



UNIVERSITÀ
DEGLI STUDI
FIRENZE

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	3
2	Concetti essenziali sulla blockchain	5
2.1	Modalità di accesso alla rete	5
2.2	Algoritmo di consenso	6
2.3	Privacy e sicurezza	6
2.4	Confronto di alcune blockchain	7

INTRODUZIONE

Capitolo di introduzione. Fatto alla fine.

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 [4] 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 il loro vasto insieme.

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 [3].

2.2 ALGORITMO DI CONSENSO

Data la natura distribuita di una blockchain è di fondamentale importanza la ricerca del consenso tra i nodi, ovvero che ogni transazione generata venga validata e diffusa attraverso la rete rimanendo inalterata. Il primo algoritmo di consenso concepito è la proof of work: l'immutabilità dei dati è garantita dalla difficoltà di computare rapidamente un puzzle crittografico. Nella rete Bitcoin ad esempio un nuovo blocco è considerato valido quando viene trovato un numero tale che inserito nell'header del blocco stesso rende il suo hash inferiore a una certa quantità. Variando tale quantità è possibile modulare il carico dei blocchi generati dall'intera rete, dando il tempo ai blocchi di diffondersi tra i vari nodi. Ogni nodo dà la sua fiducia alla catena di blocchi in cui è stata spesa la maggior quantità di lavoro computazionale. Un algoritmo di consenso concepito più recentemente è la proof of stake: i nuovi blocchi vengono validati da nodi scelti casualmente in base a quanta valuta hanno investito nella rete. Pur ritenendo un certo livello di casualità, l'algoritmo di selezione del prossimo validatore privilegia i maggiori scommettitori. La legittimità della rete è garantita perciò dal fatto che chi ha investito maggiormente avrà interesse nel suo corretto funzionamento. La rete Ethereum prevede di effettuare il cambio da proof of work a proof of stake nei prossimi anni. Per un'analisi dettagliata sugli algoritmi di consenso fare riferimento a [1].

2.3 PRIVACY E SICUREZZA

Nelle blockchain pubbliche il contenuto dei blocchi è disponibile a ogni nodo senza alcuna protezione. Assume grande importanza quindi avere sempre ben presente quali informazioni si stanno immettendo nella rete in chiaro e quali invece si cerca di proteggere. Nella rete Bitcoin tutto il contenuto di un blocco è presente completamente in chiaro tanto da poter

ricostruire la storia di ogni singolo bitcoin fino al momento della sua coniazione. In questo caso la privacy offerta agli utenti si limita alla loro anonimizzazione nella rete offrendo indirizzi usa e getta senza legami con l'identità legale del soggetto che li possiede. Anche la rete Ethereum non prevede di base alcuna forma di cifrazione del contenuto dei blocchi, essendo tuttavia presenti delle forme di privacy a zero conoscenza implementabili come zk-SNARKS per nascondere integralmente il contenuto di una transazione [2]. Discorso diverso invece per le blockchain private in quanto la preventiva autenticazione dei nodi permette di garantire che le informazioni contenute nei blocchi siano consultabili solo da soggetti autorizzati, non rendendo necessari complessi sistemi di crittografia per garantire la riservatezza delle informazioni.

2.4 CONFRONTO DI ALCUNE BLOCKCHAIN

Di seguito una comparazione essenziale delle due più grandi blockchain moderne con UniBlock:

	<i>Bitcoin</i>	<i>Ethereum</i>	<i>UniBlock</i>
<i>Accesso</i>	Pubblica	Pubblica	Ibrida
<i>Algoritmo di consenso</i>	Proof of work	Proof of work	Proof of work
<i>Privacy</i>	Non crittografata	Non crittografata	Crittografata

BIBLIOGRAFIA

- [1] Natalia Chaudhry and Muhammad Murtaza Yousaf. Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities. In *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*, pages 54–63, Dec 2018. doi: 10.1109/ICOSST.2018.8632190. (Cited on page 6.)
- [2] EthHub. Privacy on ethereum. <https://docs.ethhub.io/ethereum-roadmap/privacy/>. [Online; accessed 08-06-2022]. (Cited on page 7.)
- [3] 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.)
- [4] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, 2008. URL <https://bitcoin.org/bitcoin.pdf>. (Cited on page 5.)