

UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE ED
ELETTRICA E MATEMATICA APPLICATA



Corso di Laurea Magistrale in Ingegneria Informatica

ReverseEkans

Nome	Cognome	Matricola	E-Mail	Responsabile
Giuseppe Alfonso	Mangiola	0622702372	g.mangiola1@studenti.unisa.it	WP1
Emanuele	Relmi	0622702368	e.relmi@studenti.unisa.it	WP2
Francesco	Quagliuolo	0622702412	f.quagliuolo@studenti.unisa.it	WP3

ANNO ACCADEMICO 2024/2025

INDICE

1	WORK PACKAGE 1	4
1.1	Descrizione del modello	4
1.2	Attori del Sistema	5
1.2.1	Utente	5
1.2.2	Venditori	5
1.2.3	La piattaforma di e-commerce	5
1.2.4	Validator della blockchain	6
1.3	Attaccanti del Sistema	6
1.4	Proprietà	10
1.4.1	Confidenzialità	11
1.4.2	Privacy	11
1.4.3	Integrità	12
1.4.4	Trasparenza	12
1.4.5	Efficienza	13
1.5	Completeness	13
2	WORK PACKAGE 2	15
2.1	Architettura generale del sistema	16
2.1.1	Componenti principali del sistema	16
2.1.2	Modalità di gestione della reputazione	17
2.2	Funzionamento delle parti oneste	18
2.2.1	Gestione utente e creazione del DID	18
2.2.2	Venditore	20
2.2.3	Interazione dell'utente con il sistema tramite DID	20

INDICE

2.3	Utilizzo di NFT come prova di acquisto	22
2.3.1	Emissione del token	22
2.3.2	Verifica e pubblicazione della recensione	23
2.3.3	NFT scaduti	23
2.3.4	Vantaggi della soluzione NFT	24
2.4	Uso delle Verifiable Credentials nel sistema	24
2.4.1	Emissione della Verifiable Credential	24
2.4.2	Presentazione e verifica	25
2.4.3	Gestione della Revoca delle VC	25
2.4.4	Privacy e Selective Disclosure	26
2.4.5	Compromesso tra sicurezza e costo	27
2.5	Gestione dei casi limite	27
2.5.1	Utenti inattivi	27
2.5.2	VC scadute o revocate	28
2.5.3	DID revocati o compromessi	28
2.5.4	Utente Bannato	28
2.6	Gestione del compromesso tra pseudo-anonimato e unicità dell'utente	29
2.6.1	Verifiable Credential univoca	29
2.6.2	DID multipli, ma dimostrabilmente unificati	29
2.6.3	Struttura della ZKP anti-Sybil	30
2.6.4	Risultato del compromesso	30
2.7	Smart Contract	30
2.7.1	Funzionalità implementate	30
2.8	Validator	31
2.8.1	Compiti principali	31
2.8.2	Assunzione di sicurezza	32
2.9	Modulo di Audit	32
2.9.1	Funzionalità	32
2.10	Scelta della blockchain permissionless	34
2.10.1	Ethereum vs Hyperledger Fabric	35
2.10.2	Innovazioni future	36
2.11	Utilizzo per l'utente (dApp)	37
2.12	Formalismi matematici crittografici	37
2.12.1	Generazione DID	37
2.12.2	Firma digitale	37
2.12.3	Verifiable Credential (VC)	37
2.12.4	Verifiable Presentation (VP)	38

INDICE

2.12.5	Revoca con bitstring	38
2.12.6	Zero-Knowledge Proof (ZKP)	38
2.12.7	Selective Disclosure con BBS+	39
2.13	Conclusione	39
3	WORK PACKAGE 3	40
4	WORK PACKAGE 4	41

CAPITOLO 1

WORK PACKAGE 1

In questo primo Work Package definiamo il modello di riferimento per il sistema decentralizzato di recensioni. Identifichiamo innanzitutto gli attori onesti coinvolti nel sistema, analizzando i loro obiettivi e le funzionalità che si intendono realizzare.

Gli attori onesti sono quegli individui o entità che agiscono in conformità con le regole e le politiche stabilite, cercando di raggiungere i loro obiettivi senza compromettere l'integrità del sistema. Successivamente, esamineremo i possibili avversari (o Threat Models) che potrebbero essere interessati a compromettere il sistema, esaminando le loro risorse e le motivazioni che li spingono ad agire. Questa analisi ci permetterà di identificare gli attacchi che il sistema potrebbe subire e di comprendere quali misure di sicurezza dovranno essere adottate per contrastarli. Una volta compreso il contesto in cui il sistema opera, identificheremo le proprietà di sicurezza che si vorrebbero preservare in presenza di attacchi. Queste proprietà sono fondamentali per garantire il corretto funzionamento del sistema e la protezione delle informazioni sensibili.

1.1 Descrizione del modello

Il sistema che intendiamo progettare mira a decentralizzare la gestione delle recensioni all'interno delle piattaforme di e-commerce, sfruttando una blockchain per garantire:

- autenticità delle recensioni
- trasparenza nell'ordinamento e nella visibilità delle recensioni
- immutabilità delle valutazioni una volta registrate (se non nelle condizioni di modifica/revoca definite)

- incentivazione alla partecipazione onesta

Gli utenti devono essere verificati come effettivi acquirenti di un determinato prodotto prima di poter rilasciare una recensione, le quali saranno poi memorizzate sulla blockchain. Il sistema prevede anche meccanismi anti-frode, come la prevenzione da account falsi e la penalizzazione dell'inattività o dei comportamenti manipolativi.

1.2 Attori del Sistema

1.2.1 Utente

Gli utenti acquirenti sono soggetti che effettuano acquisti reali tramite la piattaforma. Dopo aver completato una transazione, essi hanno il diritto di rilasciare una recensione sul prodotto acquistato. L'obiettivo dell'utente è condividere la propria esperienza di acquisto in modo onesto, contribuendo così a costruire una base di recensioni affidabili per la comunità. L'utente deve poter contare su un sistema che protegga la sua identità tramite forme di pseudo-anonimato, pur garantendo la verificabilità della sua legittimità come recensore effettivo. Inoltre, deve avere la possibilità di modificare o revocare la propria recensione secondo condizioni predefinite e di contribuire alla qualità del sistema tramite la pubblicazione di recensioni oneste e tempestive.

1.2.2 Venditori

I venditori sono attori che propongono prodotti all'interno del marketplace. Il loro interesse principale è ottenere feedback autentici sui propri articoli, che riflettano realmente la qualità dei beni offerti. Attraverso il sistema di recensioni decentralizzate, il venditore può migliorare la propria reputazione in modo trasparente e meritocratico. I venditori onesti si impegnano a non tentare di manipolare il sistema, né incentivando recensioni false, né ostacolando recensioni negative legittime.

1.2.3 La piattaforma di e-commerce

La piattaforma di e-commerce rappresenta l'interfaccia principale tramite cui avviene l'interazione tra utenti e prodotti. Essa si occupa di verificare localmente l'avvenuto acquisto e di emettere un attestato crittografico (NFT non trasferibile) che costituisce la Proof-of-Purchase (PoP), poi utilizzata per autorizzare la pubblicazione di recensioni. Inoltre, la piattaforma fornisce accesso agli smart contract e alla rete blockchain tramite la dApp, ma non controlla direttamente né l'ordinamento né la registrazione delle recensioni, che sono gestiti in modo autonomo e trasparente dalla logica on-chain. La piattaforma

deve essere progettata per non poter alterare la visibilità delle recensioni, garantendo l'imparzialità e la non manipolabilità del sistema.

1.2.4 Validator della blockchain

I validators sono attori fondamentali per il corretto funzionamento dell'infrastruttura blockchain su cui si basa il sistema di recensioni per l'e-commerce. Il loro compito consiste nel validare e inserire in blocchi le transazioni effettuate dagli utenti, tra cui l'inserimento delle recensioni e le eventuali revoche o modifiche autorizzate. Nel modello proposto, si assume che i validators si comportino in modo corretto, ovvero eseguano le operazioni previste dal protocollo di consenso in modo imparziale e senza manipolazioni. In particolare, si presume che i blocchi prodotti rispettino l'ordine temporale delle transazioni, che non vi siano censure arbitrarie e che le operazioni valide non vengano rifiutate. I validators onesti rappresentano la garanzia che le regole del sistema vengano applicate in modo coerente, assicurando proprietà fondamentali come l'immutabilità, la tracciabilità e la trasparenza dei dati memorizzati sulla blockchain.

1.3 Attaccanti del Sistema

Nel contesto del sistema descritto, è fondamentale analizzare e comprendere i potenziali attaccanti che potrebbero cercare di comprometterlo, considerando le motivazioni e le risorse a loro disposizione. Questi attori e gruppi di attaccanti rappresentano diverse minacce al sistema e richiedono misure di sicurezza specifiche per essere contrastati efficacemente.

