



UNIVERSITÀ
DEGLI STUDI
FIRENZE

Scuola di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Magistrale in Informatica

Tesi di Laurea Magistrale

PROGETTAZIONE DI UNO SMART
CONTRACT A SUPPORTO DEL
PROTOCOLLO DI FAIR EXCHANGE DI
VERIOSS, UNA PIATTAFORMA BUG
BOUNTY BASATA SULLA BLOCKCHAIN

DESIGN OF A SMART CONTRACT TO
SUPPORT THE FAIR EXCHANGE PROTOCOL
OF VERIOSS, A BLOCKCHAIN-BASED
BUG-BOUNTY PLATFORM

FRANCESCO MUCCI

Relatore: Prof. *Rosario Pugliese*
Correlatori: Prof. *Gabriele Costa*, Dott. *Letterio Galletta*

Anno Accademico 2022-2023

Copyright ©: Francesco Mucci, *Progettazione di uno smart contract a supporto del protocollo di fair exchange di VeriOSS, una piattaforma bug bounty basata sulla blockchain*, Versione 1.0.0 (8 gennaio 2024), Università degli Studi di Firenze, Corso di Laurea Magistrale in Informatica, Anno Accademico 2022-2023

*A <Nome>,
<frase di dedica>.*

"Le vent se lève!... il faut tenter de vivre!"
— Paul Valéry, *Le Cimetière marin*, 1920 [1].

*"The best theory is inspired by practice
and the best practice is inspired by theory."*

— Donald E. Knuth, Theory and practice, 1991 [2].

PREFAZIONE

Durante l'anno accademico 2019-2020 ho collaborato con l'unità di ricerca SySMA della Scuola IMT Alti Studi Lucca in qualità di beneficiario della borsa di ricerca **VeriOSS smart contract development** (finanziata con i fondi del progetto PAI 2018 "*VeriOSS: a security-by-smart contract verification framework for Open Source Software*" - Po137). L'obiettivo della borsa era quello di progettare e sviluppare smart contract Solidity a supporto del protocollo di fair exchange di VeriOSS, una piattaforma per la bug bounty basata sulla blockchain. Il lavoro di tesi svolto prosegue e conclude quanto iniziato durante la suddetta collaborazione di ricerca.

Tutto il materiale prodotto per questo lavoro di tesi è accessibile attraverso diverse repository pubbliche su GitHub; in particolare:

- i file \LaTeX associati a questo documento di tesi si trovano in `github.com/FrancescoMucci/VeriOSS-thesis`.
- il codice implementato è disponibile in `github.com/FrancescoMucci/VeriOSS-challenge-reward`;
- infine, i diagrammi di sequenza, di stato e di classe sono raccolti in `github.com/FrancescoMucci/VeriOSS-diagrams`.

Per individuare e correggere involontarie somiglianze o citazioni non adeguate, è stato utilizzato *Turnitin*, il software antiplagio messo a disposizione dall'Università degli Studi di Firenze.

INDICE

Acronimi	ix
Elenco delle figure	x
Elenco delle tabelle	xi
Elenco dei codici	xii
1 INTRODUZIONE	1
1.1 Contesto	1
1.2 Problema affrontato	1
1.3 Stato dell'arte	1
1.4 Domande di ricerca	2
1.5 Approccio usato	2
1.6 Contributi originali	2
1.7 Struttura della tesi	3
2 PRELIMINARI	4
2.1 Introduzione al capitolo	5
2.2 Nozioni preliminari	5
2.3 Lavori precedenti	6
2.4 Metodi e tecniche utilizzate	6
2.5 Tecnologie utilizzate	6
2.6 Riassunto del capitolo e conclusioni	7
3 APPROCCIO	8
3.1 Introduzione al capitolo	8
3.2 Specifica dei requisiti	9
3.2.1 Requisiti funzionali	9
3.2.2 Requisiti non funzionali	9
3.3 Architettura del sistema	10
3.3.1 Design architetturale del sistema	10
3.3.2 Componente 1 del sistema	10
3.3.3 Componente n del sistema	10
3.3.4 Considerazioni sulle scelte architettureali	11
3.4 Riassunto del capitolo e conclusioni	11
4 VALUTAZIONE	12
4.1 Introduzione al capitolo	13
4.2 Implementazione	13
4.2.1 Implementazione componente 1	13

4.2.2	Implementazione componente n	14
4.2.3	Sfide implementative e soluzioni	14
4.3	Test	14
4.3.1	Test d'unità	14
4.3.2	Test d'integrazione	14
4.3.3	Test end-to-end	14
4.4	Qualità dei test	15
4.4.1	Test coverage	15
4.4.2	Mutation testing	15
4.5	Risultati	15
4.6	Riassunto del capitolo e conclusioni	16
5	DISCUSSIONE	17
5.1	Introduzione al capitolo	18
5.2	Obiettivi raggiunti	18
5.3	Debolezze e limitazioni	19
5.4	Questioni irrisolte	19
5.5	Nuove domande emerse	19
5.6	Approcci alternativi	19
5.7	Impatto scientifico e pratico dei risultati	19
5.8	Riassunto del capitolo e conclusioni	19
6	LAVORI CORRELATI	20
6.1	Introduzione al capitolo	21
6.2	Panoramica sullo stato dell'arte	21
6.3	Lavori debolmente correlati	22
6.3.1	Lavoro debolmente correlato 1	22
6.3.2	Lavoro debolmente correlato 2	22
6.4	Lavori strettamente correlati	22
6.4.1	Lavoro strettamente correlato 1	23
6.4.2	Lavoro strettamente correlato 2	23
6.5	Tendenze identificate	23
6.6	Lacune nella letteratura e nostro contributo	23
6.7	Riassunto del capitolo e conclusioni	23
7	CONCLUSIONI	24
7.1	Riassunto della tesi	24
7.2	Sviluppi futuri	24
A	CODICI SORGENTE ADDIZIONALI	25
A.1	Introduzione all'appendice	25
A.2	Codice addizionale 1	25
A.3	Codice addizionale 2	25

A.4	Codice addizionale 3	25
B	DIMOSTRAZIONI ADDIZIONALI	26
B.1	Introduzione all'appendice	26
B.2	Dimostrazione addizionale 1	26
B.3	Dimostrazione addizionale 2	26
B.4	Dimostrazione addizionale 3	26
	Bibliografia	27

ACRONIMI

ELENCO DELLE FIGURE

ELENCO DELLE TABELLE

ELENCO DEI CODICI

INTRODUZIONE

Lo scopo principale di questo capitolo è presentare il problema di ricerca trattato, illustrare gli obiettivi della tesi e delineare una panoramica del suo contenuto [3].

