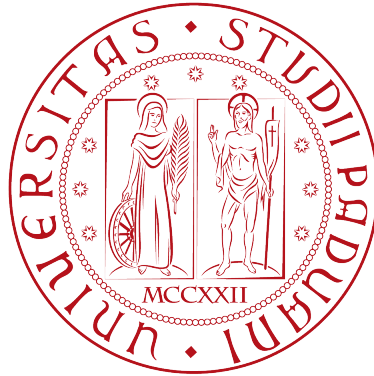


UNIVERSITÀ DEGLI STUDI DI PADOVA



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 stage è di fornire allo studente un'esperienza a metà tra il teorico e il pratico nell'ambito della blockchain e della self-sovereign identity. Durante lo stage, lo studente approfondirà le sue conoscenze sui concetti di base della blockchain, compresi il funzionamento della blockchain, le transazioni su catena, il mining dei blocchi, le tipologie di consenso e il linguaggio Solidity. Inoltre, lo studente avrà l'opportunità di esplorare i concetti di self-sovereign identity (SSI) e Zero Knowledge Proof, imparando i protocolli e le tecnologie per la gestione delle identità digitali, l'uso di crittografia per la sicurezza e la privacy delle informazioni personali e i possibili casi d'uso reali.

Successivamente, lo studente approfondirà le librerie EthersJS/Web3JS per interagire con la blockchain Ethereum e implementerà un Proof of Concept (POC) con queste librerie. Lo studente imparerà a configurare l'ambiente di sviluppo per interagire con una blockchain Ethereum di test, a progettare e implementare un'interfaccia utente (UI) per la dApp utilizzando HTML, CSS e Javascript, a interagire con la blockchain Ethereum tramite la libreria EthersJS/Web3JS per la lettura e la scrittura di dati sulla blockchain e a implementare funzionalità di autenticazione utente utilizzando la SSI e i protocolli studiati in precedenza.

Infine, lo studente discuterà di problemi e sfide relativi all'implementazione di applicazioni decentralizzate su blockchain Ethereum, studiando le possibili implementazioni future, sfide e limiti presenti, approfondendo tematiche di sicurezza e privacy connesse al loro utilizzo.

**ISO 9001**

LL-C (Certification)

**ISO 14001**

LL-C (Certification)

**ISO 27001**

LL-C (Certification)

**ISO 45001**

LL-C (Certification)

Napoli (Sede Legale)

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19
00142 - Tel. 06 976 118 66

Milano

Via G. Durando, 38
20158 - Tel. 02 365 690 26

Padova

Galleria Spagna, 28
35127 - Tel. 049 817 10 60

Verona

Via Albere, 19
37138 - Tel. 045 464 77 70

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

Durante il tirocinio, lo studente dovrà produrre un Proof of Concept di un'applicazione decentralizzata (dApp) che interagisce con la blockchain Ethereum. La dApp dovrà essere implementata utilizzando la libreria EthersJS/Web3JS per la lettura e la scrittura di dati sulla blockchain. In particolare, la dApp dovrà implementare le seguenti funzionalità:

- **Autenticazione utente:** la dApp dovrà utilizzare i protocolli di identità digitale studiati durante il tirocinio (ad esempio, DID e Verifiable Credentials) per implementare un sistema di autenticazione utente.
- **Registrazione di dati sulla blockchain:** la dApp dovrà permettere agli utenti di registrare dati sulla blockchain Ethereum, utilizzando un'interfaccia utente intuitiva e facile da usare.
- **Lettura di dati dalla blockchain:** la dApp dovrà permettere agli utenti di leggere i dati registrati sulla blockchain Ethereum in modo sicuro e affidabile.