- **Utente fraudolento**

- **Descrizione:** Si tratta di un avversario che cerca deliberatamente di compromettere l'affidabilità del sistema utilizzando una singola identità per inviare recensioni false o fuorvianti. Può tentare di ottenere un NFT senza aver realmente effettuato un acquisto (eg. tramite exploit della piattaforma o uso non autorizzato di NFT altrui), oppure utilizzare una Verifiable Credential compromessa o falsificata. Il suo obiettivo è alterare la reputazione dei prodotti senza possedere un diritto legittimo alla recensione.

- **Risorse**

- * Capacità tecniche medie per aggirare i meccanismi di verifica
- * Uso di NFT ottenuti fraudolentemente o riutilizzati
- * Possesso di VC rubate o mal rilasciate

- **Venditore malevolo**

- **Descrizione:** è un attore che, pur facendo parte legittimamente del sistema, tenta di manipolarne il funzionamento per aumentare artificialmente la propria reputazione. Può commissionare recensioni false a utenti fraudolenti o tentare di incentivare solo recensioni positive offrendo sconti o regali. Talvolta agisce anche in modo sleale contro concorrenti, cercando di sabotarne la reputazione con feedback negativi fittizi.

- **Risorse**

- * Budget economico per incentivare utenti malintenzionati
- * Reti di profili social o identità multiple
- * Accesso a piattaforme esterne per organizzare campagne coordinate

- **Attaccante Sybil**

- **Descrizione:** Un attaccante Sybil genera un gran numero di identità pseudo-anonime (DID) ciascuna associata a una Verifiable Credential apparentemente valida, con l'obiettivo di manipolare il sistema scrivendo più recensioni false, creando così un'impressione artificiale di consenso o popolarità.

- **Risorse**

- * Automazione per la creazione di molteplici DID e wallet
- * Accesso a più VC emesse fraudolentemente o a issuer compromessi
- * Capacità di orchestrare pubblicazioni multiple coordinate

- **Identity Thief**

- **Descrizione:** avversario che possiede o mira a rubare identità e/o credenziali per impersonare gli utenti legittimi e ottenere accesso non autorizzato ai servizi. Potrebbe utilizzare tecniche di phishing, furto di credenziali o exploit delle vulnerabilità per ottenere informazioni sensibili e assumere l'identità di altri utenti.

- **Risorse**

- * Disponibilità di risorse computazionali sufficienti per eseguire attacchi brute-force, decrittazione o altri metodi per ottenere informazioni sensibili o compromettere la sicurezza del sistema
- * Possesso di un vasto database di informazioni personali ottenute illegalmente, che consente la creazione di profili dettagliati delle vittime e di utilizzare le informazioni per scopi malevoli
- * Competenze nel phishing e nell'ingegneria sociale, capacità di creare siti web e messaggi convincenti

- **Insider malevolo**

- **Descrizione:** si tratta di un utente reale che ha accesso legittimo al sistema (acquirente o venditore), ma che sfrutta tale accesso per aggirare le regole, ad esempio vendendo le proprie credenziali. Può anche collaborare con un venditore per manipolare le recensioni in cambio di vantaggi.

- **Risorse**

- * Accesso autentico al sistema
- * Conoscenza delle regole di funzionamento
- * Comunicazioni private con altri attori coinvolti

- **Reviewer a pagamento**

- **Descrizione:** è un attore esterno che fornisce recensioni dietro compenso, fingendo esperienze d'acquisto mai avvenute. Opera in coordinamento con venditori maliziosi o agenzie di marketing scorrette. L'attività si basa sull'acquisizione o l'aggiramento delle prove d'acquisto (PoP), sfruttando identità multiple o strumenti per eludere i controlli anti-frode del sistema.

- **Risorse**

- * Identità multiple o prestanome
- * Esperienza nel mascherare pattern ripetitivi
- * Account acquistati o affittati già "invecchiati" per aggirare controlli

- **Validator corrotto**

- **Descrizione:** in una blockchain, i validators hanno il compito di includere o rifiutare transazioni. Un validator corrotto può censurare recensioni sgradite o includere solo quelle sponsorizzate, sabotando la neutralità del sistema.

- **Risorse**

- * Accesso diretto al consenso del sistema
- * Collusione con altri validatori o attori
- * Capacità di censura selettiva e invisibile

- **Venditore Collusivo Fuori Sistema**

- **Descrizione:** si tratta di un venditore che, pur operando apparentemente in modo regolare sulla piattaforma, contatta l'acquirente attraverso canali esterni (eg. email, social network, app di messaggistica) dopo l'acquisto, proponendo un rimborso parziale o totale in cambio di una recensione positiva. L'obiettivo di questo comportamento è quello di ottenere feedback favorevoli per migliorare

la propria reputazione pubblica, senza che l'incentivo illecito venga rilevato dal sistema di recensioni. Dal punto di vista del protocollo, la recensione appare autentica (l'utente ha realmente acquistato il prodotto), ma è in realtà distorta da un accordo economico privato non verificabile, che mina la trasparenza e l'affidabilità del sistema.

– **Risorse**

- * Accesso ai dati di contatto del cliente post-acquisto
- * Canali alternativi (email, social, chat) per negoziare incentivi non tracciabili
- * Capacità di effettuare rimborsi discreti tramite metodi esterni al sistema (PayPal, crypto, buoni regalo, ecc.)

• **Attaccante di tipo phishing/malware**

- **Descrizione:** un avversario che tenta di ottenere l'accesso alle chiavi private di un utente tramite phishing o malware. Compromette il controllo su wallet o dispositivi, può firmare transazioni arbitrarie, inviare recensioni fraudolente o riscattare incentivi legittimi altrui.

– **Risorse**

- * Capacità tecniche medie per creare pagine clone, app dannose o estensioni malevole.
- * Accesso a database di email/identità per campagne phishing mirate.
- * Malware per keylogging, intercettazione clipboard o inject di firma.

• **Issuer compromesso**

- **Descrizione:** un'entità formalmente affidabile (Issuer) che, a seguito di compromissione o comportamento malevolo, emette Verifiable Credentials (VC) false o duplicate. Queste credenziali possono essere utilizzate per creare account multipli o alterare l'equilibrio reputazionale del sistema.

– **Risorse**

- * Accesso al proprio sistema di emissione VC e alla chiave privata di firma.
- * Collaborazione con attori esterni che utilizzano le VC emesse.
- * Capacità di firmare VC formalmente valide ma semanticamente scorrette.

• **Attaccante passivo di rete**

- **Descrizione:** un osservatore che intercetta comunicazioni, come l'invio di una Verifiable Presentation, tra utente e smart contract. Se non viene usata una challenge o un nonce dinamico, può riutilizzare una presentazione firmata per

replicare un'azione (replay attack), anche senza accedere alla chiave privata dell'utente.

– **Risorse**

- * Capacità di intercettare pacchetti o monitorare traffico su canali insicuri.
- * Tool di replay automatico e scripting.
- * Accesso alla rete o a browser compromessi.

• **Analista comportamentale (Data Correlator)**

- **Descrizione:** attore passivo che, senza alterare il sistema, analizza in modo massivo metadati pubblici (timestamp, hash, CID IPFS, ecc.) per tentare di correlare le azioni di uno stesso utente su DID diversi, violando l'unlinkability. Può impiegare tecniche di fingerprinting, clustering temporale o analisi predittiva, agendo come "profilatore" degli utenti.

– **Risorse**

- * Accesso completo ai dati pubblici della blockchain e dei CID IPFS.
- * Competenze statistiche e di data mining.
- * Capacità di analisi AI per identificare pattern temporali e linguistici.

1.4 Proprietà

L'obiettivo di questo progetto è sviluppare un sistema di recensioni decentralizzato per l'e-commerce, capace di offrire un ambiente affidabile, trasparente e resistente a manipolazioni. Il sistema permette agli utenti di recensire prodotti soltanto dopo averne dimostrato l'acquisto tramite meccanismi di verifica e garantisce che tali recensioni siano pubblicate in modo immutabile e consultabile da tutti. Allo stesso tempo, è previsto il supporto per la modifica o revoca delle recensioni secondo condizioni predefinite con logiche di incentivazione/disincentivazione. Per garantire la robustezza del sistema in un ambiente basato su blockchain è necessario definire con precisione alcune proprietà fondamentali: confidenzialità, privacy (selective disclosure), integrità, trasparenza ed efficienza. Queste proprietà sono essenziali non solo per il corretto funzionamento del sistema in condizioni normali, ma anche per assicurare la resilienza rispetto a comportamenti malevoli, come la creazione di identità false, la compravendita di feedback o la manipolazione della visibilità delle recensioni. La loro implementazione costituisce la base per un modello credibile, meritocratico e decentralizzato di reputazione online.

