



POLITECNICO DI BARI

DIPARTIMENTO DI INGEGNERIA ELETTRICA E DELL'INFORMAZIONE
CORSO DI LAUREA TRIENNALE IN INGEGNERIA INFORMATICA E
DELL'AUTOMAZIONE

Chain4Good

*Progettazione e sviluppo di una piattaforma di
crowdfunding con tecnologia blockchain*

Candidati:

Angelica DE FEUDIS
Johnatan CAPUTO
Luca GENTILE

Docente:

Prof.ssa Marina
MONGIELLO

Academic Year: 2025/2026

Indice

Acronimi	ii
1 Introduzione	1
2 Background	2
2.1 Tecnologia blockchain	2
2.1.1 Transazioni	2
2.1.2 Blocchi	2
2.1.3 Consenso e costruzione della blockchain	3
2.1.4 Vantaggi della blockchain	3
2.2 Ethereum Blockchain	4
2.2.1 Smart Contract	4
2.2.2 DApps	4
2.3 DAO	4
3 Metodologia di progetto	5
3.1 Modello di processo	5
3.2 Pianificazione delle attività	5
3.3 Analisi dei rischi	5
3.4 Stima dei costi	5
4 Progettazione e implementazione	6
4.1 Analisi dei requisiti	6
4.2 Analisi SWOT	6
4.3 Architettura del Software	6
5 Prototipo	7
5.1 Dashboard	7
5.2 Creazione progetto	7
5.3 Inserimento e valutazione spesa	7
6 Validazione e discussione	8
6.1 Valutazione dell'applicazione	8
6.2 Realizzazione dei requisiti	8
7 Conclusioni e sviluppi futuri	9
Riferimenti bibliografici	10

Acronimi

PoW Proof of Work.

1 Introduzione

2 Background

2.1 Tecnologia blockchain

Una blockchain è una base di dati distribuita, condivisa e immutabile, mantenuta da una rete di nodi.

Nata come infrastruttura di supporto per la criptovaluta Bitcoin [1], la blockchain si è progressivamente evoluta in una tecnologia *general-purpose*, trovando applicazione in un'ampia gamma di contesti.

Come suggerito dal termine stesso, la blockchain è una catena cronologicamente ordinata di blocchi, dove ciascun blocco contiene un insieme di transazioni validate dalla rete. Ogni blocco è collegato al precedente attraverso un riferimento crittografico, detto *hash*. Questa struttura dati rende estremamente difficile la modifica o la cancellazione delle informazioni già registrate: qualsiasi tentativo di alterare un blocco comporterebbe infatti la modifica di tutti i blocchi successivi, rendendo l'attacco facilmente rilevabile e computazionalmente impraticabile.

2.1.1 Transazioni

La transazione rappresenta l'unità fondamentale di informazione all'interno della blockchain. Essa descrive un'operazione richiesta da un utente, come ad esempio il trasferimento di un asset digitale. Ogni transazione è creata da un nodo della rete e viene firmata digitalmente utilizzando una coppia di chiavi crittografiche. Prima di essere registrata nella blockchain, ogni transazione viene validata dalla rete secondo regole condivise e, una volta confermata, viene inserita in un blocco che è crittograficamente collegato ai blocchi precedenti.

2.1.2 Blocchi

Un blocco è una struttura dati che aggrega un insieme di transazioni validate in un determinato intervallo di tempo. Oltre alle transazioni, ogni blocco contiene informazioni di gestione fondamentali, tra cui: 1

- l'hash del blocco precedente, che collega crittograficamente i blocchi tra loro;
- un timestamp, che indica il momento di creazione del blocco;
- dati aggiuntivi richiesti dal protocollo di consenso adottato.

L'inclusione dell'hash del blocco precedente rende la blockchain una struttura immutabile per costruzione: anche una minima modifica a una singola transazione altererebbe l'hash del blocco, invalidando l'intera catena successiva. Questo meccanismo costituisce uno dei principali fattori di sicurezza della blockchain.

2.1.3 Consenso e costruzione della blockchain

In una rete blockchain decentralizzata, più nodi possono proporre contemporaneamente nuovi blocchi. Per determinare quale blocco debba essere aggiunto alla catena in modo univoco e condiviso, viene utilizzato un protocollo di consenso distribuito. Il consenso è un algoritmo che permette alla rete di concordare su un'unica versione valida del ledger, anche in presenza di nodi malfunzionanti o potenzialmente malevoli.

Il primo protocollo di consenso largamente diffuso è la [Proof of Work \(PoW\)](#), introdotta da Bitcoin, in cui i nodi competono per risolvere un problema computazionale complesso. Il nodo che risolve per primo il problema ottiene il diritto di aggiungere il nuovo blocco alla blockchain e di propagarlo alla rete.

Altri protocolli di consenso, come Proof of Stake o meccanismi basati su votazione, sono stati successivamente sviluppati per migliorare efficienza energetica, latenza e scalabilità. Una volta che un blocco è stato validato e accettato dalla maggioranza dei nodi, esso viene aggiunto alla blockchain e diventa parte integrante del ledger. Con il passare del tempo e l'aggiunta di nuovi blocchi, le informazioni contenute nei blocchi più vecchi diventano sempre più sicure, poiché la loro modifica richiederebbe il controllo di una grande porzione della potenza di calcolo o dei validatori della rete.

2.1.4 Vantaggi della blockchain

- Decentralizzazione:
- Immutabilità:
- Trasparenza e assenza di fiducia:
- Sicurezza:

2.2 Ethereum Blockchain

2.2.1 Smart Contract

2.2.2 DApps

2.3 DAO

3 Metodologia di progetto

3.1 Modello di processo

3.2 Pianificazione delle attività

3.3 Analisi dei rischi

3.4 Stima dei costi

4 Progettazione e implementazione

4.1 Analisi dei requisiti

4.2 Analisi SWOT

4.3 Architettura del Software

5 Prototipo

5.1 Dashboard

5.2 Creazione progetto

5.3 Inserimento e valutazione spesa

6 Validazione e discussione

6.1 Valutazione dell'applicazione

6.2 Realizzazione dei requisiti

7 Conclusioni e sviluppi futuri

Riferimenti bibliografici

- [1] S. Nakamoto, B. Bit et al., «Bitcoin: A peer-to-peer electronic cash system,» 2008, 2007.