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

Tesi di Laurea

UNIBLOCK: BLOCKCHAIN UNIVERSITARIA

UNIBLOCK: UNIVERSITY BLOCKCHAIN

CLAUDIO NAVE

Relatore: *Francesco Tiezzi*

Anno Accademico 2021-2022

INDICE

1

INTRODUZIONE

Capitolo di introduzione. Fatto alla fine.

2

CONCETTI ESSENZIALI SULLA BLOCKCHAIN

Nella sua più primitiva definizione una blockchain è una struttura dati in grado di registrare informazioni e garantirne l'immutabilità nel tempo ridondando i dati su un gran numero di nodi senza che sia necessaria un'entità centrale che vigili su possibili minacce o malfunzionamenti. Concepita nel 2008 da Satoshi Nakamoto [2] come mezzo per decentralizzare il mondo delle transazioni finanziarie, è stata oggetto nel corso del tempo di un forte interesse accademico e commerciale venendo applicata e sviluppata in un gran numero di scenari diversi. Pur essendo presenti sul panorama attuale svariati esempi di blockchain anche molto diverse tra loro in complessità e implementazione, possiamo individuare alcune primitive di base la cui analisi permette di categorizzare e partizionare il vasto insieme delle blockchain.

2.1 MODALITÀ DI ACCESSO ALLA RETE

Una prima differenza fondamentale delle blockchain è la modalità con cui i nuovi nodi possono entrare a far parte della rete. Nelle blockchain pubbliche qualunque dispositivo può diventare un nodo della rete senza alcun controllo sulla sua legittimità. Per questo motivo tali blockchain prendono il nome di permissionless blockchain in quanto non c'è alcuna differenza gerarchica tra i vari nodi e chiunque può entrare a farne parte. In generale questo tipo di blockchain presenta un numero di partecipanti molto elevato grazie alla bassa soglia di entrata. Nelle blockchain private invece l'entrata nella rete è preceduta da una fase di autenticazione del soggetto come l'appartenenza a una determinata azienda. Tali blockchain sono quindi confinate nelle realtà che le sviluppano e le loro pool di nodi sono di conseguenza molto ridotte in quanto solo chi è qualificato può entrare a farne parte. Inoltre riflettendo la gerarchia dell'organizzazione proprietaria della blockchain sono in genere presenti differenze di responsabilità tra i vari nodi, da qui il nome di permissioned blockchain.

Possiamo identificare inoltre un terzo tipo di blockchain, quello ibrido, in cui vengono uniti alcune caratteristiche delle blockchain pubbliche con quelle private. Nelle blockchain ibride alcune funzioni sono lasciate come pubbliche mentre altre richiedono una preventiva autenticazione. Le blockchain pubbliche sono di gran lunga il tipo più comune di blockchain, ma quelle private stanno guadagnando terreno avendo attirato l'attenzione del mondo finanziario [1].

2.2 ALGORITMO DI CONSENSO

algoritmo di consenso

2.3 PRIVACY E SICUREZZA

privacy e sicurezza bitcoint non criptato etherum c'è il concetto di privacy

2.4 CONFRONTO DI ALCUNE BLOCKCHAIN

riferimenti a bitcoin, ethereum, hyperledger (permissioned)

tabella di confronto righe -> caratteristiche colonne -> blockchain (compresa la mia)

Ci possono essere blockchain pubbliche e private.

BIBLIOGRAFIA

[1] Christine V. Helliar, Louise Crawford, Laura Rocca, Claudio Teodori, and Monica Veneziani. Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*, 54:102136, 2020. ISSN 0268-4012. doi: https://doi.org/10.1016/j.ijinfomgt.2020.102136. URL https://www.sciencedirect.com/science/article/pii/S0268401219314586. (Cited on page 6.)

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, 2008. URL https://bitcoin.org/bitcoin.pdf. (Cited on page 5.)