1.4.1 Confidenzialità

- **C1:** L'identità reale dell'utente non deve essere associata pubblicamente alle recensioni espresse. Ogni interazione deve avvenire tramite identificatori pseudo-anonimi, eventualmente riconducibili all'utente solo in presenza di specifiche condizioni legali.
- **C2:** Tutte le comunicazioni tra client e piattaforma, comprese le operazioni di verifica d'acquisto (Proof-of-Purchase) e scrittura recensioni, devono avvenire tramite canali sicuri e cifrati (eg. TLS o crittografia applicativa end-to-end).
- **C3:** Il sistema deve ridurre al minimo i metadati esposti (eg. timestamp precisi, IP, pattern comportamentali) per evitare rischi di deanonimizzazione tramite tecniche di correlazione.
- **C4:** Il sistema deve evitare che le attività di uno stesso utente possano essere correlate tra loro nel tempo, a meno che l'utente stesso non lo autorizzi esplicitamente. Questo implica l'uso di tecniche come l'impiego di chiavi crittografiche diverse per ogni recensione. In questo modo si riduce il rischio di tracciamento comportamentale a lungo termine e si protegge ulteriormente il diritto alla riservatezza dell'utente.

1.4.2 Privacy

Il sistema impiega identificatori pseudo-anonimi (DID) e credenziali verificabili (VC) per proteggere l'identità dell'utente, garantendo che ogni interazione sia verificabile, ma non tracciabile. A tal fine, vengono rispettate le seguenti proprietà:

- **Minimizzazione dei dati (Minimization):** ogni transazione include solo le informazioni strettamente necessarie (eg. hash del contenuto, identificativo del token), evitando esposizione di dati personali o metadati sensibili.
- **Verificabilità condizionata (Predicate Disclosure):** l'utente può dimostrare di aver diritto a pubblicare una recensione (eg. possesso di NFT e VC valida), senza rivelare la propria identità reale né altri attributi non necessari.
- **Non tracciabilità (Unlinkability):** recensioni diverse inviate dallo stesso utente non sono collegabili tra loro, a meno che l'utente non decida volontariamente di accumulare reputazione aggregata (via prove ZKP). In tal caso, la verifica avviene in modo crittograficamente sicuro, senza comprometterne l'anonimato.
- **Non riutilizzabilità (Non-transferability):** ogni NFT può essere impiegato una sola volta per scrivere una recensione, impedendo la duplicazione o la cessione dei diritti di pubblicazione.

- **Non falsificabilità (Unforgeability):** ogni credenziale e ogni transazione è firmata digitalmente. Nessun utente può pubblicare una recensione senza possedere sia una VC valida che un NFT non scaduto o revocato.
- **Protezione contro correlazioni (Untraceability):** il sistema impiega DID diversi e rotabili per ogni interazione e minimizza i timestamp visibili, impedendo correlazioni tra recensioni inviate dallo stesso utente.
- **Resistenza alla sorveglianza passiva (Unobservability):** anche osservando il traffico blockchain o IPFS, un attore esterno non può inferire legami tra utenti, recensioni e reputazione, grazie all'uso di hash, CID e metadati minimizzati.

Queste proprietà derivano da una progettazione orientata alla privacy e all'autonomia dell'utente, ispirata ai principi del paradigma Self-Sovereign Identity e alle tecniche di presentazione selettiva delle credenziali (*Selective Disclosure*).

1.4.3 Integrità

- **I1:** Ogni recensione deve essere immutabile una volta pubblicata, salvo condizioni specifiche di modifica o revoca definite a livello di smart contract.
- **I2:** Solo utenti che hanno effettivamente acquistato un prodotto devono poter lasciare una recensione; la verifica dell'acquisto deve essere crittograficamente solida e legata all'identità pseudo-anonima dell'utente.
- **I3:** Le recensioni devono essere firmate digitalmente, in modo da impedire manipolazioni o negazioni ex post (non ripudio).
- **I4:** Il sistema deve impedire che due utenti possano aggregare le proprie credenziali o attività per simulare una recensione congiunta o aumentare artificiosamente la reputazione di un contenuto.
- **I5:** Il sistema deve garantire che le recensioni valide vengano registrate secondo l'ordine temporale con cui sono state emesse, senza che attori intermedi (eg. piattaforma, validator) possano ritardare o censurare selettivamente transazioni per influenzare la visibilità o la reputazione dei contenuti.

1.4.4 Trasparenza

- **T1:** Gli algoritmi di ordinamento e visibilità delle recensioni devono essere pubblici e non modificabili, così da evitare favoritismi o manipolazioni da parte della piattaforma.

- **T2:** Tutte le transazioni rilevanti (recensioni, modifiche) devono essere consultabili pubblicamente sulla blockchain o in un registro parallelo verificabile, secondo il principio dell'immutabilità.
- **T3:** Le regole per la revoca o la modifica di una recensione devono essere chiare, predefinite e non arbitrate dalla piattaforma, ma applicate automaticamente dal sistema.
- **T4:** La fiducia in eventuali componenti terze (eg. piattaforma, validator) deve essere giustificata da meccanismi tecnici o economici che ne scoraggino comportamenti sleali (eg. penalità, perdita di reputazione, verifica pubblica).

1.4.5 Efficienza

- **E1:** Il sistema consente una rapida verifica dell'acquisto, senza richiedere operazioni pesanti lato utente o validator.
- **E2:** Il processo di pubblicazione della recensione deve essere fluido e a basso costo computazionale, compatibile con dispositivi consumer (eg. smartphone).
- **E3:** Le operazioni crittografiche coinvolte (firma, verifica, Proof-of-Purchase) devono essere ottimizzate per l'uso quotidiano e non introdurre frizioni inutili nell'esperienza utente.
- **E4:** Il sistema deve essere progettato per gestire un elevato numero di recensioni e accessi contemporanei, mantenendo prestazioni stabili anche in caso di picchi di attività.

1.5 Completeness

La proprietà di *completeness* descrive il comportamento del sistema quando tutti gli attori coinvolti agiscono in modo onesto, rispettando le regole previste dal protocollo. In tale scenario, non si verificano attacchi né violazioni, e il sistema è in grado di offrire tutte le funzionalità desiderate in maniera sicura, trasparente ed efficiente.

In particolare:

- un utente effettua un acquisto legittimo attraverso una piattaforma e-commerce integrata con il sistema di recensioni;
- la piattaforma verifica e registra la transazione, generando una prova di acquisto (*Proof-of-Purchase*) che attesta, in modo crittograficamente sicuro, che l'utente ha realmente usufruito del servizio;

1. WORK PACKAGE 1

- tramite un'identità pseudo-anonima, l'utente accede alla funzionalità di recensione e, dopo il superamento della verifica, redige un feedback firmato digitalmente, che viene inoltrato alla rete;
- i validator onesti includono la recensione nella blockchain secondo l'ordine cronologico, garantendone l'immutabilità, la tracciabilità e la pubblica consultabilità, senza censure né ritardi;
- la piattaforma mostra la recensione applicando criteri di ordinamento e visibilità pubblici, verificabili e non modificabili in modo arbitrario;
- l'utente ha facoltà, qualora previsto, di revocare o aggiornare la recensione entro i limiti e secondo le regole definite nel sistema (eg. tempo massimo, consenso firmato);
- l'utente riceve reputazione positiva se pubblica la recensione entro il tempo previsto, o negativa se non lo fa;
- il sistema assegna eventuali incentivi e reputazione sulla base del rispetto delle scadenze e della pubblicazione effettiva di recensioni;
- durante l'intero processo, il sistema protegge la privacy dell'utente, evitando l'esposizione di metadati sensibili e garantendo l'integrità e il corretto tracciamento di tutte le operazioni.

CAPITOLO 2

WORK PACKAGE 2

In questo capitolo viene proposta una soluzione progettuale che risponde al modello delineato nel *Work Package 1 (WP1)*. L'obiettivo è progettare un sistema decentralizzato per la gestione di recensioni online affidabili nel contesto dell'e-commerce, che rispetti i vincoli funzionali e di sicurezza individuati, raggiungendo un ragionevole compromesso tra efficienza, trasparenza, confidenzialità, privacy e integrità.

La soluzione proposta si basa sull'utilizzo di una blockchain *permissionless*, che garantisce l'immutabilità delle recensioni, la verificabilità pubblica delle interazioni e la resistenza a manipolazioni arbitrarie da parte di malintenzionati. Gli utenti interagiscono tramite identità pseudo-anonime e possono pubblicare recensioni solo a seguito della verifica crittografica dell'avvenuto acquisto. Tutte le interazioni significative (inserimento, modifica, revoca) sono firmate digitalmente e registrate on-chain, assicurando tracciabilità e non ripudio.