L'introduzione, insieme alle conclusioni, rappresenta uno dei capitoli più importanti dell'intera tesi: molti lettori si concentreranno principalmente su questi due e daranno un'occhiata rapida alle figure e alle tabelle presenti nel resto del lavoro [4].

1.1 CONTESTO

Per prima cosa, come indicato sia da Pfandzelter et al. [3] che da Zobel [5], presenteremo l'area di ricerca che fa da sfondo al nostro lavoro di tesi. In questa sezione forniremo dunque una breve panoramica del particolare campo di studio, evidenziandone la rilevanza e le motivazioni per cui merita attenzione.

1.2 PROBLEMA AFFRONTATO

In secondo luogo, introdurremo lo specifico problema di ricerca che si vuole affrontare e, anche in questo caso, argomenteremo al fine di mettere in evidenza la sua importanza [5].

1.3 STATO DELL'ARTE

Successivamente, come suggerito da Zobel [5], riassumeremo in modo sintetico le soluzioni standard al problema affrontato, enfatizzando le limitazioni di queste soluzioni per far comprendere meglio le motivazioni dietro al nostro lavoro di ricerca.

1.4 DOMANDE DI RICERCA

In questa sezione elencheremo esplicitamente le domande di ricerca che guideranno il nostro studio, cioè le domande che identificano le lacune nelle conoscenze esistenti che cercheremo di colmare [3]. Ad ogni domanda identificata sarà associato un obiettivo che la nostra tesi si prefigge di raggiungere; tali obiettivi indicano cosa abbiamo intenzione di dimostrare, sviluppare, testare o esplorare.

Sarà appropriato introdurre le domande di ricerca nell'introduzione solo se risultano chiare anche senza aver prima esaminato i lavori precedenti; qualora ciò non fosse possibile, potrebbe essere opportuno posticipare la loro presentazione [6].

1.5 APPROCCIO USATO

A questo punto, specificheremo l'approccio seguito per risolvere il problema affrontato, fornendo una breve descrizione della soluzione proposta. Zobel [5] ci ricorda di menzionare eventuali articoli usati come base di partenza per il lavoro svolto e di evidenziare le motivazioni per cui la soluzione fornita può essere ritenuta efficace, trattando in modo succinto le tecniche usate per valutarla.

È in questa sezione che specifichiamo come abbiamo risposto alle domande di ricerca illustrando brevemente le tecniche, i processi e i metodi utilizzati per raggiungere i nostri obiettivi [3].

1.6 CONTRIBUTI ORIGINALI

In questa penultima sezione, metteremo in evidenza i contributi originali dati dal nostro lavoro di tesi alla specifica area di ricerca [3]: andremo quindi a illustrare sinteticamente i nuovi metodi, le teorie, i modelli o le implementazioni software introdotte dal nostro lavoro.

Se il lavoro presentato è parte di un progetto più grande, è importante specificare chiaramente quale sia stato il nostro particolare contributo a tale progetto [4].

1.7 STRUTTURA DELLA TESI

Per concludere, delineeremo la struttura della tesi: per ogni capitolo forniremo una breve descrizione del suo contenuto e del suo contributo al lavoro complessivo [4].

Seguendo l'approccio proposto da Pfandzelter et al. [3], il restante lavoro di tesi è strutturato nei seguenti capitoli:

- Capitolo 2 - PRELIMINARI: introduce le nozioni fondamentali per la comprensione del lavoro svolto e inquadra la tesi collegandola a eventuali lavori precedenti.
- Capitolo 3 - APPROCCIO: illustra l'idea risolutiva proposta per il problema affrontato.
- Capitolo 4 - VALUTAZIONE: dimostra, attraverso un processo di valutazione, l'efficacia dell'approccio risolutivo adottato.
- Capitolo 5 - DISCUSSIONE: conduce un'analisi critica e oggettiva dell'approccio e del metodo di valutazione utilizzati.
- Capitolo 6 - LAVORI CORRELATI: esamina le ricerche correlate mettendole a confronto con il lavoro realizzato.
- Capitolo 7 - CONCLUSIONI: riassume in modo conciso quanto svolto (concentrandosi principalmente sui risultati ottenuti) e suggerisce possibili sviluppi futuri.

Oltre ai capitoli principali, potremmo decidere di includere nella nostra tesi delle appendici; queste dovrebbero contenere materiale che, pur essendo necessario per comprendere il lavoro svolto, non rappresenta una parte centrale della tesi o non può essere inserito nel testo principale a causa delle sue dimensioni eccessive o del formato particolare [4].

Ad esempio, potremmo inserire come appendice: codici sorgente sviluppati; dimostrazioni matematiche articolate; tabelle e figure di grandi dimensioni; diagrammi complessi; descrizioni dettagliate di processi di misura, degli esperimenti condotti e dei risultati sperimentali ottenuti; manuali d'uso e di manutenzione redatti; sondaggi condotti con relativi risultati [4].

La tesi include, oltre ai capitoli, anche le seguenti appendici:

- Appendice A - CODICI SORGENTE ADDIZIONALI:
- Appendice B - DIMOSTRAZIONI ADDIZIONALI:

PRELIMINARI

Gli obiettivi di questo capitolo sono i seguenti:

- dimostrare che lo studente possiede una comprensione completa dell'area di ricerca in cui opera [3];
- fornire al lettore le nozioni avanzate¹ essenziali per la comprensione della tesi [5];
- inquadrare la tesi nel suo contesto, collegandola ai lavori precedenti, pubblicati o inediti, che costituiscono la base per il progetto svolto [7].

Alla luce di quanto detto, sarà necessario:

- introdurre concetti, definizioni e terminologia che verranno utilizzati nel resto della tesi [3];
- presentare i lavori che costituiscono il fondamento del nostro progetto [7];
- descrivere i metodi e le tecniche che formano la base del nostro lavoro [8];
- illustrare l'hardware e il software impiegato [8].

