo conoscenze di base su questi argomenti, col fine di poterne sperimentare l'utilizzo per risolvere problemi concreti nel contesto della blockchain e dell'identità digitale. In particolare, lo studio sarà realizzato in autonomia, analizzando approfondendo a fini di studio teorico e pratico quanto presente in letteratura e sulla base della guida/esperienza fornita dall'azienda stessa.

La realizzazione della tesi di laurea dovrebbe riflettere questo processo di apprendimento delle tecnologie studiate, fornendo una descrizione dettagliata delle tecnologie, dei problemi affrontati e delle soluzioni proposte, affinché possa essere utilizzata come riferimento per un futuro sviluppo di un sistema di identità digitale basato su blockchain.

Tutor aziendale ed interazione con lo studente

Durante lo stage, lo studente avrà come tutor aziendale Fabio Pallaro, che lo guiderà e lo supporterà nell'approfondimento delle tecnologie oggetto di studio. Il tutor aziendale sarà il responsabile della supervisione delle attività svolte dallo studente e della valutazione dei risultati ottenuti. Questi si prefigge di presentare allo studente l'organizzazione dell'azienda, del tirocinio, coinvolgendolo nei progetti presenti e fornendo una panoramica di massima delle tecnologie utilizzate, oggetto di studio e della tesi realizzata.

A questo proposito, di comune accordo, lo studente e il tutor aziendale intendono stabilire degli incontri regolari svolti direttamente, al fine di valutare congiuntamente i progressi del lavoro svolto, chiarire eventuali dubbi e fornire un feedback sullo stato di avanzamento. Questi incontri saranno svolti regolarmente, almeno una volta la settimana, e potranno essere svolti anche in modalità telematica con il tutor interno, in base alla necessità ed alla disponibilità di entrambi. In questo modo, lo studente può essere guidato e supportato nella realizzazione della tesi di laurea, al fine di poterla presentare in modo completo e soddisfacente.

Prodotti attesi

Lo studente dovrà produrre una relazione scritta che riassume lo studio condotto nel periodo invididuato, fornendo una panoramica completa e approfondita delle tecnologie oggetto di studio (analizzando le caratteristiche, le potenzialità e le criticità di ciascuna di esse). Questa, in particolare, illustra i seguenti punti.

1. Introduzione

   Descrizione del contesto in cui si inserisce il progetto di stage e del problema affrontato, sulla base dello studio svolto e della realtà aziendale presente. In questa sezione sarà inclusa un'analisi del contesto di lavoro, spiegando la motivazione del progetto e dei suoi obiettivi ed impatti.

2. Analisi delle tecnologie

   Descrizione delle tecnologie oggetto di studio, con analisi delle caratteristiche, delle potenzialità e delle criticità di ciascuna di esse. Qui verranno inoltre riportate eventuali vulnerabilità di sicurezza. Per ciascuna di queste, saranno individuati opportuni casi d'uso reali. Le sottosezioni dedicate forniranno un quadro completo dell'utilizzo delle tecnologie, commentando nel dettaglio le caratteristiche utili per risolvere il problema affrontato.

3. Scenario di applicabilità

   Studio e descrizione di un possibile scenario di applicazione delle tecnologie oggetto di studio, con analisi dei vantaggi e degli svantaggi rispetto a soluzioni alternative. Questa ha l'obiettivo di individuare campi di applicazione, sulla base dei vari consorzi internazionali interessati e analizzando casi d'uso reali.

   In particolare, verrà analizzato il caso di applicazione della SSI, con particolare riferimento alla tecnologia Zero Knowledge Proof. L'analisi sarà svolta criticamente, contestualizzata e con riferimento a soluzioni alternative, individuando punti di forza e limiti presenti.

4. Conclusioni e sviluppi futuri. Riassunto dei risultati ottenuti, delle conclusioni raggiunte e delle eventuali prospettive future di sviluppo e ricerca su questi temi. In particolare, vengono presentate le principali conclusioni emerse dallo studio e del lavoro svolto, fornendo una visione d'insieme delle tecnologie e delle loro implicazioni.

Qualora, al termine dell'analisi, lo studente disponga ancora di tempo a sua disposizione, potrà dedicarsi a approfondimenti o implementazioni aggiuntive, concordate con l'azienda ospitante.

Contenuti formativi previsti

Durante questo progetto di stage lo studente avrà occasione di approfondire le sue conoscenze in ambito blockchain e self-sovereign identity, come indicato di seguito in dettaglio.

- **Concetti di base blockchain**
  - Studio del funzionamento della blockchain;
  - Concetto di wallet e funzionamento firma asimmetrica delle transazioni su catena;
  - Validazione e mining dei blocchi;
  - Tipologie di Consenso e studio delle catene più conosciute;
  - Concetto di Smart contract e linguaggio Solidity;
  - Scalabilità e limiti della tecnologia blockchain;
  - Tokenizzazione e creazione di token su blockchain;
  - Concetto di immutabilità nella blockchain e il ruolo della crittografia;

  - Vulnerabilità principali in Solidity (e.g. reentrancy, integer overflow/underflow, etc.).