**Napoli (Sede Legale)**Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30**Roma**

Largo C. Salinari, 19

Milano

Via G. Durando, 38

Padova

Galleria Spagna, 28

Verona

Via Albere, 19

00142 - Tel. 06 976 118 66 20158 - Tel. 02 365 690 26 35127 - Tel. 049 817 10 60 37138 - Tel. 045 464 77 70

Sync Lab S.r.l. - Cap. soc. €100.000 i.v. - N.Reg. Imprese NA/CF/P.IVA:07952560634 – Cod. fattura elettronica: SUBM70N - synclab@pec.it - direzione@synclab.it - www.synclab.it

Inoltre, lo studente dovrà produrre un documento che descriva il percorso di studio realizzato durante il tirocinio. In particolare, il documento dovrà includere i seguenti elementi di massima:

1. **Introduzione:** una breve descrizione del progetto e degli obiettivi dello stage.
2. **Descrizione della dApp:** una descrizione dettagliata dell'applicazione decentralizzata sviluppata durante il tirocinio, comprese le funzionalità implementate e le tecnologie utilizzate.
3. **Analisi delle tecnologie:** una descrizione delle tecnologie utilizzate per implementare la dApp, compresi i protocolli di identità digitale e i protocolli di Zero Knowledge Proof e di Self-Sovereign Identity.
4. **Problematiche e soluzioni:** una discussione delle problematiche incontrate durante lo sviluppo della dApp e delle soluzioni adottate per risolverle.
5. **Sfide e limiti:** un'analisi critica delle sfide incontrate durante lo sviluppo della dApp e nello studio autonomo delle tecnologie blockchain, comprese le ricerche di sicurezza effettuate e le possibili soluzioni future.
6. **Scenari futuri:** una discussione delle possibili implementazioni future delle tecnologie blockchain e delle applicazioni decentralizzate.
7. **Conclusioni:** una sintesi delle attività svolte durante il tirocinio e delle competenze acquisite.

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;



ISO 9001

LL-C (Certification)



ISO 14001

LL-C (Certification)



ISO 27001

LL-C (Certification)



ISO 45001

LL-C (Certification)

Napoli (Sede Legale)

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19
00142 - Tel. 06 976 118 66

Milano

Via G. Durando, 38
20158 - Tel. 02 365 690 26

Padova

Galleria Spagna, 28
37138 - Tel. 049 817 10 60

Verona

Via Albere, 19
37138 - Tel. 045 464 77 70

- 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.

• Studio delle librerie EthersJS/Web3JS e implementazione tramite Proof of Concept (POC)

- Studio delle principali librerie Javascript per interagire con la blockchain Ethereum (EthersJS, Web3JS, ecc.);
- Analisi delle caratteristiche e delle funzionalità offerte dalle librerie;
- Implementazione di un Proof of Concept (POC) con librerie EthersJS/Web3JS;
- Configurazione dell'ambiente di sviluppo per interagire con una blockchain Ethereum di test;
- Studio dell'architettura di un'applicazione decentralizzata (dApp) su blockchain Ethereum e dei componenti principali (smart contract, frontend, backend);
- Implementazione di un'interfaccia utente (UI) per la dApp utilizzando HTML, CSS e Javascript;
- Interazione con la blockchain Ethereum tramite la libreria EthersJS/Web3JS per la lettura e la scrittura di dati sulla blockchain;

**Napoli (Sede Legale)**

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19
00142 - Tel. 06 976 118 66

Milano

Via G. Durando, 38
20158 - Tel. 02 365 690 26

Padova

Galleria Spagna, 28
37138 - Tel. 049 817 10 60

Verona

Via Albere, 19
37138 - Tel. 045 464 77 70

- Implementazione di funzionalità di autenticazione utente utilizzando la SSI e i protocolli studiati in precedenza;
- Testing e debugging del POC implementato;
- Discussione di problemi e sfide relativi all'implementazione di applicazioni decentralizzate su blockchain Ethereum.

Pianificazione del lavoro

1. Prima Settimana - Introduzione alle tecnologie blockchain (20 ore)

- Introduzione alle tecnologie blockchain;
- Studio del funzionamento della blockchain e dei concetti di base (wallet, firma asimmetrica, transazioni, etc.);
- Studio dei principali tipi di blockchain e dei meccanismi di consenso;

2. Seconda Settimana - Concetti avanzati di blockchain (20 ore)

- Studio di concetti avanzati di blockchain come Smart contract, Solidity e tokenizzazione;
- Analisi di vulnerabilità principali in Solidity (e.g. reentrancy, integer overflow/underflow, etc.);
- Studio della scalabilità e dei limiti della tecnologia blockchain;

3. Terza Settimana - Token, scalabilità e immutabilità(20 ore)

- Studio della tokenizzazione e della creazione di token su blockchain;
- Studio della scalabilità e dei limiti della tecnologia blockchain;
- Concetto di immutabilità nella blockchain e il ruolo della crittografia;