La progettazione presentata in questo WP descrive dettagliatamente il comportamento delle parti oneste coinvolte e i componenti principali del sistema, con particolare attenzione ai seguenti aspetti:

- Verifica dell'acquisto tramite meccanismi crittografici (*Proof-of-Purchase*) legati all'identità pseudo-anonima dell'utente;
- Meccanismo di scrittura e pubblicazione delle recensioni, con struttura dei dati immutabile e regole di visibilità e ordinamento trasparenti e non modificabili;
- Sistema di reputazione basato esclusivamente sul comportamento verificabile (recensione pubblicata o meno), senza giudizi soggettivi da parte di altri utenti;


- Meccanismi di incentivazione che premiano automaticamente l'utente dopo l'acquisto, subordinatamente alla pubblicazione della recensione entro un tempo massimo stabilito;
- Possibilità di revoca o modifica delle recensioni secondo regole predefinite e automatizzate tramite smart contract;
- Protezione della privacy dell'utente e prevenzione della tracciabilità incrociata, nel rispetto dello pseudo-anonimato.
- Utilizzo del protocollo IPFS (InterPlanetary File System) per la conservazione off-chain di contenuti testuali delle recensioni, metadati sensibili, e registri di revoca. Ogni contenuto archiviato è referenziato tramite il suo CID (Content Identifier), il cui hash è pubblicato on-chain.

Tutte le scelte architetturali saranno giustificate in relazione alle proprietà analizzate nel WP1 e alle minacce potenziali, per garantire la solidità e l'affidabilità del sistema.

2.1 Architettura generale del sistema


Il sistema proposto per la gestione decentralizzata delle recensioni nel contesto dell'e-commerce si basa su una rete blockchain *permissionless*, supportata da smart contract e da una piattaforma applicativa decentralizzata (dApp) che funge da interfaccia utente. L'architettura è progettata per garantire un comportamento verificabile, trasparente e resistente alla manipolazione da parte di attori malevoli. Ogni interazione critica viene registrata on-chain, mentre i dati sensibili sono gestiti off-chain in modo sicuro.

2.1.1 Componenti principali del sistema

- **Utente pseudo-anonimo** (

16

infatti, il sistema supporta l'uso di DID multipli e tecniche di *zero-knowledge proof* (ZKP) per proteggere l'identità e la reputazione.

- **Venditore** (

2.1.2 Modalità di gestione della reputazione

La reputazione di ciascun utente è calcolata automaticamente sulla base del numero di NFT ricevuti e del numero di recensioni pubblicate nei tempi previsti.

- Ogni NFT rappresenta un'opportunità per pubblicare una recensione.
- Se l'utente recensisce entro 60 giorni, l'NFT è marcato come “utilizzato” e si assegna reputazione positiva.
- Se l'utente non recensisce entro il termine, l'NFT è marcato come “scaduto” e si assegna reputazione negativa.

L'utente può dimostrare, tramite prove a conoscenza zero, di aver maturato una reputazione positiva, senza rivelare identità o contenuti. Questo approccio consente di preservare la proprietà dell'anonimato e al contempo mitigare i rischi legati agli attacchi Sybil o alla creazione massiva di recensioni scollegate.

2.2 Funzionamento delle parti oneste

Questa sezione descrive il comportamento previsto delle componenti oneste del sistema, ovvero le entità che agiscono nel rispetto delle regole e delle proprietà progettuali identificate nel WP1. Ogni attore onesto segue un protocollo deterministico e verificabile, che garantisce il corretto funzionamento del sistema e la coerenza dei dati registrati on-chain. Le azioni compiute dai partecipanti sono regolate da procedure crittografiche sicure e dalla logica codificata nei contratti intelligenti, allo scopo di prevenire errori, frodi e ambiguità.

2.2.1 Gestione utente e creazione del DID

Nel sistema proposto, la gestione dell'identità dell'utente si basa sull'impiego di *Decentralized Identifiers (DID)*, ovvero identificatori univoci e pseudo-anonimi che permettono a ciascun utente di operare sulla piattaforma senza esporre la propria identità reale. I DID sono auto-generati dagli utenti in locale e sono legati a una coppia di chiavi crittografiche. Questa scelta garantisce un buon compromesso tra autenticità delle azioni e tutela della privacy.

Registrazione iniziale

Prima dell'avvio della procedura, l'utente si autentica tramite un sistema di identità digitale certificata, come **SPID** o **CIE**. Questa autenticazione consente all'Issuer di verificare l'identità reale dell'utente, mantenendo separati i dati personali dal successivo identificatore pseudo-anonimo (DID). La prima interazione con la piattaforma è connotata dai seguenti passaggi:

1. L'utente genera localmente una **coppia di chiavi** (sk_{DID} , pk_{DID}) e il corrispondente DID (eg. `did:ethr:0xABC123...`), secondo lo standard *W3C*.

2. L'utente richiede una **Verifiable Credential (VC)** da un Issuer autorizzato, che attesta la validità della sua registrazione e firma la VC.
3. L'utente memorizza la VC in un wallet compatibile (MetaMask).
4. L'utente invia una **Verifiable Presentation (VP)**, un pacchetto firmato che dimostra il possesso della VC, e una firma al contratto di registrazione.
5. Lo smart contract verifica:
 - L'autenticità della VC e la firma del *trusted Issuer*;
 - L'unicità della registrazione (la VC non è stata già usata);
 - Il legame tra DID e chiave usata per firmare la richiesta.
6. Se tutte le verifiche hanno esito positivo, il DID viene registrato come identità pseudo-anonima abilitata all'uso della piattaforma, mediante il mapping `registered[DID] = hash(VC)`, che viene aggiornato on-chain.

Vantaggi L'adozione dei DID offre i seguenti benefici:

- **Privacy:** l'identità reale dell'utente non viene mai esposta on-chain.
- **Sybil resistance:** l'emissione della VC è vincolata a un'autorità che rilascia un solo attestato per identità reale, difatti l'uso di SPID o CIE come prerequisito per l'emissione impedisce la creazione di identità multiple, pur mantenendo il DID completamente pseudo-anonimo on-chain.
- **Autenticazione decentralizzata:** l'utente dimostra di essere titolare del DID tramite challenge-response, firmando ogni richiesta con la propria chiave privata.
- **Interoperabilità:** i DID possono essere riutilizzati in altri contesti Web3 compatibili, migliorando l'usabilità e la coerenza dell'identità decentralizzata.

Mitigazioni di sicurezza Il sistema include alcune contromisure critiche:

- **Check di non riutilizzo:** ogni VC può essere usata una sola volta per registrare un DID.
- **Protezione contro identity theft:** solo il possessore della chiave privata può firmare la richiesta di accesso, riducendo il rischio di furti.
- **Registrazione dell'hash on-chain:** i contenuti delle VC, comprensivi di eventuali dati sensibili, sono conservati off-chain nel wallet dell'utente. Solo l'hash del documento viene registrato on-chain, al fine di garantire integrità e verificabilità, senza esporre il contenuto originale.

In questo modo, l'identificazione è solida e rispettosa della privacy, e il sistema impedisce la creazione di account multipli o il furto d'identità, senza la necessità di un'autorità centrale che conservi dati personali.

2.2.2 Venditore

Il venditore propone un prodotto ed è soggetto alla ricezione di recensioni pubbliche. Non ha la possibilità di modificare, rimuovere o influenzare l'ordine, la visibilità o il contenuto delle recensioni associate ai propri prodotti. La reputazione del venditore è determinata in modo trasparente e automatico sulla base delle recensioni effettivamente pubblicate dai clienti che hanno completato un acquisto. La piattaforma fornisce al venditore solo l'accesso alla consultazione pubblica dei dati registrati on-chain, senza controllo diretto sulle logiche di gestione.

2.2.3 Interazione dell'utente con il sistema tramite DID

Una volta completata la fase di registrazione e ottenuto un identificatore decentralizzato (DID), l'utente è in grado di partecipare attivamente al sistema, mantenendo un livello elevato di riservatezza. Tutte le operazioni compiute vengono autorizzate attraverso la firma digitale generata con la propria chiave privata associata al DID, garantendo così l'autenticità delle azioni, senza mai esporre informazioni personali. Tutte le interazioni sono registrate tramite smart contract sulla blockchain.

Pubblicazione di una recensione

Quando l'utente finalizza un acquisto sulla piattaforma e-commerce, riceve un attestato crittografico sotto forma di **NFT non trasferibile** (*soulbound token*) che ne conferma la transazione. Questo token funge da credenziale spendibile per l'invio di una recensione entro un termine massimo di 60 giorni.