¹ In questo contesto, consideriamo come conoscenza comune tutto ciò che è stato trattato nei corsi obbligatori dello specifico corso di laurea [3].

2.1 INTRODUZIONE AL CAPITOLO

All'inizio di ogni capitolo includeremo una breve introduzione che fornisce contesto al capitolo stesso; questa introduzione faciliterà la transizione logica da un capitolo all'altro mostrando come quello corrente si colleghi ai precedenti [5].

Per essere più precisi, in ognuna di queste introduzioni forniremo [7]:

- gli obiettivi generali del capitolo, specificando cosa si intende affrontare e quale aspetto del nostro lavoro verrà esplorato;
- una spiegazione di come il capitolo corrente si inserisca nel contesto più ampio della tesi, collegandolo ai temi generali e agli obiettivi più ampi del nostro lavoro;
- un breve riassunto di come si è concluso il capitolo precedente e come quello corrente si costruisce sulle fondamenta del primo (ciò va fatto solo se pertinente);
- un sommario del contenuto del capitolo, fornendo, ad esempio, una concisa panoramica delle sezioni e sottosezioni presenti.

2.2 NOZIONI PRELIMINARI

Iniziamo con l'introduzione di concetti, definizioni e teorie fondamentali che costituiscono le basi del nostro lavoro. Questa sezione potrebbe includere, ad esempio, modelli matematici e teoremi essenziali per la comprensione della tesi.

È importante tenere a mente che non stiamo scrivendo un libro di testo: ogni volta che introduciamo un termine o un concetto sarà sufficiente fornirne una breve spiegazione e includere un riferimento bibliografico; in tal modo il lettore potrà approfondire autonomamente l'argomento [4].

Di seguito elenchiamo le fonti per le nozioni preliminari.

- Piattaforme bug bounty:
 - TO DO
- Blockchain, Ethereum e Solidity:
 - *"Mastering Ethereum: Building Smart Contracts and DApps"* [9];

- *"Solidity Documentation - Release 0.8.18"* [10];
- *"Ethereum Development Documentation"* [11]
- Verifica formale di smart contract Solidity:
 - TO DO
- Fair exchange protocol:
 - TO DO

2.3 LAVORI PRECEDENTI

Successivamente, se la tesi è una diretta continuazione di articoli o progetti di ricerca preesistenti, esporremo questi lavori evidenziando come la nostra ricerca si sviluppi a partire dalle loro fondamenta.

Elenco dei lavori precedenti:

- *"VeriOSS: Using the Blockchain to Foster Bug Bounty Programs"* [12];
- *"Verifying a Blockchain-Based Remote Debugging Protocol for Bug Bounty"* [13];

2.4 METODI E TECNICHE UTILIZZATE

In questa sezione descriveremo i metodi e le tecniche adottate nel corso della tesi, quali le analisi statistiche o i metodi di sviluppo software utilizzati per portare avanti il nostro progetto.

Nel caso di un progetto implementativo, descriveremo la metodologia di sviluppo impiegata (es. Agile, Waterfall, TDD, BDD) e come questa abbia influenzato il processo di implementazione.

2.5 TECNOLOGIE UTILIZZATE

Concludiamo il capitolo presentando le tecnologie, inclusi gli strumenti software e hardware, impiegati nella nostra ricerca, spiegando il loro ruolo e come hanno contribuito al raggiungimento degli obiettivi della tesi.

Nel caso di un progetto implementativo, in questa sezione elencheremo i linguaggi di programmazione, i framework, i database e altri strumenti utilizzati per lo sviluppo e il test del software. Ogni scelta andrà motivata illustrando quali sono i vantaggi per il nostro progetto.

2.6 RIASSUNTO DEL CAPITOLO E CONCLUSIONI

Alla fine di ogni capitolo includeremo un breve riassunto del suo contenuto, una riflessione su come quanto trattato contribuisca agli obiettivi generali della tesi e, per concludere, un'anticipazione di come i capitoli successivi faranno uso di quanto introdotto in quello corrente (in tal modo metteremo in evidenza come questi sono tra loro collegati) [5].

APPROCCIO

Questo è il primo dei due capitoli centrali in cui descriviamo il lavoro progettuale svolto. Il suo obiettivo principale è rispondere alla domanda: *"Come abbiamo risolto il problema di ricerca affrontato?"* [3].

Sarà qui che presenteremo, tramite una descrizione ad alto livello, la nostra idea risolutiva. A seconda della natura del problema affrontato, potremmo dunque trovarci a descrivere la progettazione di uno studio comparativo, l'architettura di un nuovo sistema, un nuovo algoritmo per la soluzione di un problema irrisolto oppure un algoritmo noto, ma che risolve un problema nuovo [3].

Di norma, se la nostra domanda di ricerca è del tipo *"Come posso risolvere questo problema?"*, la soluzione proposta dovrà essere presentata senza illustrare il processo iterativo che ci ha portato alla sua formulazione [3]. La situazione cambia se la domanda di ricerca è *"Quale tra i vari approcci noti è il migliore?"*: in questo caso, descriveremo come intendiamo eseguire il nostro studio comparativo, inserendo una descrizione dettagliata dei singoli approcci nel capitolo sulle nozioni preliminari [3].

La struttura di questo capitolo sarà fortemente influenzata dal tipo di progetto intrapreso e generalmente coprirà le prime fasi del suo sviluppo [7]: per un progetto implementativo, includeremo la specifica dei requisiti e una descrizione ad alto livello del design del software, facendo uso di strumenti come pseudocodice o diagrammi di flusso per facilitarne la comprensione.

3.1 INTRODUZIONE AL CAPITOLO

All'inizio di ogni capitolo includeremo una breve introduzione che fornisce contesto al capitolo stesso; questa introduzione faciliterà la transizione logica da un capitolo all'altro mostrando come quello corrente si colleghi ai precedenti [5].