4. Quarta Settimana - Self-sovereign identity (SSI): protocolli, tecnologie e criticità (20 ore)

- Studio del concetto di self-sovereign identity;
- Descrizione di protocolli e tecnologie per la gestione delle identità digitali;
- Analisi delle caratteristiche, delle potenzialità e delle criticità di ciascuna di esse;



ISO 9001

LL-C (Certification)



ISO 14001

LL-C (Certification)



ISO 27001

LL-C (Certification)



ISO 45001

LL-C (Certification)

Napoli (Sede Legale)

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19

Milano

Via G. Durando, 38

Padova

Galleria Spagna, 28

Verona

Via Albere, 19

80143 - Tel. 081 787 50 30 00142 - Tel. 06 976 118 66 20158 - Tel. 02 365 690 26 35127 - Tel. 049 817 10 60 37138 - Tel. 045 464 77 70

Sync Lab S.r.l. - Cap. soc. €100.000 i.v. - N.Reg. Imprese NA/CF/P.IVA:07952560634 – Cod. fattura elettronica: SUBM70N - syncclub@pec.it - direzione@syncclub.it - www.syncclub.it

5. Quinta Settimana - Zero Knowledge Proof (ZKP) e sua applicazione alla SSI (20 ore)

- Studio del concetto di Zero Knowledge Proof;
- Applicazione di Zero Knowledge Proof alla SSI;
- Casi d'uso reali della SSI e della tecnologia Zero Knowledge Proof;
- Primo studio consorzi internazionali coinvolti e finanziamenti europei;

6. Sesta Settimana - Studio delle librerie EthersJS/Web3JS (20 ore)

- Studio delle principali librerie Javascript per interagire con la blockchain Ethereum (EthersJS, Web3JS, ecc.);
- Analisi delle caratteristiche e delle funzionalità offerte dalle librerie;
- Configurazione dell'ambiente di sviluppo per interagire con una blockchain Ethereum di test;

7. Settima e Ottava Settimana - Implementazione Proof of Concept con EthersJS/Web3JS (40 ore)

- Definizione dei requisiti per il PoC da implementare;
- Studio delle librerie EthersJS/Web3JS per interagire con la blockchain Ethereum;
- Configurazione dell'ambiente di sviluppo per interagire con una blockchain Ethereum di test;
- Studio dell'architettura di un'applicazione decentralizzata (dApp) su blockchain Ethereum e dei componenti principali (smart contract, frontend, backend);
- Implementazione di un'interfaccia utente (UI) per la dApp utilizzando HTML, CSS e Javascript;
- Interazione con la blockchain Ethereum tramite la libreria EthersJS/Web3JS per la lettura e la scrittura di dati sulla blockchain;
- Implementazione di funzionalità di autenticazione utente utilizzando la SSI e i protocolli studiati in precedenza;
- Testing e debugging del POC implementato;
- Discussione di problemi e sfide relativi all'implementazione di applicazioni decentralizzate su blockchain Ethereum.

**ISO 9001**

LL-C (Certification)

**ISO 14001**

LL-C (Certification)

**ISO 27001**

LL-C (Certification)

**ISO 45001**

LL-C (Certification)

Napoli (Sede Legale)

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19

00142 - Tel. 06 976 118 66

Milano

Via G. Durando, 38

20158 - Tel. 02 365 690 26

Padova

Galleria Spagna, 28

35127 - Tel. 049 817 10 60

Verona

Via Albere, 19

37138 - Tel. 045 464 77 70

8. Nona Settimana - SSI: approfondimenti e implementazione nel PoC

- Studio approfondito 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;
- Integrazione della SSI nel POC sviluppato in precedenza;
- Testing e debugging delle funzionalità di autenticazione utente utilizzando la SSI;
- Discussione di problemi e sfide relativi all'utilizzo della SSI in applicazioni decentralizzate su blockchain Ethereum.

9. Decima Settimana - ZKP: approfondimenti e implementazione nel PoC

- Studio di Zero Knowledge Proof (ZKP);
- Approfondimento dell'utilizzo di ZKP per la SSI;
- Implementazione di una funzionalità di ZKP nel POC sviluppato in precedenza;
- Testing e debugging delle funzionalità di ZKP implementate;
- Discussione di problemi e sfide relativi all'utilizzo di ZKP in applicazioni decentralizzate su blockchain Ethereum e nella SSI.

