UNIVERSITÀ DEGLI STUDI ROMA TRE

Facoltà di Ingegneria
Corso di Laurea Magistrale in Ingegneria Informatica

Tesi Di Laurea

Blockchain

Laureando
Gianmaria Del Monte
Matricola 499829

Relatore
Prof. Maurizio Pizzonia

Anno Accademico 2019/2020

qui la dedica

Introduzione

Introduzione

Indice

Capitolo 1

Background

1.1 Bitcoin e Blockchain

Bitcoin è una tecnologia open-source per lo scambio di valute, denominate *bitcoin*, decentralizzato, presentato nel 2008 da una persona anonima, con lo pseudonimo di Satoshi Nakamoto [2]. A differenza di valute tradizionali che esistono fisicamente sotto forma di banconote, i bitcoin sono monete virtuali. Esse vengono scambiate tra i partecipanti alla rete Bitcoin che comunicano mediante il protocollo Bitcoin. Quindi con il termine Bitcoin, si indicano vari aspetti: la tecnologia in sé, lo stack protocollare di comunicazione adottato tra i partecipanti alla rete e la valuta scambiata. Bitcoin è una rete P2P, a cui partecipano nodi chiamati *peer*, in cui non esistono nodi speciali o più importanti di altri, come nei sistemi di pagamento elettronici tradizionali, in cui c'è un server centrale che gestisce tutti i pagamenti.

Il concetto fondamentale di Bitcoin è quello di *transazione*: una transazione trasferisce dei bitcoin da una conto sorgente ad un conto destinazione. Le transazioni possono sono create da qualsiasi peer della rete, che dimostri essere proprietario del conto sorgente e vengono inviate a tutti i nodi della rete. A differenza di pagamenti elettronici tradizionali, in cui un server centrale accetta o rifiuta le transazioni generate dai propri clienti, le transazioni sono accettate o rifiutate dalla rete Bitcoin secondo un meccanismo di *consenso distribuito*, utilizzando un approccio denominato *Proof-of-work*. La transazioni accettate vengono quindi raggruppate in blocchi di transazioni, secondo un processo che richiede un enorme quantità di potenza computazionale, che vengono aggiunti ai blocchi della *blockchain*. Questo processo è definito *mining* ed è svolto dai peer che ricoprono il ruolo di *miners*. Il mining ha due obiettivi:

1. creazione di bitcoin: ogni nodo che aggiunge un blocco alla blockchain

viene ricompensato dalla rete con una quantità di bitcoin fissata per ogni blocco e che decresce nel tempo;

2. validazione delle transazioni secondo le regole di consenso, assicurando che le transazioni siano non valide e non corrette.

Inizialmente il mining veniva effettuato da personal computer potenti. Man mano che i miners si aggiungevano alla rete Bitcoin, per cui diveniva sempre più difficile *minare* un blocco, si utilizzarono delle Graphical Processing Units, o GPU, come quelle utilizzate nei videogiochi. Tuttavia negli ultimi tempi si utilizzano sistemi Application Specific Integrated Circuit, o ASIC, che implementano in hardware gli algoritmi di mining impiegati in Bitcoin per aumentare le performance. Sono state create anche soluzioni che hanno l'obiettivo di condividere la propria potenza computazionale in mining farm con vari partecipanti, in cui si suddividono i bitcoin guadagnati.

1.1.1 Wallet e chiavi private

1.1.2 Transazioni

1.1.3 Mining

1.1.4 Attacchi noti

1.2 Trilemma

1.3 MHT

Capitolo 2

Stato dell'arte

2.1 Algorand

2.2 Bernardini

2.3 Sharding

Capitolo 3

Una soluzione scalabile

3.1 Architettura

3.2 Analisi Multicast

3.3 Teoremi

Conclusione

conclusione

Ringraziamenti

Ringrazio tutti

Bibliografia

[1] Andreas M Antonopoulos. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.