Per essere più precisi, in ognuna di queste introduzioni forniremo [7]:

- gli obiettivi generali del capitolo, specificando cosa si intende affrontare e quale aspetto del nostro lavoro verrà esplorato;
- una spiegazione di come il capitolo corrente si inserisca nel contesto più ampio della tesi, collegandolo ai temi generali e agli obiettivi più ampi del nostro lavoro;
- un breve riassunto di come si è concluso il capitolo precedente e come quello corrente si costruisce sulle fondamenta del primo (ciò va fatto solo se pertinente);
- un sommario del contenuto del capitolo, fornendo, ad esempio, una concisa panoramica delle sezioni e sottosezioni presenti.

3.2 SPECIFICA DEI REQUISITI

In questa sezione verranno elencati i requisiti funzionali e non funzionali del nostro progetto implementativo. Specificheremo, in sostanza, cosa il nostro sistema è tenuto a fare, ma non come lo andrà a fare [14].

3.2.1 *Requisiti funzionali*

I requisiti funzionali specificano le funzionalità che il sistema dovrà essere in grado di eseguire. Questi requisiti delineano gli input e gli output, le funzioni eseguite dal sistema e i dati che esso deve gestire. Sono inclusi anche i dettagli sulle interfacce utente e le interazioni tra il sistema e altri sistemi [15].

3.2.2 *Requisiti non funzionali*

I requisiti non funzionali descrivono le caratteristiche qualitative generali del sistema software. Questi comprendono aspetti come le prestazioni, l'usabilità, la sicurezza, l'affidabilità, la disponibilità, la manutenibilità e la portabilità. Includono anche i vincoli entro cui ci si aspetta che il sistema finale operi, quali il sistema operativo, la velocità di elaborazione, la larghezza di banda della rete, la capacità di memoria e il linguaggio di programmazione utilizzato [15].

3.3 ARCHITETTURA DEL SISTEMA

In questa sezione descriviamo l'architettura del sistema software che intendiamo implementare.

3.3.1 *Design architetturale del sistema*

Illustreremo, anzitutto, la struttura del nostro sistema, evidenziando le relazioni tra i vari sottosistemi che lo compongono. Ci concentreremo su una visione ad alto livello, evitando di addentrarci eccessivamente nei dettagli specifici; per far ciò, forniremo una descrizione generale di come le responsabilità siano state suddivise e assegnate alle diverse componenti e di come queste interagiscono tra loro per realizzare le funzionalità desiderate. Al fine di rendere la trattazione più chiara, includeremo una rappresentazione visiva dell'architettura del sistema, utilizzando, ad esempio, un diagramma UML [16].

3.3.2 *Componente 1 del sistema*

Per ogni componente del sistema, forniremo un'analisi dettagliata delle sue responsabilità e delle sue interfacce di input e di output. Presenteremo, ove necessario, una descrizione dei suoi aspetti algoritmici e, inoltre, analizzeremo il modo in cui essa interagisce con le altre componenti, utilizzando ad esempio dei sequence diagram per illustrare ciascun caso d'uso [16].

Responsabilità

Interfacce

Dettagli algoritmici

Comportamento dinamico

3.3.3 *Componente n del sistema*

Responsabilità

Interfacce

Dettagli algoritmici

Comportamento dinamico

3.3.4 *Considerazioni sulle scelte architettureali*

In questa sezione spieghiamo le ragioni che hanno guidato la decomposizione del sistema nelle sue componenti [16]. Evidenzieremo, inoltre, eventuali misure di sicurezza integrate nell'architettura e strategie impiegate per assicurare prestazioni efficienti.

3.4 RIASSUNTO DEL CAPITOLO E CONCLUSIONI

Alla fine di ogni capitolo includeremo un breve riassunto del suo contenuto, una riflessione su come quanto trattato contribuisca agli obiettivi generali della tesi e, per concludere, un'anticipazione di come i capitoli successivi faranno uso di quanto introdotto in quello corrente (in tal modo metteremo in evidenza come questi sono tra loro collegati) [5].

VALUTAZIONE

Questo è il secondo dei due capitoli centrali in cui descriviamo il lavoro progettuale svolto. Il suo obiettivo principale è dimostrare, attraverso un processo di valutazione, l'efficacia dell'approccio risolutivo presentato nel capitolo precedente [3].

Il metodo di valutazione scelto dipenderà dalla specifica domanda di ricerca; alcuni metodi che potremmo adottare sono i seguenti [3]:

- **Implementazione:** nel caso in cui abbiamo progettato l'architettura di un nuovo sistema, possiamo dimostrarne la validità fornendo una sua implementazione; in tal caso, è essenziale che questa sia accompagnata da dei test che ne verifichino il comportamento o da dei benchmark che ne attestino il miglioramento rispetto a soluzioni esistenti.
- **Verifica formale:** forniamo una dimostrazione formale della correttezza del nostro approccio.
- **Simulazione:** testare la soluzione proposta in un ambiente controllato può essere un metodo efficace per valutarla; per esempio, potremmo creare un ambiente simulato per eseguire il nostro algoritmo o sistema; se scegliamo questa via, sarà cruciale definire accuratamente cosa misurare durante la simulazione al fine di ottenere dei risultati significativi.

In sostanza, a seconda del metodo di valutazione scelto, dovremo presentare: i risultati sperimentali; i teoremi e le relative dimostrazioni; l'analisi dei dati e le scoperte fatte [5].

La struttura di questo capitolo, esattamente come quella del precedente, dipenderà dal tipo di progetto intrapreso e, in genere, tratterà le fasi conclusive del suo sviluppo [7]: in un progetto implementativo,

presentiamo una discussione dettagliata dell'implementazione e delle sue criticità, includendo anche una descrizione dei test eseguiti.

4.1 INTRODUZIONE AL CAPITOLO

All'inizio di ogni capitolo includeremo una breve introduzione che fornisce contesto al capitolo stesso; questa introduzione faciliterà la transizione logica da un capitolo all'altro mostrando come quello corrente si colleghi ai precedenti [5].

Per essere più precisi, in ognuna di queste introduzioni forniremo [7]:

- gli obiettivi generali del capitolo, specificando cosa si intende affrontare e quale aspetto del nostro lavoro verrà esplorato;
- una spiegazione di come il capitolo corrente si inserisca nel contesto più ampio della tesi, collegandolo ai temi generali e agli obiettivi più ampi del nostro lavoro;
- un breve riassunto di come si è concluso il capitolo precedente e come quello corrente si costruisce sulle fondamenta del primo (ciò va fatto solo se pertinente);
- un sommario del contenuto del capitolo, fornendo, ad esempio, una concisa panoramica delle sezioni e sottosezioni presenti.