Il processo si articola nei seguenti passaggi:

- L'utente redige la recensione e firma la richiesta con la chiave privata (EdDSA) associata al proprio DID;
- Invia la recensione e l'ID dell'NFT al contratto di gestione delle recensioni;
- Lo smart contract verifica che il token sia valido e appartenga all'utente, che non sia stato già utilizzato (`reviewUsed == false`) e che non sia scaduto;
- In caso di esito positivo, la recensione viene registrata on-chain e referenziata via IPFS, divenendo pubblicamente consultabile, e l'NFT viene marcato come usato. Inoltre, all'utente viene assegnata reputazione positiva e l'incentivo previsto viene immediatamente assegnato.

NFT non utilizzati

Se l'utente non pubblica alcuna recensione entro il termine massimo di 60 giorni:

- lo smart contract marca l'NFT come “scaduto”;
- viene assegnata **reputazione negativa** all'utente.

Reputazione e prove crittografiche

Per contribuire alla reputazione senza violare l'anonimato, l'utente può generare una **Zero-Knowledge Proof** che attesti proprietà aggregate, come:

- Numero minimo di recensioni pubblicate entro il termine previsto;
- Assenza di NFT scaduti o penalità reputazionali;
- Partecipazione continuativa e coerente nel tempo.

La prova viene verificata da uno smart contract compatibile con circuiti ZK (Semaphore), senza che sia necessario rivelare esplicitamente il contenuto delle recensioni firmate né il DID dell'utente.

Modifica e Revoca della Recensione

Ogni recensione registrata sulla blockchain può essere successivamente **modificata** o **revocata** dall'autore legittimo, rispettando condizioni di integrità e trasparenza.

Revoca L'utente può revocare la propria recensione soltanto se:

- è ancora il proprietario del NFT associato (verifica ownership);
- non ha già modificato o revocato in precedenza la stessa recensione;
- la richiesta è firmata digitalmente con la propria chiave privata associata al DID.

La revoca è implementata come un evento immutabile **ReviewRevoked** che mantiene traccia della decisione e il contenuto della recensione viene sostituito con un placeholder nullo. Il token di prova d'acquisto viene comunque marcato come “consumato” e non potrà essere riutilizzato, impedendo strategie abusive.

Modifica L'autore può modificare il contenuto testuale di una recensione, purché:

- ne detenga ancora la proprietà (verifica NFT);
- il contenuto precedente non sia stato revocato;

- venga fornita una nuova versione firmata, referenziata tramite un identificatore crittografico univoco (hash) e memorizzata off-chain in modo verificabile.

Le modifiche:

1. invalidano la versione precedente della recensione, mantenendo la tracciabilità storica;
2. vengono registrate come eventi di aggiornamento on-chain;
3. sono visibili attraverso lo storico pubblico delle versioni.

Cooldown Per prevenire abusi da parte di recensori che aggiornano ripetutamente il contenuto, viene introdotto un periodo di cooldown minimo di 24 ore tra due modifiche successive.

2.3 Utilizzo di NFT come prova di acquisto

Per garantire che solo gli utenti che abbiano effettivamente acquistato un prodotto possano pubblicarne una recensione, il sistema impiega un meccanismo di **Proof-of-Purchase** basato su *Non-Fungible Tokens (NFT)*. Ogni acquisto su una piattaforma e-commerce integrata genera un NFT. Il token rappresenta un attestato crittografico unico e verificabile, associato in modo univoco all'utente (tramite DID) e all'acquisto effettuato.

2.3.1 Emissione del token

Al momento della conferma di un acquisto su una piattaforma e-commerce integrata, lo smart contract corrispondente esegue il *minting* di un NFT contenente:

- **productId**: identificativo del prodotto acquistato;
- **ownerDID**: DID dell'utente;
- **purchaseDate**: data e ora dell'acquisto;
- **NFTstatus** == valid;
- **reviewStatus**: inizialmente impostato su **pending**;
- Eventuali metadati (eg. nome del prodotto, codice ordine hashato).

Il token viene assegnato all'utente ed è **non trasferibile** (soulbound), inoltre viene marcato come utilizzato una volta impiegato per pubblicare una recensione. Questo previene il riutilizzo fraudolento e la possibilità di vendere il diritto di recensire. Oltre all'NFT di acquisto, il sistema assegna automaticamente all'utente, dopo l'invio di una recensione,

un **badge soulbound** (NFT non trasferibile) che attesta la partecipazione al sistema di recensioni. Questo badge può essere usato per sbloccare funzionalità o status futuri.

2.3.2 Verifica e pubblicazione della recensione

L'utente può utilizzare l'NFT ricevuto per pubblicare una recensione entro 60 giorni dalla data di acquisto. Per fare ciò, deve presentare:

- Il contenuto della recensione, firmato con la propria chiave privata;
- L'identificativo dell'NFT associato all'acquisto.

Lo smart contract verifica che:

- Il token sia ancora valido e appartenga all'utente;
- Che lo stato (`reviewStatus`) sia ancora `pending`;
- Che non siano trascorsi più di 60 giorni dalla data di acquisto.

Se tutti i controlli sono soddisfatti:

- La recensione viene registrata sulla blockchain (hash su IPFS);
- Il token viene marcato come usato (`NFTstatus == used`);
- viene assegnata reputazione positiva all'utente.

Se la recensione viene pubblicata entro il termine, oltre all'incremento reputazionale, può essere aggiornato anche il livello del badge NFT posseduto, per riflettere il grado di partecipazione, secondo il seguente schema:

- **Bronze Reviewer** – 1 recensione pubblicata;
- **Silver Reviewer** – almeno 10 recensioni puntuali;
- **Gold Reviewer** – almeno 50 recensioni e zero penalità.

2.3.3 NFT scaduti

Se l'utente non recensisce entro 60 giorni:

- lo smart contract marca l'NFT come scaduto (`NFTstatus == expired`);
- viene automaticamente assegnata una penalità reputazionale (reputazione negativa).

Questa logica incoraggia gli utenti a contribuire attivamente al sistema di recensioni e scoraggia comportamenti inattivi o opportunistici.

2.3.4 Vantaggi della soluzione NFT

L'adozione di NFT soulbound per rappresentare la prova d'acquisto offre numerosi vantaggi, tra cui:

- **Immutabilità e trasparenza:** la prova dell'acquisto è pubblica e verificabile da chiunque;
- **Autenticità verificabile on-chain (Non ripudio):** ogni recensione è legata in modo inequivocabile a un acquisto valido tramite un token pubblico;
- **Resistenza allo spam:** un solo acquisto equivale ad un solo diritto di recensire;
- **Resistenza alla manipolazione:** gli NFT non sono trasferibili né falsificabili;
- **Compatibilità con reputazione verificabile:** la presenza o l'uso degli NFT può contribuire a meccanismi di reputazione, validabili via ZKP;
- **Automazione reputazionale:** il sistema calcola la reputazione esclusivamente sulla base del comportamento verificabile;
- **Incentivazione tempestiva:** l'utente riceve l'incentivo subito dopo l'acquisto, ma la reputazione dipende dal rispetto del termine di pubblicazione.

L'intero processo di generazione e verifica del token avviene on-chain, per assicurare massima affidabilità, trasparenza e auditabilità. Tuttavia, i metadati estesi o sensibili (eg. descrizione completa dell'ordine) sono conservati off-chain, tramite IPFS, e referenziati via hash, per ridurre costi e tutelare la privacy.

2.4 Uso delle Verifiable Credentials nel sistema

Per rafforzare il controllo sull'unicità e sull'autenticità delle identità senza rinunciare al principio di pseudo-anonimato, il sistema adotta il modello delle **Verifiable Credentials (VC)**, standardizzato dal W3C. Le VC permettono di attestare in modo sicuro e crittograficamente verificabile che un determinato DID appartenga a un utente registrato, senza dover rivelare direttamente l'identità reale.

2.4.1 Emissione della Verifiable Credential

Durante la fase di registrazione, l'utente interagisce con un'entità di fiducia, che agisce come *Issuer*, la quale rilascia una credenziale firmata (VC) contenente informazioni minime che attestano la registrazione dell'utente.

La VC include:

- L'identificatore del soggetto (`did:ethr:0xABC123...`);
- Lo stato di utente verificato (eg. `verified-user: true`);
- L'identificativo dell'Issuer;
- La firma crittografica della VC (EdDSA);
- Data di scadenza e condizioni di revoca.

La credenziale viene conservata nel wallet dell'utente (MetaMask con plugin VC) e non è pubblicata on-chain. Solo il suo hash può essere referenziato per finalità di verifica, riducendo l'esposizione di metadati sensibili.

2.4.2 Presentazione e verifica

Quando un utente desidera compiere un'operazione vincolata all'identità (registrarsi, scrivere una recensione), genera una **Verifiable Presentation (VP)**.

La VP è una struttura firmata che contiene:

- La VC originale o selezionata parzialmente (*selective disclosure*);
- Una **challenge** generata dal verificatore, usata per impedire replay-attack;
- Una firma che prova il possesso legittimo della VC.

