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 [7] 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 comuni a tutte.

2.1 BLOCCHI E TRANSAZIONI

In una blockchain le informazioni sono tipicamente registrate in transazioni, a loro volta raggruppato in un blocco. Alla

2.2 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 [6].

2.3 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 certà 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 [3].

2.4 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 conoscienza implementabili come zk-SNARKS per nascondere integralmente il contenuto di una transazione [5]. 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.

2.5 CONFRONTO DI ALCUNE BLOCKCHAIN

Di seguito una comparazione di tre grandi blockchain moderne con UniBlock:

	Bitcoin	***Ethereum***	***Hyperledger Fabric***	***UniBlock***
Accesso	Pubblica	Pubblica	Privata	Ibrida
Consenso	Proof of work	Proof of work	Crash Fault Tolerance	Proof of work
Privacy	Non crittografata	Non crittografata	Non crittografata	Crittografata

3

CONCETTI ESSENZIALI DI CRITTOGRAFIA

UniBlock impiega varie tecnologie di cifratura moderne. Una disamina dettagliata del processo completo sarà oggetto dei prossimi capitoli, daremo ora una panoramica generale dei principali algoritmi usati.

SHA-3 Algoritmo di hashing crittografico pensato come futuro successore della famiglia di algoritmi SHA-2 [4]. Usato in UniBlock come puzzle crittografico alla base della proof of work.

AES Algoritmo di cifratura simmetrica a blocchi diventato lo standard de facto per questo genere di algoritmi avendo supporto implementativo a livello di assembly nella maggior parte delle CPU moderne [8]. Permette di criptare simmetricamente, ovvero per mezzo di un'unica chiave sia in cifratura che in decifratura, un blocco di 128 bit. Per criptare più di 128 bit vengono usate particolari modalità di operazione come ECB, in cui l'inseme di bit viene partizionato in gruppi di 128 bit e criptati singolarmente. UniBlock usa la modalità di operazione GCM, modalità estremamente efficiente che garantisce oltre alla cifratura anche l'integratià dei dati.

X25519 Algoritmo di scambio di una chiave tramite Diffie-Hellman basato sulla curva ellittica Curve25519 [1]. L'agloritmo di Diffie-Hellman permette a due soggetti di scambiarsi tramite un canale insicuro delle informazioni pubbliche, ad esempio le rispettive chiavi pubbliche di un cifrario a chiave pubblica, e combinarle in modo tale da raggiungere ognuno distintamente a una chiave uguale per entrambi così da poterla usare ad esempio per inizializzare una cifratura simmetrica. Nell'algoritmo X25519 le chiavi pubbliche scambiate sono coordinate sul campo finito della curva ellittica Curve25519, che verranno combinate con le rispettive chiavi private per giungere a una coordinata comune.

ED25519 Algoritmo di firma a chiave pubblica basato sulla curva ellittica Curve25519 [2]. Data una coppia di chiavi, una pubblica e una privata, l'algoritmo permette di generare una firma mediante la chiave privata così che chiunque possa verificare tramite la chiave pubblica che il messaggio non è stato alterato ed è stato prodotto dalla persona che possiede la chiave privata.

BIBLIOGRAFIA

[1] Daniel J. Bernstein. Curve25519: New diffie-hellman speed records. In *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography*, volume 3958 of *Lecture Notes in Computer Science*, pages 207–228. Springer, 2006. doi: 10.1007/11745853_14. URL https://iacr.org/archive/pkc2006/39580209/39580209.pdf. (Cited on page 9.)

[2] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. *Journal of Cryptographic Engineering*, 2(2):77–89, Sep 2012. ISSN 2190-8516. doi: 10.1007/s13389-012-0027-1. URL https://doi.org/10.1007/s13389-012-0027-1. (Cited on page 10.)

[3] 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.)

[4] Morris Dworkin. Sha-3 standard: Permutation-based hash and extendable-output functions, 2015-08-04 2015. (Cited on page 9.)

[5] EthHub. Privacy on ethereum. https://docs.ethhub.io/ethereum-roadmap/privacy/. [Online; accessed 08-06-2022]. (Cited on page 7.)

[6] 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.)

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

[8] Information Technology Laboratory (National Institute of Standards and Technology). Announcing the advanced encryption standard (aes). Technical report, 2001. URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. (Cited on page 9.)