10. Undicesima Settimana - Scalabilità nella blockchain e analisi second layer (20 ore)

- Studio della scalabilità della tecnologia blockchain;
- Analisi dei limiti della blockchain Ethereum e delle possibili soluzioni;
- Studio delle soluzioni di second layer per la scalabilità, come gli State Channels e i Sidechains;
- Implementazione di una soluzione di second layer nel POC sviluppato in precedenza;
- Testing e debugging della soluzione di second layer implementata;



ISO 9001

LL-C (Certification)



ISO 14001

LL-C (Certification)



ISO 27001

LL-C (Certification)



ISO 45001

LL-C (Certification)

Napoli (Sede Legale)

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19

00142 - Tel. 06 976 118 66

Milano

Via G. Durando, 38

20158 - Tel. 02 365 690 26

Padova

Galleria Spagna, 28

35127 - Tel. 049 817 10 60

Verona

Via Albere, 19

37138 - Tel. 045 464 77 70

- Implicazioni e limitazioni dell'uso delle soluzioni di second layer in ambito blockchain.

11. Dodicesima Settimana - Analisi di vulnerabilità e sicurezza (20 ore)

- Studio delle vulnerabilità principali della blockchain Ethereum;
- Analisi dei rischi di sicurezza per i contratti intelligenti su Ethereum;
- Studio delle tecniche di hacking utilizzate per attaccare le blockchain;
- Utilizzo di strumenti di sicurezza per analizzare e proteggere le reti blockchain;
- Analisi delle vulnerabilità degli exchange di criptovalute e delle strategie per mitigare i rischi;
- Valutazione della sicurezza delle criptovalute e dei portafogli digitali;

12. Tredicesima Settimana - Implementazione misure individuate nel PoC (20 ore)

- Revisione e analisi dei risultati dell'analisi di vulnerabilità e sicurezza della blockchain Ethereum e dei contratti intelligenti;
- Implementazione di contromisure per mitigare i rischi di sicurezza identificati durante l'analisi di vulnerabilità;
- Studio delle best practices per la sicurezza delle applicazioni decentralizzate (dApp) su blockchain Ethereum;
- Valutazione dell'efficacia delle contromisure implementate per mitigare i rischi di sicurezza;
- Discussione di nuove minacce di sicurezza per la blockchain Ethereum e dei metodi per affrontarle.

13. Quattordicesima Settimana - Analisi di limiti e sfide nell'implementazione decentralizzata (20 ore)

- Analisi delle principali implementazioni di blockchain (ad esempio, Bitcoin, Ethereum, Ripple, etc.);
- Studio delle differenze tra le implementazioni di blockchain pubbliche e private;
- Discussione dei limiti attuali della tecnologia blockchain e delle aree in cui è necessario migliorare;
- Analisi delle potenziali applicazioni della blockchain in vari settori (ad esempio, finanza, supply chain, sanità, etc.);



ISO 9001

LL-C (Certification)



ISO 14001

LL-C (Certification)



ISO 27001

LL-C (Certification)



ISO 45001

LL-C (Certification)

Napoli (Sede Legale)

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19

00142 - Tel. 06 976 118 66

Milano

Via G. Durando, 38

20158 - Tel. 02 365 690 26

Padova

Galleria Spagna, 28

35127 - Tel. 049 817 10 60

Verona

Via Albere, 19

37138 - Tel. 045 464 77 70

- Studio delle opportunità e dei rischi associati alla tokenizzazione di asset tradizionali tramite la blockchain;
- Discussione delle implicazioni legali e regolamentari della blockchain e delle criptovalute.

14. Quindicesima Settimana - Consorzi internazionali coinvolti e finanziamenti europei (20 ore)

- Approfondimento sulle organizzazioni di standardizzazione, come ISO e IEEE, e sul loro ruolo nello sviluppo e nella definizione degli standard blockchain;
- Studio delle partnership tra aziende e organizzazioni per lo sviluppo di progetti blockchain, come il consorzio R3;
- Analisi dei finanziamenti disponibili per lo sviluppo di progetti blockchain a livello nazionale e internazionale, come il programma Horizon 2020 dell'Unione Europea;
- Esplorazione delle implicazioni legali e regolatorie nell'ambito della partecipazione a progetti blockchain finanziati da enti pubblici o privati;
- Discussione delle strategie di networking e di comunicazione per individuare e partecipare a progetti di ricerca e sviluppo sulla blockchain;
- Approfondimento sui processi di selezione dei progetti finanziati, e su come aumentare le probabilità di successo nella partecipazione a bandi pubblici o privati.

