



**UNIVERSITÀ DEGLI STUDI DI ROMA
TOR VERGATA**

FACOLTÀ DI INGEGNERIA

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

A.A. 2016/2017

Tesi di Laurea Specialistica

UNA PIATTAFORMA COLLABORATIVA BASATA SU
BLOCKCHAIN E SMART CONTRAT:
un caso di studio per il mondo accademico.

RELATORE

Prof. Giuseppe F. Italiano

CANDIDATO

Gabriele Belli

Indice

Abstract	1
1 Introduzione	4
1.1 Panoramica	4
1.2 Obiettivi	5
1.3 Stato dell'arte	10
1.4 Guida alla lettura	11
2 La blockchain	13
2.1 Introduzione	13
2.2 Storia	16
2.3 Struttura del blocco	17
2.4 Merkle Trees	18
2.5 Mining	20
2.5.1 Proof of Work	22
2.5.2 Proof of Stake	25
2.6 La blockchain nell'uso pratico	27
3 Chiavi, indirizzi e wallet	31
3.1 Introduzione	31

3.2	Wallet	32
3.2.1	Chiavi private	33
3.2.2	Chiavi pubbliche	34
3.2.3	Crittografie a curve ellittiche	34
3.3	Indirizzi	35
4	Il network Ethereum	37
4.1	Cos'è ethereum	37
4.2	Storia di ethereum	38
4.3	Account e SmartContract	39
4.4	Transazioni e Messaggi	40
4.4.1	Transazioni	40
4.4.2	Messaggi	42
4.5	Transizione di Stato di Ethereum	43
4.6	EVM	44
4.7	DAPP	45
4.8	I client	46
4.8.1	Metamask	47
5	I linguaggi e il gas	49
5.1	I linguaggi	49
5.2	Solidity	50
5.3	La EVM ed il gas	53
5.4	Gas e transazioni	55
5.5	Considerazioni sul gas	57

6 Progetto di alto livello	58
6.1 Architettura alto livello	58
6.2 Dapp e blockchain	59
6.2.1 Smart contract: storage	59
6.2.2 Architettura e funzionamento	60
6.3 Applicazione mobile	65
6.4 Consegna dei messaggi	68
7 Implementazione	70
7.1 Implementazione del contratto	70
7.2 Iterazioni con il contratto	72
7.3 Message broker	73
7.3.1 Publish	73
7.3.2 Subscribe	75
8 Test, Sviluppi futuri e conclusioni	76
8.1 Test	76
8.2 Sviluppi futuri	79
8.3 Conclusioni	80
Elenco delle figure	83
Bibliografia	83

Abstract

Il lavoro di tesi ha come obiettivo la realizzazione di una piattaforma collaborativa di supporto ai docenti in grado di facilitare la gestione dei corsi e l'interazione con gli studenti in maniera semplice, veloce e che, con ambizione, permetta la creazione e il mantenimento di documenti di proprietà in maniera sicura, trasparente ed immutabile.

La piattaforma è costituita da una web App ibrida e da due applicazioni mobile, una per gli studenti ad una per i docenti; sono presenti vari blocchi ognuno con un proprio obiettivo principale.

Uno degli aspetti più interessanti della piattaforma è la possibilità offerta di possedere un registro di documenti generici e di poterne dimostrare la proprietà; tali documenti potrebbero essere nel caso specifico: incarichi di tutoraggio, verbalizzazione di esami, etc...

Per fornire tale servizio mi sono servito della combinazione di tre tecnologie: la blockchain, il protocollo IPFS e la firma digitale.

L'utilizzazione della blockchain è stata resa necessaria in quanto, come qualità intrinseca di essa, troviamo delle proprietà fondamentali per l'ecosistema: la decentralizzazione, la trasparenza, la sicurezza e l'immutabilità; siamo pertanto certi che qualsiasi valore venga memorizzato su questa non possa essere modificato o eliminato.

Nello specifico è stata utilizzata la tecnologia Ethereum, una piattaforma che si ap-

poggia sulla blockchain, ed è stata sfruttata la sua proprietà fondamentale ovvero quella di gestire smart contracts in modo intelligente, questi contratti sono generati tramite un linguaggio di programmazione costruito al suo interno e Turing-complete. Poiché lo store di dati su di essa richiede un costo, anche elevato, che varia a seconda delle dimensioni di bytes del file si è reso necessario adottare un sistema di storage diverso e più economico; per questo motivo ho deciso di utilizzare il protocollo Interplanetary File System.

I file all'interno della rete IPFS sono identificati univocamente dal loro hash e sono distribuiti con un protocollo basato su BitTorrent.

L'hash del documento viene firmato e inserito all'interno della blockchain.

Il problema dello storage decentralizzato attraverso l'uso della blockchain è uno tra gli ambiti applicativi con maggiore appeal in quanto in una soluzione centralizzata il cloud provider può analizzare i file che custodisce in qualsiasi momento, è per questo motivo che una soluzione che preveda l'utilizzo della blockchain di Ethereum ci consente di avere pieno controllo sui dati che decidiamo di memorizzare.

Le soluzioni attualmente esistenti al problema hanno caratteristiche più generali rispetto a quanto presentato in questa tesi e sono utilizzati in diversi contesti; inoltre tale soluzione cerca di trovare un giusto compromesso tra economicità, sicurezza ed user-experience.

La piattaforma è dotata inoltre di un applicazione mobile sia per i docenti che per gli studenti, la prima consente ai docenti di comunicare in maniera semplice, veloce e sicura con gli studenti iscritti ad un determinato corso inviando loro notifiche.

Per tale funzionalità è stato utilizzato RabbitMQ un message broker open-source che mette a disposizione il pattern publish/subscribe.

L'applicazione degli studenti invece permette a questi di controllare in modo rapido

la sezione delle informazioni del dipartimento e di iscriversi ad un determinato corso. Nei capitoli della relazione verrà fornito dapprima una visione generale del problema: da dove nasce e come è affrontato; successivamente verranno analizzate in modo più approfondito le tecnologie utilizzate e gli aspetti fondamentali che mi hanno portato alla scelta di queste.

Ho deciso di dedicare ampio spazio alla tecnologia blockchain e ad Ethereum con la speranza di fornire una visione chiara, ma allo stesso tempo dettagliata dell'argomento e creare un collante di tutto il materiale utilizzato per approfondire l'argomento.

Nei restanti capitoli verrà presentata la piattaforma, partendo da una visione generale fino ad arrivare progressivamente a fornire un'immagine dettagliata dell'intero sistema.