4.2 IMPLEMENTAZIONE

In questa sezione presenteremo un'analisi dettagliata dell'implementazione del sistema illustrato nel capitolo precedente.

4.2.1 *Implementazione componente 1*

Per ogni componente implementata, forniremo, anzitutto, una descrizione accurata delle sue sotto-componenti e delle risorse che usa o gestisce; dopodiché, spiegheremo come essa esegua i compiti necessari per adempiere alle proprie responsabilità.

4.2.2 *Implementazione componente n*

4.2.3 *Sfide implementative e soluzioni*

Illustreremo eventuali sfide incontrate durante il processo di implementazione e come queste siano state superate.

4.3 TEST

In questa sezione descriviamo i test effettuati per verificare che il sistema si comporti nel modo atteso.

4.3.1 *Test d'unità*

L'obiettivo dei test d'unità è verificare che le singole componenti funzionino correttamente quando isolate dal resto del sistema [17].

Test componente 1

Test componente n

4.3.2 *Test d'integrazione*

L'obiettivo dei test d'integrazione è verificare che due o più componenti del sistema, già testate individualmente in isolamento, continuino a funzionare correttamente una volta messe insieme e fatte interagire [17].

Test integrazione componenti 1 e 2

Test integrazione componenti n-1 e n

4.3.3 *Test end-to-end*

L'obiettivo dei test end-to-end è verificare che il nostro sistema operi correttamente durante l'interazione con un suo client, sia esso umano o un'altra applicazione, attraverso le interfacce fornite [17].

4.4 QUALITÀ DEI TEST

Descriviamo i metodi e le tecniche impiegati per valutare la qualità dei nostri test.

4.4.1 *Test coverage*

Illustreremo la metodologia adottata per monitorare il test coverage, ovvero la percentuale di linee di codice di ogni singola componente eseguite durante i test. Più alto sarà il test coverage e più bassa sarà la probabilità che la componente contenga dei bug non rilevati dai test [17].

È buona norma puntare a raggiungere un test coverage del 100%, utilizzando unicamente i test d'unità per la specifica componente; tuttavia, un coverage completo non garantisce di per sé la correttezza dei test (è condizione necessaria, ma non sufficiente): ci dice solamente che tutte le linee di codice sono state eseguite, ma non se le asserzioni dei test sono esaustive e appropriate [17].

4.4.2 *Mutation testing*

Per aumentare la fiducia nella qualità dei nostri test, possiamo utilizzare un framework di mutation testing per introdurre mutazioni nelle componenti testate e verificare che i nostri test d'unità rilevino queste mutazioni (fallendo) [17].

Dato che il mutation testing è un processo che richiede tempo, di solito viene utilizzato per valutare unicamente i test d'unità delle componenti che contengono la logica del sistema [17].

4.5 RISULTATI

In questa sezione illustriamo in modo chiaro e conciso quali sono i risultati ottenuti dalla nostra ricerca, evitando, almeno per il momento, qualsiasi tipologia di analisi critica [6].

Nel contesto di un progetto implementativo, presenteremo, anzitutto, una sintesi dei risultati ottenuti dai test. Dopodiché, illustreremo come l'implementazione realizzata soddisfi i requisiti specificati nel capitolo precedente e evidenzieremo i risultati chiave relativi alle prestazioni, alla scalabilità e alla manutenibilità del sistema.

4.6 RIASSUNTO DEL CAPITOLO E CONCLUSIONI

Alla fine di ogni capitolo includeremo un breve riassunto del suo contenuto, una riflessione su come quanto trattato contribuisca agli obiettivi generali della tesi e, per concludere, un'anticipazione di come i capitoli successivi faranno uso di quanto introdotto in quello corrente (in tal modo metteremo in evidenza come questi sono tra loro collegati) [5].

DISCUSSIONE

Questo capitolo si focalizza sull'analisi critica e obiettiva del lavoro svolto, esaminando sia l'approccio risolutivo al problema affrontato sia il metodo di valutazione impiegato per dimostrarne l'efficacia [3].

Per condurre questa analisi possiamo lasciarci guidare dalle successive domande [5]:

- In cosa il lavoro ha avuto successo?
- E in cosa invece ha fallito?
- Quali problemi non sono stati risolti?
- Quali nuove domande sono emerse?
- Quali approcci alternativi avremmo potuto considerare?
- Quali sono le implicazioni dei risultati ottenuti?

Altre domande che possono venirci in aiuto sono le seguenti [4]:

- I risultati ottenuti corrispondono agli obiettivi iniziali?
- Siamo riusciti a rispondere alle nostre domande di ricerca?
- Qual'è l'importanza scientifica e pratica dei risultati ottenuti?

Inizieremo, quindi, l'analisi valutando se i risultati ottenuti corrispondono agli obiettivi prefissati della nostra ricerca e se abbiamo efficacemente risposto alle domande di ricerca poste. Successivamente, valuteremo le debolezze e le limitazioni del nostro lavoro, esplorando anche le questioni ancora aperte, le nuove domande emerse e gli eventuali approcci alternativi che avremmo potuto esplorare. Concluderemo discutendo

l'importanza scientifica e pratica dei nostri risultati, evidenziando come questi possano essere applicati nella pratica e contribuire alle teorie esistenti.

Se ritenuto necessario, questo capitolo può essere convertito in una sezione del capitolo conclusivo; tale sezione andrebbe posizionata subito dopo il riassunto della tesi [5].

5.1 INTRODUZIONE AL CAPITOLO

All'inizio di ogni capitolo includeremo una breve introduzione che fornisce contesto al capitolo stesso; questa introduzione faciliterà la transizione logica da un capitolo all'altro mostrando come quello corrente si colleghi ai precedenti [5].