15. Sedicesima Settimana - Discussione scenari di applicabilità e conclusione (20 ore)

- Analisi dei casi d'uso più interessanti e promettenti per la blockchain e le criptovalute in ambiti specifici come la finanza, la logistica, la salute, la pubblica amministrazione, etc.;
- Discussione dei vantaggi e delle limitazioni dell'utilizzo della blockchain e delle criptovalute rispetto alle tecnologie tradizionali;
- Esplorazione di nuovi sviluppi tecnologici e di progetti di ricerca in corso che potrebbero influenzare l'evoluzione della blockchain e delle criptovalute;
- Valutazione dei possibili impatti socio-economici e delle opportunità per l'innovazione che potrebbero derivare dall'adozione su larga scala della blockchain e delle criptovalute;
- Discussione delle sfide e dei rischi che potrebbero sorgere con l'uso della blockchain e delle criptovalute, come la scalabilità, la privacy, la sicurezza e la regolamentazione.



ISO 9001

LL-C (Certification)



ISO 14001

LL-C (Certification)



ISO 27001

LL-C (Certification)



ISO 45001

LL-C (Certification)

Napoli (Sede Legale)

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19
00142 - Tel. 06 976 118 66

Milano

Via G. Durando, 38
20158 - Tel. 02 365 690 26

Padova

Galleria Spagna, 28
37138 - Tel. 045 464 77 70

Verona

Via Albere, 19
37138 - Tel. 045 464 77 70

Ripartizione ore

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

60	Blockchain: introduzione alle tecnologie
40	Concetti di base ed avanzati
20	Token, scalabilità ed immutabilità
40	Self-sovereign identity (SSI) e Zero Knowledge Proof (ZKP)
20	Studio e descrizione dei protocolli impiegati per SSI
20	Concetto di ZKP, applicazione alla SSI e primo studio consorzi coinvolti
120	Proof of Concept: studio ed implementazione con librerie JS, applicazione di SSI, ZKP e scalabilità
20	Studio e analisi delle tecnologie impiegate
40	Creazione ambiente di lavoro, definizione requisiti, implementazione blockchain base e prima UI
40	Studio approfondito ZKP e SSI e loro implementazione nel PoC
40	Soluzioni di scalabilità ed implementazione second layer nel PoC
40	Analisi di sicurezza e vulnerabilità e implementazione nel PoC
20	Valutazione e discussione delle contromisure di sicurezza
20	Implementazione misure di sicurezza nel PoC
60	Limiti, sfide, ricerche e scenari di applicabilità
20	Analisi di limiti, sfide e discussione delle implicazioni legate a blockchain
20	Approfondimento e discussione dei finanziamenti coinvolti e delle strategie di organizzazione
20	Valutazione di casi d'uso reali e discussione delle sfide future
Totale ore	320



Napoli (Sede Legale)

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19

Milano

Via G. Durando, 38

Padova

Galleria Spagna, 28

Verona

Via Albere, 19

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 crittografia 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).

**ISO 9001**

LL-C (Certification)

**ISO 14001**

LL-C (Certification)

**ISO 27001**

LL-C (Certification)

**ISO 45001**

LL-C (Certification)

Napoli (Sede Legale)

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19

00142 - Tel. 06 976 118 66

Milano

Via G. Durando, 38

20158 - Tel. 02 365 690 26

Padova

Galleria Spagna, 28

35127 - Tel. 049 817 10 60

Verona

Via Albere, 19

37138 - Tel. 045 464 77 70

- Desiderabili

- D01: Implementare una dApp tramite le librerie EthersJS/Web3JS, utilizzando un smart contract di esempio;
- D02: Realizzare una UI (interfaccia utente) per la dApp utilizzando HTML, CSS e JavaScript;
- D03: Utilizzare la SSI e i protocolli studiati per implementare funzionalità di autenticazione utente nella dApp;
- D04: Testare e debuggare la dApp implementata;
- D05: Discutere problemi e sfide relativi all'implementazione di applicazioni decentralizzate su blockchain Ethereum, con particolare attenzione alla scalabilità e alla sicurezza.