- **Self-Sovereign Identity e Zero Knowledge Proof**
  - Studio del concetto di self-sovereign identity (SSI);
  - Descrizione di protocolli e tecnologie per la gestione delle identità digitali;
  - Analisi delle caratteristiche, delle potenzialità e delle criticità di ciascuna di esse;
  - Approfondimento delle tecniche di crittografia utilizzate per garantire la sicurezza e la privacy delle informazioni personali nell'ambito della SSI;
  - Casi d'uso reali individuati;
  - Consorzi internazionali coinvolti e finanziamenti europei;
  - Studio di un possibile scenario futuro di applicabilità, discutendo problemi e sfide correlati;
  - Zero Knowledge Proof: cos'è e come potrebbe servire per la SSI.

Pianificazione del lavoro

1. **Settimana 1-2 (40 ore)** - Introduzione al progetto di stage e presentazione degli obiettivi da raggiungere. Formazione di base sulle tecnologie blockchain e self-sovereign identity.
2. **Settimana 3-4 (40 ore)** - Blockchain: studio del funzionamento della blockchain, concetto di wallet e firma asimmetrica delle transazioni, validazione e mining dei blocchi, tipologie di consenso, Smart contract e linguaggio Solidity, limiti e scalabilità della tecnologia blockchain. Studio della creazione di token su blockchain.
3. **Settimana 5-6 (40 ore)** - Self-sovereign identity: studio del concetto di SSI, protocolli e tecnologie per la gestione delle identità digitali, analisi delle caratteristiche e delle criticità di ciascuna di esse. Studio delle vulnerabilità principali in Solidity.
4. **Settimana 7-8 (40 ore)** - Crittografia e protocolli utizzati nella blockchain: approfondimento delle tecniche utilizzate per garantire la sicurezza e la privacy delle informazioni personali nell'ambito della blockchain e della SSI, ruolo della crittografia nell'immutabilità della blockchain.

5. **Settimana 9-10 (40 ore)** - Casi d'uso reali di self-sovereign identity: individuazione di casi d'uso reali di SSI e presentazione di esempi di applicazioni attuali. Studio dei consorzi internazionali coinvolti e dei finanziamenti europei legati alla self-sovereign identity.
6. **Settimana 11-12 (40 ore)** - Zero Knowledge Proof: studio di cos'è e come potrebbe servire per la SSI, analisi delle applicazioni reali e delle sfide tecniche da affrontare.
7. **Settimana 13-14 (40 ore)** - Approfondimento degli aspetti di sicurezza della blockchain: studio delle vulnerabilità principali in Solidity, tecniche e strumenti per la sicurezza degli smart contract.
8. **Settimana 15-16 (40 ore)** - Possibili scenari futuri di applicazione della blockchain e della SSI: studio di un possibile scenario futuro di applicabilità, discutendo problemi e sfide correlati.

Ripartizione ore

La pianificazione, in termini di quantità di ore di lavoro, sarà così distribuita:

Durata in ore	Descrizione dell'attività
20	**Introduzione**
20	**Blockchain: consenso e tipologie, validazione, mining dei blocchi**
20	**Smart Contract e Linguaggio Solidity**
20	**Tokenizzazione e immutabilità nella blockchain**
20	**Scalabilità e limiti della blockchain**
20	**Self-sovereign identity (SSI)**
20	**Protocolli e tecnologie usati nella SSI**
20	**Crittografia ed immutabilità nella blockchain**
20	**Casi d'uso reali individuati nella SSI**
20	**Consorzi internazionali coinvolti e finanziamenti europe**
20	**Zero Knowledge Proof: studio e tecniche**
20	**Applicazioni di Zero Knowledge Proof nella SSI**
20	**Vulnerabilità principali in Solidity**
20	**Strumenti per la sicurezza degli smart contract**
20	**Studio di scenario di applicabilità**
20	**Conclusione**
Totale ore	**320**

Obiettivi

Notazione

Si farà riferimento ai requisiti secondo le seguenti notazioni:

- *O* per i requisiti obbligatori, vincolanti in quanto obiettivo primario richiesto dal committente;
- *D* per i requisiti desiderabili, non vincolanti o strettamente necessari, ma dal riconoscibile valore aggiunto;
- *F* per i requisiti facoltativi, rappresentanti valore aggiunto non strettamente competitivo.

Le sigle precedentemente indicate saranno seguite da una coppia sequenziale di numeri, identificativo del requisito.