Lo smart contract agisce da **Verifier** e controlla:

- La validità della firma dell'Issuer (*trusted Issuer*);
- Che la VC non sia scaduta o revocata (tramite `revocation registry`);
- Che la presentazione non sia stata già riutilizzata (*non replayable*);
- Che il DID sia legittimo e coerente con la registrazione.

Solo se tutte queste condizioni risultano soddisfatte, l'azione richiesta dall'utente viene autorizzata.

2.4.3 Gestione della Revoca delle VC

La revoca delle Verifiable Credentials (VC) è fondamentale per garantire la validità e unicità dell'identità nel tempo, in particolare in caso di compromissione, riemissione o declassamento dell'identità stessa.

Modello adottato

Il sistema adotta il modello **W3C Revocation List 2020**, in cui ogni VC include un `revocationIndex` associato a una bitstring pubblica. La lista di revoca è mantenuta *off-chain* e distribuita tramite *IPFS*. Ogni versione è identificata da un **CID (Content Identifier)**, pubblicato dallo smart contract dell'Issuer. In questo modo, ogni utente o smart contract può accedere al file JSON firmato, scaricarlo da IPFS e verificare lo stato di revoca senza dipendere da API centralizzate.

Verifica della validità

Al momento della presentazione di una VC, lo smart contract recupera l'hash della stessa e l'indice di revoca e verifica che il bit corrispondente nella bitstring non sia impostato a 1, altrimenti nega l'autorizzazione.

In pseudo-codice:

```
if RevocationList[vcIndex] == 1 → reject
```

Il contratto accede al CID della lista e confronta l'hash SHA-256 della VC con la posizione indicata.

Sicurezza e Privacy

Il meccanismo garantisce:

- **Integrità:** la Revocation List è firmata e referenziata tramite hash.
- **Verificabilità pubblica:** chiunque può scaricarla via IPFS.
- **Privacy:** nessun dato personale è esposto, solo l'hash della VC è usato per la verifica.

Alternative future: EVOKE

In scenari ad alta scalabilità, il sistema potrà adottare accumulatori crittografici (eg. Merkle tree o accumulatori RSA) come nel modello **EVOKE**, per ridurre lo spazio di verifica locale e migliorare le performance su dispositivi IoT.

2.4.4 Privacy e Selective Disclosure

Il sistema adotta tecniche di *selective disclosure* per minimizzare i dati esposti durante la presentazione delle credenziali. In particolare, viene impiegata la tecnica **BBS+ Signature**, che consente di derivare sottoprove firmate a partire da una VC completa,

mantenendo validità crittografica. L'utente può così presentare selettivamente solo i campi strettamente necessari, proteggendo le altre informazioni contenute nella VC originale, senza bisogno di emettere più credenziali.

Questo approccio migliora:

- La **confidenzialità**, evitando l'esposizione di dati personali on-chain;
- La **non linkabilità**, poiché transazioni distinte non sono correlabili tra loro;
- La **flessibilità**, supportando interazioni multi-identità e selettive in ambienti decentralizzati.

2.4.5 Compromesso tra sicurezza e costo

L'intero ciclo $VC \rightarrow VP \rightarrow$ verifica è progettato per essere scalabile:

- Le **VC** sono emesse e conservate **off-chain** nei wallet, con hash referenziati on-chain solo quando necessario.
- Le **Revocation List** sono distribuite tramite IPFS, identificabili attraverso un *CID* firmato e referenziato negli smart contract, evitando congestione e dipendenza da API centrali.
- Le **VP** sono firmate localmente e verificate solo nei punti critici (registrazione, pubblicazione recensione), minimizzando il costo computazionale on-chain.

In questo modo, si ottiene un equilibrio ottimale tra sicurezza crittografica, protezione dell'identità e sostenibilità tecnica.

2.5 Gestione dei casi limite

Il sistema è progettato per mantenere coerenza, correttezza e sicurezza anche in presenza di condizioni anomale, errori operativi o utenti inattivi. Questa sezione descrive i principali scenari limite e le strategie previste per gestirli senza compromettere l'integrità del sistema reputazionale.

2.5.1 Utenti inattivi

Gli utenti che non interagiscono con il sistema per lunghi periodi non perdono l'accesso, ma:

- le loro **VC possono scadere** naturalmente, impedendo operazioni critiche finché non ne viene emessa una nuova;

- gli **NFT non utilizzati** per scrivere recensioni vengono marcati automaticamente come **expired** dopo 60 giorni;
- a ogni NFT scaduto corrisponde una penalità reputazionale automatica (reputazione negativa).

2.5.2 VC scadute o revocate

Ogni VC include un campo di scadenza e un indice nella Revocation List. L'azione viene bloccata dal contratto se si verifica almeno una delle seguenti condizioni:

- la data di validità è scaduta;
- il bit associato nella Revocation List è impostato a 1.

In entrambi i casi, l'utente dovrà ottenere una nuova VC valida per proseguire.

2.5.3 DID revocati o compromessi

Nel caso in cui un utente smarrisca la propria chiave privata o sospetti un furto, può:

1. generare un nuovo DID,
2. ottenere una nuova VC dal medesimo Issuer,
3. invalidare quella precedente tramite aggiornamento della Revocation List.

Il sistema consente di migrare identità senza esporre dati personali e mantiene coerenza nei circuiti ZKP tramite aggiornamento dei nullifier.

2.5.4 Utente Bannato

Un utente può essere bannato dal sistema in seguito alla rilevazione automatica o manuale di comportamenti fraudolenti, come la pubblicazione di recensioni false, la violazione delle policy di registrazione o l'abuso dei meccanismi reputazionali. Il DID dell'utente viene inserito in una *ban list* consultabile on-chain, impedendogli di:

- pubblicare recensioni;
- ricevere incentivi;
- modificare o revocare recensioni precedenti.

Il ban può essere revocato solo tramite una procedura di verifica off-chain condotta da un comitato di validatori.

2.6 Gestione del compromesso tra pseudo-anonimato e unicità dell'utente

Nel progettare un sistema decentralizzato che tuteli la riservatezza dell'utente ma impedisca abusi come la creazione di identità multiple, è necessario bilanciare due esigenze apparentemente opposte: la **non tracciabilità delle azioni** e l'**unicità verificabile dell'identità**. Infatti, l'adozione di identificatori pseudo-anonimi (DID) per separare tra loro le recensioni, se da un lato protegge la privacy dell'utente, dall'altro introduce il rischio di attacchi di tipo *Sybil*, in cui un singolo individuo agisce come molteplici entità per ottenere vantaggi indebiti (incentivi ripetuti, manipolazione reputazionale). Per affrontare questo compromesso, il sistema impiega un'architettura fondata su Verifiable Credentials e Zero-Knowledge Proof, in grado di separare logicamente identità pubbliche e azioni on-chain, mantenendo al contempo la garanzia che ogni utente rappresenti una sola entità logica. Per mitigare questo rischio, il sistema prevede l'impiego della seguente strategia:

2.6.1 Verifiable Credential univoca

Durante la fase di registrazione, ogni utente deve ottenere una **Verifiable Credential** (VC) firmata da un Issuer affidabile, attestante che ha superato una procedura di identificazione controllata. Questa VC non contiene dati personali, ma è legata crittograficamente a un segreto univoco controllato dall'utente (*nullifier*). Tale VC rappresenta la "radice identitaria" che dimostra che l'utente è registrato una sola volta. A partire da essa, l'utente può generare qualsiasi numero di DID operativi senza perdere la proprietà di unicità logica.

2.6.2 DID multipli, ma dimostrabilmente unificati

Per preservare l'**unlinkability** tra le interazioni, l'utente può scegliere di utilizzare un DID diverso per ogni azione. Tuttavia, quando necessario (eg. per ricevere premi o partecipare a meccanismi di reputazione), l'utente è tenuto a generare una **Zero-Knowledge Proof** (ZKP) che attesti il possesso di una VC valida. Questo meccanismo consente di:

- Mantenere DID disaccoppiati nel dominio pubblico;
- Garantire che tutte le azioni provengano da un'unica identità logica (anti-Sybil);
- Prevenire il rilascio multiplo di premi;
- Proteggere la reputazione senza dover rivelare il contenuto delle recensioni.

2.6.3 Struttura della ZKP anti-Sybil

Il sistema utilizza un circuito ZKP predefinito (*Semaphore*) per generare una prova non rivelabile contenente:

- **hash(VC)**: identificativo crittografico della credenziale;
- **nullifier**: segreto univoco per prevenire riutilizzi;
- **MerkleRoot**: radice di un albero contenente tutti gli utenti registrati.

La verifica viene effettuata on-chain tramite un contratto compatibile con ZK-verification.