Per essere più precisi, in ognuna di queste introduzioni forniremo [7]:

- gli obiettivi generali del capitolo, specificando cosa si intende affrontare e quale aspetto del nostro lavoro verrà esplorato;
- una spiegazione di come il capitolo corrente si inserisca nel contesto più ampio della tesi, collegandolo ai temi generali e agli obiettivi più ampi del nostro lavoro;
- un breve riassunto di come si è concluso il capitolo precedente e come quello corrente si costruisce sulle fondamenta del primo (ciò va fatto solo se pertinente);
- un sommario del contenuto del capitolo, fornendo, ad esempio, una concisa panoramica delle sezioni e sottosezioni presenti.

5.2 OBIETTIVI RAGGIUNTI

In questa sezione valuteremo se i risultati ottenuti corrispondono agli obiettivi prefissati e se siamo riusciti a rispondere alle nostre domande di ricerca.

Non sarà necessario illustrare nuovamente i risultati in quanto questi dovrebbero già essere stati trattati nel capitolo *Valutazione* [3].

5.3 DEBOLEZZE E LIMITAZIONI

Valutiamo le debolezze e le limitazioni del nostro lavoro.

5.4 QUESTIONI IRRISOLTE

Illustriamo eventuali questioni irrisolte.

5.5 NUOVE DOMANDE EMERSE

Evidenziamo le nuove domande che sono emerse dalla ricerca svolta.

5.6 APPROCCI ALTERNATIVI

Trattiamo approcci alternativi che avremmo potuto prendere in considerazione.

5.7 IMPATTO SCIENTIFICO E PRATICO DEI RISULTATI

Discutiamo infine dell'importanza scientifica e pratica dei risultati ottenuti, riflettendo sulle loro potenziali implicazioni e ripercussioni. Considereremo, quindi, come questi risultati possano essere applicati nella pratica o contribuire a teorie esistenti.

Per scrivere questa sezione, possiamo provare a rispondere alla seguente domanda: "Quali lezioni o scoperte fatte durante il nostro lavoro di ricerca possono essere applicate in altri contesti?" [6].

5.8 RIASSUNTO DEL CAPITOLO E CONCLUSIONI

Alla fine di ogni capitolo includeremo un breve riassunto del suo contenuto, una riflessione su come quanto trattato contribuisca agli obiettivi generali della tesi e, per concludere, un'anticipazione di come i capitoli successivi faranno uso di quanto introdotto in quello corrente (in tal modo metteremo in evidenza come questi sono tra loro collegati) [5].

LAVORI CORRELATI

L'obiettivo di questo capitolo è di sottolineare l'originalità e la rilevanza del nostro lavoro di tesi rispondendo alle seguenti domande chiave [18]:

- Quali sono le origini delle nostre idee?
- Sono state pubblicate o proposte idee simili precedentemente?
- Quali sono gli aspetti originali del nostro lavoro?

In sostanza, il capitolo serve a mostrare che non ci siamo limitati a reinventare la ruota [4]. Per far ciò, esamineremo altri studi presenti in letteratura che cercano di risolvere lo stesso problema di ricerca o uno correlato [3], mettendo in evidenza le similitudini e le differenze rispetto al nostro approccio [4].

Ogni lavoro correlato verrà affrontato separatamente seguendo questa metodologia: [3]:

1. riassumiamo l'idea principale dello studio;
2. analizziamo i punti di forza, le limitazioni e i difetti (anche in confronto con il nostro approccio);
3. evidenziamo se e come il nostro studio sia stato influenzato dal lavoro esaminato.

Tireremo le fila dell'analisi evidenziando se emergono delle tendenze e identificando sia l'approccio più diffuso sia quello raccomandato per affrontare il problema di ricerca in questione. Per concludere, sottolineeremo le nuove conoscenze prodotte dal nostro lavoro di ricerca [4].

Sebbene questo capitolo possa essere posizionato sia dopo i preliminari teorici e tecnici sia prima delle conclusioni, seguendo il consiglio

di Pfandzelter et al. [3], la seconda opzione è preferibile per evitare di presentare i lavori correlati prima che il lettore abbia acquisito una piena comprensione dell'approccio utilizzato nel nostro lavoro di tesi. Alternativamente, se l'analisi dei lavori correlati è sufficientemente breve, può essere direttamente integrata nel capitolo sui preliminari o in quello contenente la discussione [6].

6.1 INTRODUZIONE AL CAPITOLO

All'inizio di ogni capitolo includeremo una breve introduzione che fornisce contesto al capitolo stesso; questa introduzione faciliterà la transizione logica da un capitolo all'altro mostrando come quello corrente si colleghi ai precedenti [5].

Per essere più precisi, in ognuna di queste introduzioni forniremo [7]:

- gli obiettivi generali del capitolo, specificando cosa si intende affrontare e quale aspetto del nostro lavoro verrà esplorato;
- una spiegazione di come il capitolo corrente si inserisca nel contesto più ampio della tesi, collegandolo ai temi generali e agli obiettivi più ampi del nostro lavoro;
- un breve riassunto di come si è concluso il capitolo precedente e come quello corrente si costruisce sulle fondamenta del primo (ciò va fatto solo se pertinente);
- un sommario del contenuto del capitolo, fornendo, ad esempio, una concisa panoramica delle sezioni e sottosezioni presenti.

6.2 PANORAMICA SULLO STATO DELL'ARTE

In questa sezione descriviamo i progressi e le scoperte principali compiute fino ad oggi nel campo di ricerca pertinente al nostro lavoro, stabilendo così il contesto per l'analisi dei lavori correlati.

6.3 LAVORI DEBOLMENTE CORRELATI

Procediamo con un'analisi dei lavori che hanno un legame indiretto o generale con il problema di ricerca che stiamo affrontando.

6.3.1 *Lavoro debolmente correlato 1*

Idea principale

Punti di forza

Limitazioni e difetti

Influenza sul nostro lavoro

6.3.2 *Lavoro debolmente correlato 2*

Idea principale

Punti di forza

Limitazioni e difetti

Influenza sul nostro lavoro

6.4 LAVORI STRETTAMENTE CORRELATI

Esaminiamo poi in dettaglio i lavori che si propongono di risolvere il problema di ricerca da noi affrontato e che adottano un approccio simile al nostro.