Obiettivi fissati

Si prevede lo svolgimento dei seguenti obiettivi:

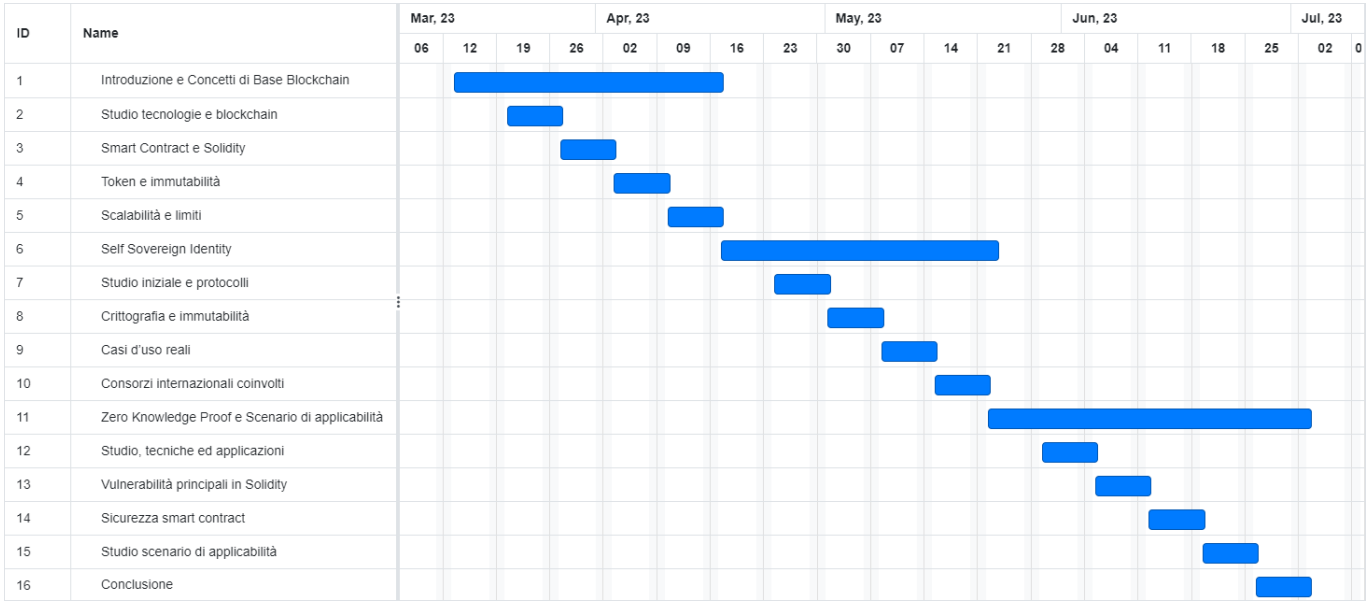
- Obbligatori
  - *O01*: Descrivere i concetti di base della blockchain, tra cui la sua architettura, i nodi della rete, la criptografia e il consenso distribuito;
  - *O02*: Analizzare il concetto di Smart contract e il linguaggio Solidity, con particolare attenzione alle vulnerabilità principali e alle tecniche per evitare errori di programmazione;
  - *O03*: Approfondire il funzionamento della firma asimmetrica delle transazioni su catena e la validazione dei blocchi, studiando le tipologie di consenso e le catene più conosciute;
  - *O04*: Studiare le tecniche di crittografia utilizzate per garantire la sicurezza e la privacy delle informazioni personali nell'ambito della Self-Sovereign Identity (SSI) e dei protocolli per la gestione delle identità digitali;
  - *O05*: Individuare casi d'uso reali per la SSI, analizzando i consorzi internazionali coinvolti in ambito di ricerca e i finanziamenti europei;
  - *O06*: Discutere le sfide e i problemi legati alla SSI, studiando un possibile scenario futuro di applicabilità e basato su Zero Knowledge Proof (ZKP).
- Desiderabili

  - *D01*: Analizzare la scalabilità e i limiti della tecnologia blockchain;
  - *D02*: Analizzare le criticità e le sfide nella gestione dell'identità digitale, come la perdita o la violazione dei dati, la mancanza di standard e la scarsa adozione da parte degli utenti;
  - *D03*: Esplorare le tecnologie di smart contract e di blockchain programmabile, per esempio Ethereum, e il loro possibile utilizzo in un sistema SSI;
  - *D04*: Approfondimento delle tecniche di tokenizzazione e creazione di token su blockchain.

- Facoltativi
  - *F01*: Approfondire gli aspetti tecnici relativi alla blockchain, analizzando le vulnerabilità principali e le tecniche per mitigarle;
  - *F02*: Analisi di progetti blockchain già esistenti, individuando criticità e punti di forza;
  - *F03*: Studio di altre tecnologie emergenti nel campo della gestione delle identità digitali, come ad esempio la tecnologia DID (Decentralized Identifiers).

Pianificazione temporale

Di seguito è riportato il diagramma di Gantt relativo al piano di lavoro previsto, che riassume le attività da svolgere e le relative date di inizio e fine.



Approvazione

Il presente piano di lavoro è stato approvato dai seguenti

Fabio Pallaro Tutor aziendale

Gabriel Rovesti Stagista

Prof.ssa Ombretta Gaggi Tutor interno

2023-08-03