- Facoltativi

- F01: Approfondire l'utilizzo di altri linguaggi di programmazione per gli smart contract, come Vyper;
- F02: Analizzare l'utilizzo di altre tecnologie blockchain, come Polkadot o Cardano, per implementare la SSI;
- F03: Esplorare altre funzionalità delle librerie EthersJS/Web3JS, come l'invio di transazioni;
- F04: Investigare i limiti e le sfide legate all'utilizzo della tecnologia blockchain.



ISO 9001

LL-C (Certification)



ISO 14001

LL-C (Certification)



ISO 27001

LL-C (Certification)



ISO 45001

LL-C (Certification)

Napoli (Sede Legale)Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30**Roma**

Largo C. Salinari, 19

Milano

Via G. Durando, 38

Padova

Galleria Spagna, 28

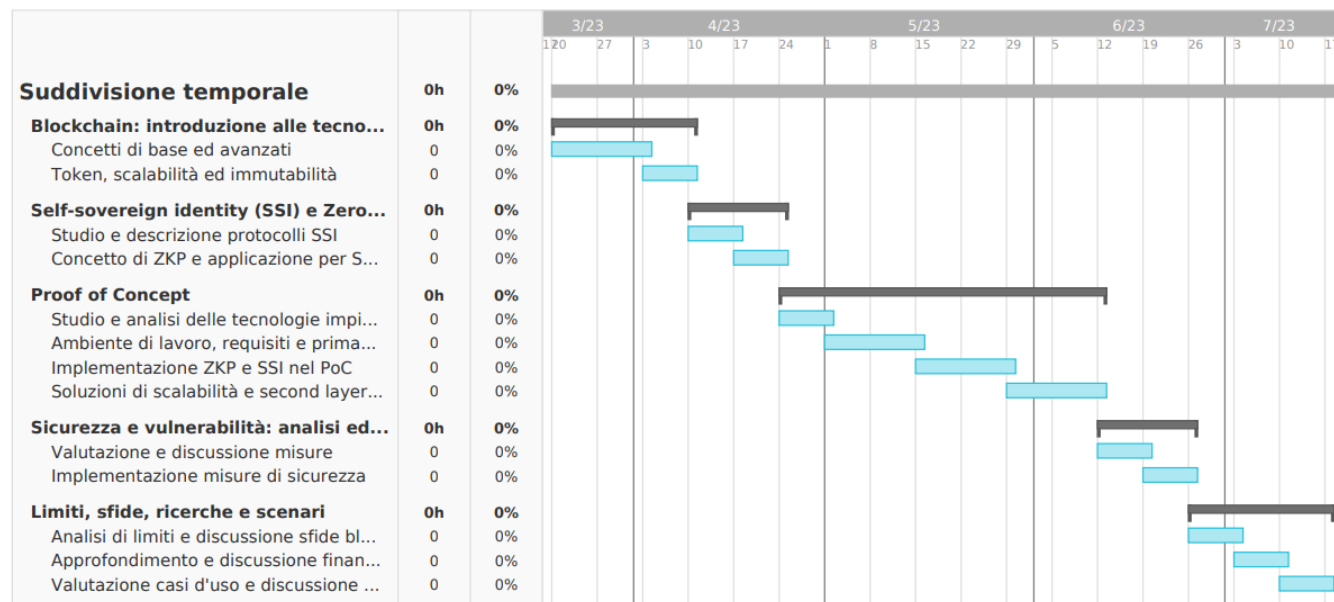
Verona

Via Albere, 19

00142 - Tel. 06 976 118 66 20158 - Tel. 02 365 690 26 35127 - Tel. 049 817 10 60 37138 - Tel. 045 464 77 70

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

2023-10-03



Napoli (Sede Legale)

Via G. Porzio CDN is B8
80143 - Tel. 081 787 50 30

Roma

Largo C. Salinari, 19
00142 - Tel. 06 976 118 66

Milano

Via G. Durando, 38
20158 - Tel. 02 365 690 26

Padova

Galleria Spagna, 28
35127 - Tel. 049 817 10 60

Verona

Via Albere, 19
37138 - Tel. 045 464 77 70