Elenchiamo i lavori strettamente correlati che andremo ad analizzare:

- *"Decentralized Security Bounty Management on Blockchain and IPFS" [19];*
- *"Bountychain: Toward Decentralizing a Bug Bounty Program with Blockchain and IPFS" [20];*
- *"Blockchain-Based Bug Bounty Framework" [21];*
- *Automated Responsible Disclosure of Security Vulnerabilities [22];*

6.4.1 *Lavoro strettamente correlato 1*

Idea principale

Punti di forza

Limitazioni e difetti

Influenza sul nostro lavoro

6.4.2 *Lavoro strettamente correlato 2*

Idea principale

Punti di forza

Limitazioni e difetti

Influenza sul nostro lavoro

6.5 TENDENZE IDENTIFICATE

Evidenziamo le eventuali tendenze emerse a seguito dell'analisi dei lavori correlati e identifichiamo sia l'approccio più diffuso sia quello raccomandato per affrontare il particolare problema di ricerca.

6.6 LACUNE NELLA LETTERATURA E NOSTRO CONTRIBUTO

Identifichiamo le lacune nella letteratura esistente e mostriamo come il nostro lavoro miri a colmarle, mettendo in tal modo in evidenza il contributo originale apportato dalla nostra ricerca.

6.7 RIASSUNTO DEL CAPITOLO E CONCLUSIONI

Alla fine di ogni capitolo includeremo un breve riassunto del suo contenuto, una riflessione su come quanto trattato contribuisca agli obiettivi generali della tesi e, per concludere, un'anticipazione di come i capitoli successivi faranno uso di quanto introdotto in quello corrente (in tal modo metteremo in evidenza come questi sono tra loro collegati) [5].

CONCLUSIONI

Il capitolo conclusivo, insieme all'introduzione, rappresenta uno dei capitoli più importanti dell'intera tesi: molti lettori si concentreranno principalmente su questi due e daranno un'occhiata rapida alle figure e alle tabelle presenti nel resto del lavoro [4].

7.1 RIASSUNTO DELLA TESI

Il capitolo conclusivo della tesi si apre comunemente con un riassunto sintetico del lavoro svolto che si sofferma soprattutto sui risultati chiave raggiunti [8]. Questa sezione dovrà quindi contenere:

1. un riepilogo del problema indagato [3];
2. una descrizione essenziale del metodo adottato per risolverlo [3];
3. una sintesi dei risultati conseguiti [5] e del contributo fornito dal nostro lavoro di tesi [18].

7.2 SVILUPPI FUTURI

È essenziale dedicare una sezione alla prospettiva di ulteriori ricerche che possano estendere o approfondire lo studio presente. Questa parte dovrebbe concentrarsi principalmente sugli aspetti ancora da esplorare, piuttosto che sulle metodologie da adottare [8]. Potrebbe includere, per esempio, proposte non implementate in questa tesi o strategie per superare le limitazioni e le debolezze individuate [3].



CODICI SORGENTE ADDIZIONALI

Le appendici dovrebbero includere materiale che, pur essendo necessario per comprendere il lavoro svolto, non rappresenta una parte centrale della tesi o non può essere inserito nel testo principale a causa delle sue dimensioni eccessive o del formato particolare [4].

A.1 INTRODUZIONE ALL'APPENDICE

Poiché è possibile che il lettore consulti le appendici senza aver letto integralmente la tesi, è consigliabile includere in ognuna di queste una breve introduzione che ne descriva il contenuto e che la collochi nel contesto più ampio del lavoro svolto [4].

A.2 CODICE ADDIZIONALE 1

A.3 CODICE ADDIZIONALE 2

A.4 CODICE ADDIZIONALE 3

DIMOSTRAZIONI ADDIZIONALI

Le appendici dovrebbero includere materiale che, pur essendo necessario per comprendere il lavoro svolto, non rappresenta una parte centrale della tesi o non può essere inserito nel testo principale a causa delle sue dimensioni eccessive o del formato particolare [4].

B.1 INTRODUZIONE ALL'APPENDICE

Poiché è possibile che il lettore consulti le appendici senza aver letto integralmente la tesi, è consigliabile includere in ognuna di queste una breve introduzione che ne descriva il contenuto e che la collochi nel contesto più ampio del lavoro svolto [4].

B.2 DIMOSTRAZIONE ADDIZIONALE 1

B.3 DIMOSTRAZIONE ADDIZIONALE 2

B.4 DIMOSTRAZIONE ADDIZIONALE 3

BIBLIOGRAFIA

- [1] Paul Valéry: *Il cimitero marino*. Interlinea edizioni, 2016, ISBN 9788868570880. Pubblicato per la prima volta nel 1920 con il titolo *Le Cimetière marin*. (Cited on page iii.)
- [2] Donald E. Knuth: *Theory and practice*. Theoretical Computer Science (Elsevier), vol. 90 (no. 1): pp. 1–15, 1991. [https://doi.org/10.1016/0304-3975\(91\)90295-D](https://doi.org/10.1016/0304-3975(91)90295-D). (Cited on page iv.)
- [3] Tobias Pfandzelter, Martin Grambow, Trever Schirmer e David Bermbach: *Writing a Computer Science Thesis*. Pubblicato dal gruppo di ricerca *Mobile Cloud Computing* della *TU Berlin* sulla pagina web del gruppo, dicembre 2022. <https://github.com/pfandzelter/thesis-tips>. (Cited on pages 1, 2, 3, 4, 8, 12, 17, 18, 20, 21, and 24.)
- [4] *Guide to Writing a Thesis in Technical Fields*. Pubblicato dalla *Tampere University* sulla pagina web dedicata alla tesi per i corsi magistrali in ambito tecnologico, gennaio 2019. https://content-webapi.tuni.fi/proxy/public/2019-10/tau-thesis_guide_for_technical_fields_2019_version-3-1.pdf. (Cited on pages 1, 2, 3, 5, 17, 20, 24, 25, and 26.)
- [5] Justin Zobel: *Writing for Computer Science*. Springer Publishing Company, terza edizione, 2015, ISBN 1447166388. <https://doi.org/10.1007/978-1-4471-6639-9>. (Cited on pages 1, 2, 4, 5, 7, 8, 11, 12, 13, 16, 17, 18, 19, 21, 23, and 24.)
- [6] Tomi Männistö, Juha Tiihonen e Fabian Fagerholm: *Scientific Writing - Guide of the Empirical Software Engineering Research Group of the University of Helsinki*. Pubblicato dall'*Empirical Software Engineering Research Group* della *Università di Helsinki* sulla pagina web del gruppo, novembre 2022. <https://www.cs.helsinki.fi/group/ese/ScientificWritingGuide.pdf>. (Cited on pages 2, 15, 19, and 21.)
- [7] *Master in Computer Science - Guidelines for the Thesis*. Pubblicato dalla *Libera Università di Bolzano* sulla pagina web dedicata alla tesi per i corsi magistrali affini all'informatica, 2022. <https://guide.unibz.it/assets/graduation/Computer-Science/>