2.6.4 Risultato del compromesso

Questa strategia garantisce:

- **Non linkabilità**: ogni recensione o voto può essere firmato con DID diversi, senza possibilità di tracciamento esterno;
- **Unicità garantita**: ogni utente può dimostrare, quando richiesto, di essere un'entità registrata unica;
- **Resilienza agli attacchi Sybil**: nessun attore può ottenere vantaggi moltiplicando le proprie identità operative.

2.7 Smart Contract

Gli smart contract costituiscono il nucleo logico e immutabile del sistema. Tutte le regole di registrazione, validazione, reputazione e pubblicazione delle recensioni sono codificate in modo trasparente e deployate sulla blockchain. Nessuna entità può modificarne il comportamento dopo la pubblicazione.

2.7.1 Funzionalità implementate

I principali contratti intelligenti implementano le seguenti funzionalità:

- **Registrazione dell'utente**: verifica della VC e del DID tramite challenge crittografica e registrazione nel sistema.
- **Minting dell'NFT**: generazione automatica di NFT come prova d'acquisto alla conferma dell'ordine.
- **Pubblicazione della recensione**: verifica dell'NFT e registrazione della recensione firmata. Se entro 60 giorni, viene marcata come “valida” e assegna reputazione positiva.

- **Scadenza automatica NFT:** gestione periodica dei token inutilizzati entro il termine. Se scaduti, l'utente riceve reputazione negativa.
- **Revoca e modifica recensione:** permette all'utente di revocare o aggiornare il contenuto della recensione, nel rispetto dei vincoli di integrità e storico.
- **Calcolo reputazione:** calcola la reputazione di un DID come rapporto tra NFT ricevuti e recensioni pubblicate entro i termini.
- **Gestione utenti bannati:** controlla l'esistenza del DID in una ban list consultabile, impedendo azioni non autorizzate.
- **Verifica ZKP:** accetta prove a conoscenza zero per dimostrare l'identità o la partecipazione, senza rivelare dati sensibili.

Funzione	Descrizione
registerVC	Verifica autenticità della VC e registra il DID nel sistema
mintNFT	Genera NFT alla conferma di un acquisto valido
submitReview	Registra una recensione se l'NFT è valido; assegna reputazione positiva
expireNFT	Marca automaticamente come "scaduti" gli NFT oltre i 60 giorni; assegna reputazione negativa
editReview	Permette la modifica della recensione da parte dell'autore
revokeReview	Revoca la recensione pubblicata e disabilita l'NFT corrispondente
getReputationScore	Restituisce il punteggio reputazionale di un DID
isBanned	Verifica se il DID è presente nella ban list on-chain
verifyZKP	Verifica una prova a conoscenza zero presentata dall'utente

Table 2.1: Funzionalità implementate negli smart contract

2.8 Validator

I validator sono i nodi della rete blockchain che eseguono la validazione e l'inclusione delle transazioni nei blocchi. Operano secondo il meccanismo di consenso del network (eg. Proof-of-Stake), assicurando che tutte le azioni rilevanti vengano registrate in modo ordinato e immutabile.

2.8.1 Compiti principali

I validator onesti assicurano che ogni transazione conforme al protocollo venga elaborata correttamente, contribuendo alla trasparenza e all'affidabilità del sistema.

In particolare, essi si occupano di:

- **Inclusione delle recensioni:** garantiscono che ogni recensione validamente firmata e verificata venga scritta sulla blockchain secondo l'ordine temporale previsto.
- **Registrazione delle modifiche:** ogni operazione di revoca o aggiornamento viene tracciata come evento separato, e i validator assicurano che sia correttamente inclusa in un blocco.
- **Gestione delle scadenze:** le transazioni automatiche che marciano NFT come *expired* e aggiornano la reputazione devono essere processate senza ritardi o omissioni.
- **Verifica di prove ZKP:** i validator processano le transazioni contenenti Zero-Knowledge Proof, garantendo che la validazione delle identità e delle interazioni anonime avvenga correttamente.
- **Conservazione della coerenza temporale:** assicurano che tutte le interazioni (eg. pubblicazione recensione, modifica, scadenza NFT) avvengano in ordine cronologico, evitando manipolazioni strategiche.

2.8.2 Assunzione di sicurezza

Il modello prevede che una maggioranza onesta di validator partecipi al protocollo. Anche in presenza di minoranze malevoli, la blockchain garantisce:

- Ordine cronologico delle recensioni e delle modifiche;
- Disponibilità e persistenza dei dati pubblicati;
- Resistenza alla censura, alla sostituzione di contenuti o all'omissione di eventi validi.

2.9 Modulo di Audit

Il sistema prevede un modulo di audit pubblico che consente a utenti, revisori indipendenti o enti di fiducia di verificare la correttezza e la trasparenza delle operazioni registrate sulla piattaforma. Questo modulo agisce da interfaccia di consultazione per i dati on-chain e off-chain referenziati, rendendo possibile un controllo distribuito sull'intero sistema, favorendo un ecosistema verificabile e meritocratico.

2.9.1 Funzionalità

- **Consultazione recensioni:** ogni recensione è associata a un identificatore crittografico (hash) e a un NFT. Il modulo permette la consultazione dei contenuti,

dei metadati essenziali (data di emissione, autore), dello stato (attiva, modificata, revocata) e dell'esito delle verifiche effettuate in fase di pubblicazione.

- **Tracciamento delle modifiche e revoche:** il sistema mantiene uno storico completo delle versioni di ciascuna recensione. Eventuali modifiche o revoche sono visualizzabili sotto forma di eventi pubblici registrati e l'utente può verificare la validità di ciascuna versione tramite l'hash originale.
- **Verifica degli NFT:** è possibile ispezionare lo stato di ogni NFT (usato, scaduto) e correlarlo con la pubblicazione della recensione.
- **Esposizione reputazionale:** la reputazione degli utenti è calcolata automaticamente dal sistema come rapporto tra NFT ricevuti e recensioni pubblicate entro i termini.
- **Verifica ZKP:** l'utente può dimostrare la propria reputazione in modo anonimo tramite Zero-Knowledge Proof. Il modulo consente di visualizzare la presenza e validità delle prove registrate, senza rivelare l'identità dell'utente.
- **Monitoraggio anomalie:** il sistema può evidenziare schemi sospetti, come attività automatizzate, voti incrociati o comportamenti strategici non conformi, offrendo strumenti per il monitoraggio comunitario e per il mantenimento dell'equilibrio reputazionale.
- **Accesso strutturato ai dati:** il modulo espone i dati registrati in formato machine-readable, facilitando analisi statistiche, audit esterni o esportazione verso strumenti di visualizzazione interattiva.

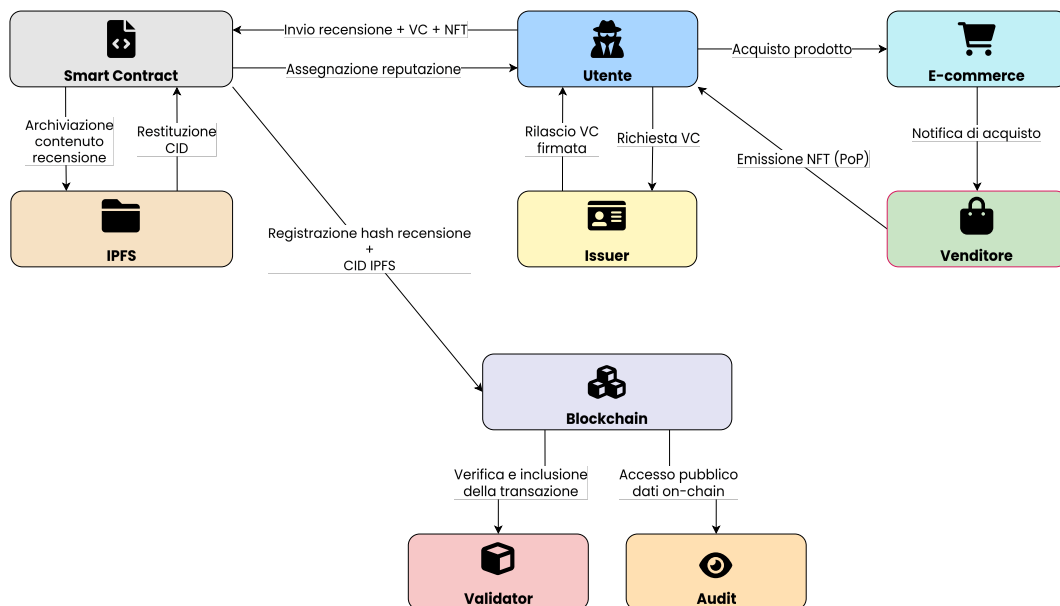


Figure 2.1: Diagramma dell'architettura del sistema

2.10 Scelta della blockchain permissionless

Il sistema proposto adotta una blockchain di tipo permissionless per garantire trasparenza, immutabilità e accessibilità pubblica dei dati. Questa scelta architetturale permette di garantire che nessun attore possa alterare, censurare o manipolare i dati registrati, favorendo un ecosistema aperto e meritocratico. Tuttavia, tale scelta implica anche alcune sfide in termini di costi e prestazioni. Per tale motivo, si propone un confronto sintetico tra le due principali opzioni architettureali:

Criterio	Blockchain permissionless	Blockchain permissioned
Accesso	Aperto a chiunque, nessuna autorizzazione richiesta	Limitato a nodi autorizzati
Decentralizzazione	Elevata (assenza di trust centralizzato)	Parziale, dipende da chi controlla l'accesso
Resistenza alla censura	Garantita (nessuno può impedire la scrittura di dati validi)	Debole (il consorzio può filtrare o rifiutare)
Trasparenza	Totale, i dati sono pubblici e verificabili da chiunque	Limitata, dipende dal livello di accesso concesso
Prestazioni	Più lente (consenso pubblico)	Più rapide (consenso ottimizzato)
Costi	Costi di transazione più elevati (gas)	Costi più bassi e controllabili
Governance	Distribuita e trasparente	Centralizzata o consortile

Table 2.2: Confronto tra blockchain permissionless e permissioned

Alla luce dei requisiti funzionali e di sicurezza analizzati, si ritiene che l'adozione di una rete *permissionless* sia la scelta più coerente per:

- Garantire la massima verificabilità pubblica delle recensioni;
- Evitare l'introduzione di autorità centrali di controllo;
- Supportare un sistema di reputazione distribuito e sottoponibile ad audit;
- Ridurre al minimo i presupposti di fiducia.

Eventuali esigenze prestazionali future possono essere soddisfatte tramite layer off-chain o soluzioni di scaling, mantenendo inalterata la natura pubblica e immutabile del registro principale.

2.10.1 Ethereum vs Hyperledger Fabric

Viene di seguito rilasciata una tabella comparativa tra Ethereum e Hyperledger Fabric, al fine di mettere in luce gli aspetti che hanno condotto alla scelta di una blockchain permissionless per questo progetto.

Parametro	Ethereum (permissionless)	Hyperledger Fabric (permissioned)
Modello di trust	Trustless, basato su consenso distribuito (PoS)	Basato su identità note e fidate
Accessibilità	Aperto a chiunque, adatto a scenari pubblici e community-driven	Limitato a entità registrate (consorzi privati)
Scalabilità	Scalabilità media	Alta scalabilità grazie al controllo su accessi e consenso
Governance	Decentralizzata, gestita dalla community e dagli stakeholder di Ethereum	Centralizzata o consorziata, con meccanismi privati di aggiornamento
Censura	Censura-resistente, ogni transazione è registrata pubblicamente	Possibile censura o controllo delle transazioni da parte degli admin
Auditabilità	Pubblica, trasparente, verificabile da chiunque	Audit interna, limitata ai membri autorizzati
Costo transazioni	Gas fee variabile	Costi trascurabili, ottimizzato per ambienti enterprise
Adatto per	Sistemi pubblici, e-commerce, reputazione e incentivazione aperta	Applicazioni interaziendali, supply chain, settori regolamentati

Table 2.3: Confronto tra Ethereum e Hyperledger Fabric

2.10.2 Innovazioni future

In uno sviluppo futuro, l'adozione di soluzioni Layer 2 per il rollup (come zkSync o Arbitrum) potrebbe ridurre i costi di transazione e migliorare la scalabilità, mantenendo l'integrità e la trasparenza del sistema Ethereum.

2.11 Utilizzo per l'utente (dApp)

Per rendere il sistema utilizzabile anche da utenti non tecnici, è prevista una piattaforma web decentralizzata (dApp) che funge da interfaccia intuitiva per tutte le operazioni previste, le cui caratteristiche principali sono:

- **Integrazione con wallet:** supporto per MetaMask con estensioni per la gestione di VC e firme ZKP.
- **Interfacce grafiche guidate (GUI):** la dApp fornisce interazioni semplificate per:
 - generazione del DID;
 - richiesta e caricamento VC;
 - caricamento della recensione con upload automatico su IPFS;
 - gestione e consultazione della reputazione.
- **Gestione errori:** feedback chiari in caso di VC scaduta, DID non valido o NFT scaduto/usato.
- **Notifiche off-chain:** aggiornamenti via email o notifiche browser su scadenze NFT, stato della VC, ricezione incentivi.

2.12 Formalismi matematici crittografici

2.12.1 Generazione DID

Un DID assume la forma: `did:ethr:0xABC123....`

È creato localmente tramite generazione di una coppia chiave pubblica/privata (pk, sk) e registrazione su un resolver Ethereum compatibile.

2.12.2 Firma digitale

Ogni messaggio m è firmato localmente tramite:

$$\sigma = \text{Sign}_{sk}(m)$$

La verifica avviene tramite:

$$\text{Verify}_{pk}(m, \sigma) = \text{true}$$

2.12.3 Verifiable Credential (VC)

Una VC è un JSON strutturato contenente:

- `credentialSubject.id` = `did:ethr:...`
- `Issuer` = `did:ethr:0xBEEF1234...`
- `proof.signature` = $\text{Sign}_{sk_{Issuer}}(VC)$

2.12.4 Verifiable Presentation (VP)

Contiene una VC più una firma:

$$\sigma_{VP} = \text{Sign}_{sk_{user}}(\text{challenge} \parallel \text{hash}(VC))$$

Verificabile via:

$$\text{Verify}_{pk_{user}}(\text{challenge} \parallel \text{hash}(VC), \sigma_{VP}) = \text{true}$$

2.12.5 Revoca con bitstring

Ogni VC contiene un `revocationIndex`. L'Issuer mantiene una bitstring pubblica:

$$\text{RevocationList}[\text{revocationIndex}] = 1 \Rightarrow VC \text{ revocata}$$

Verificabile pubblicamente da chiunque.

2.12.6 Zero-Knowledge Proof (ZKP)

L'utente può generare una prova non rivelabile di possesso di una VC valida, senza esporre il contenuto o il proprio DID. Il circuito predefinito (*Semaphore*) utilizza i seguenti elementi:

- `hash(VC)`: hash della credenziale usata;
- `nullifier`: segreto univoco per impedire il riutilizzo della prova;
- `MerkleRoot`: radice dell'albero delle identità registrate.

La prova generata è:

$$\pi = \text{ZK-Proof}(\text{hash}(VC), \text{nullifier}, \text{Merkle root})$$

Verificabile via:

$$\text{Verify}_{ZK}(\pi) = \text{true}$$

2.12.7 Selective Disclosure con BBS+

Per garantire la minimizzazione dei dati esposti, il sistema adotta le firme **BBS+**, che permettono all'utente di selezionare un sottoinsieme dei dati contenuti nella VC e firmarli mantenendo validità crittografica.

Data una credenziale firmata:

$$VC = \{claim_1, claim_2, \dots, claim_n\}$$

L'utente può presentare:

$$Proof_{BBS+} = \text{Sign}_{sk}(\text{subset}(VC))$$

Tale sottoprova è verificabile senza accesso all'intera VC:

$$\text{Verify}_{pk}(\text{subset}(VC), \text{Proof}_{BBS+}) = \text{true}$$

2.13 Conclusione

Il sistema progettato nel presente WP2 rappresenta una soluzione completa e coerente rispetto al modello individuato nel WP1, capace di affrontare le criticità più rilevanti dei sistemi di recensioni centralizzati nel contesto dell'e-commerce. La progettazione tiene conto della necessità di garantire l'autenticità delle recensioni, la verifica dell'effettivo utilizzo del servizio, l'integrità dei dati, la confidenzialità degli utenti e la trasparenza delle regole applicate.

L'adozione di una blockchain permissionless consente di registrare in modo immutabile e pubblico le recensioni e tutte le operazioni critiche correlate, eliminando la necessità di una fiducia centralizzata. L'uso di NFT soulbound come prova di acquisto e Verifiable Credentials come attestati d'identità verificata garantisce la legittimità delle recensioni, prevenendo spam e falsi utenti. Inoltre, l'implementazione di tecniche a conoscenza zero (ZKP) permette di costruire una reputazione verificabile, senza compromettere l'anonimato degli utenti.

Ogni componente del sistema (smart contract, verificatori, moduli di audit) è pensato per essere trasparente, verificabile e resistente alla manipolazione. Le scelte architetturali (on-chain per le prove e i diritti, off-chain per i dati sensibili) permettono un'elevata sicurezza senza sacrificare prestazioni e scalabilità.

CAPITOLO 3

WORK PACKAGE 3

CAPITOLO 4

WORK PACKAGE 4