- Master/Guidelines-Thesis-Master-2022.pdf. (Cited on pages 4, 5, 8, 9, 12, 13, 18, and 21.)
- [8] *Writing Your Thesis*. Pagina web dedicata alle linee guida per la tesi presente sul sito del laboratorio *Computer Science 7 (Computer Networks and Communication Systems)* della *Friedrich-Alexander Universität*. <https://www.cs7.tf.fau.eu/teaching/student-theses/writing-your-thesis/>, consultata in data 16 novembre 2023. (Cited on pages 4 and 24.)
- [9] Andreas M. Antonopoulos e Gavin Wood: *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly, prima edizione, dicembre 2018, ISBN 9781491971949. <https://github.com/ethereumbook/ethereumbook>. (Cited on page 5.)
- [10] The Solidity Authors: *Solidity Documentation - Release 0.8.18*, febbraio 2023. https://docs.soliditylang.org/_/downloads/en/v0.8.18/pdf/. (Cited on page 6.)
- [11] Ethereum Foundation: *Ethereum Development Documentation*. Documentazione online. <https://ethereum.org/developers/docs>, consultato in data 15 gennaio 2024. (Cited on page 6.)
- [12] Andrea Canidio, Gabriele Costa e Letterio Galletta: *VeriOSS: Using the Blockchain to Foster Bug Bounty Programs*. Nel *2nd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2020)*, volume 82 della serie *Open Access Series in Informatics (OASIs)*, pagine 6:1–6:14. Schloss Dagstuhl, Leibniz-Zentrum für Informatik, Germania, febbraio 2021. <https://doi.org/10.4230/OASIs.Tokenomics.2020.6>. (Cited on page 6.)
- [13] Pierpaolo Degano, Letterio Galletta e Selene Gerali: *Verifying a Blockchain-Based Remote Debugging Protocol for Bug Bounty*. Nel *Protocols, Strands, and Logic*, volume 13066 della serie *Lecture Notes in Computer Science*, pagine 124–138. Springer International Publishing, Cham, Svizzera, novembre 2021. https://doi.org/10.1007/978-3-030-91631-2_7. (Cited on page 6.)
- [14] William D. Shoaff: *How to Write a Master's Thesis in Computer Science*. Pubblicato sulla pagine web del Prof. Shoaff, ospitata sul sito del Dipartimento di Informatica del *Florida Institute of Technology*, agosto 2001. <https://cs.fit.edu/~wds/guides/howto/howto.html>. (Cited on page 9.)

- [15] Narayanan Subramanian: *Requirements specification and analysis*. Nel testo di Benjamin W. Wah (curatore): *Wiley Encyclopedia of Computer Science and Engineering, 5 Volume Set*, capitolo R. Wiley, febbraio 2009. (Cited on page 9.)
- [16] *Software Design Report*. Pubblicato sul sito del Dipartimento di Ingegneria Informatica della *Harran University*. https://web.harran.edu.tr/assets/uploads/other/files/bilgisayar/files/Software_Design_Document_Template.pdf, consultata in data 17 novembre 2023. (Cited on pages 10 and 11.)
- [17] Lorenzo Bettini: *Test-Driven Development, Build Automation, Continuous Integration with Java, Eclipse and friends*. Leanpub, febbraio 2021. <https://leanpub.com/tdd-buildautomation-ci>. (Cited on pages 14 and 15.)
- [18] Luca Aceto: *How to Write a Paper*. Slides pubblicate sulla pagina web dedicata ai consigli su come fare ricerca dell'*Icelandic Center of Excellence in Theoretical Computer Science*. <http://icetcs.ru.is/luca/howto-lectures/howtowrite-gssi.pdf>, consultata in data 17 novembre 2023. (Cited on pages 20 and 24.)
- [19] Alex Hoffman, Eric Becerril-Blas, Kevin Moreno e Yoohwan Kim: *Decentralized Security Bounty Management on Blockchain and IPFS*. Nel *10th Annual Computing and Communication Workshop and Conference (CCWC)*, pagine 241–247, Las Vegas, Nevada, USA, 2020. <https://www.doi.org/10.1109/CCWC47524.2020.9031109>. (Cited on page 22.)
- [20] Alex Hoffman, Phillipe Austria, Chol Hyun Park e Yoohwan Kim: *Bountychain: Toward Decentralizing a Bug Bounty Program with Blockchain and IPFS*. *International Journal of Networked and Distributed Computing* (Atlantis Press), vol. 9: pp. 86–93, luglio 2021. <https://doi.org/10.2991/ijndc.k.210527.001>. (Cited on page 22.)
- [21] Lital Badash, Nachiket Tapas, Asaf Nadler, Francesco Longo e Asaf Shabtai: *Blockchain-Based Bug Bounty Framework*. Nel *Proceedings of the 36th Annual ACM Symposium on Applied Computing (SAC '21)*, pagine 239–248, Repubblica di Corea (evento virtuale), 2021. <https://doi.org/10.1145/3412841.3441906>. (Cited on page 22.)

- [22] Andrea Lisi, Prateeti Mukherjee, Laura De Santis, Lei Wu, Dmitrij Lagutin e Yki Kortensniemi: *Automated Responsible Disclosure of Security Vulnerabilities*. IEEE Access, vol. 10: pp. 10472–10489, 2022. <https://www.doi.org/10.1109/ACCESS.2021.3126401>. (Cited on page 22.)

RINGRAZIAMENTI

<Ringraziamento 1>.

<Ringraziamento 2>.

<Ringraziamento 3>.

<Ringraziamento 4>.

<Ringraziamento 5>.