Università degli Studi di Milano Bicocca

Dipartimento di Informatica, Sistemistica e Comunicazione

Corso di Laurea Magistrale in Informatica

SINTESI TESI

ANALISI E IMPLEMENTAZIONE DI PROTOCOLLI DI VOTO ELETTRONICO SU BLOCKCHAIN CON DIMOSTRAZIONI ZERO-KNOWLEDGE

Relatore: Prof. Alberto Leporati

Co-relatore: Dott. Raffaele Nicodemo

Tesi di Laurea Magistrale di:

Luca Virgilio

Matricola 794866

Anno Accademico 2019-2020

In un mondo improntato sempre più alla globalizzazione e al digitale, la tecnologia ha pervaso ogni aspetto della nostra vita. Malgrado ciò, non è ancora stato creato un sistema di voto elettronico che sia considerato universalmente sicuro ed affidabile. Negli ultimi anni sta emergendo una nuova tecnologia, la blockchain, che grazie alle sue proprietà di sicurezza, trasparenza e immutabilità, potrebbe rivoluzionare diversi settori. Questo lavoro si pone l'obiettivo di mostrare come attraverso l'uso della blockchain è possibile costruire un sistema di voto elettronico che garantisca tutte le proprietà necessarie per il corretto svolgimento della votazione.

La blockchain è un insieme di tecnologie che permette di risolvere il problema del consenso distribuito in una rete asincrona. ll termine blockchain è stato coniato successivamente all'implementazione e alla diffusione di Bitcoin. Bitcoin nasce dall'esigenza di creare una valuta digitale decentralizzata senza alcun banchiere centrale che convalidi le transazioni. Normalmente una banconota è firmata tramite un codice seriale generato dalla banca centrale. Dato che in Bitcoin non esiste un'autorità centrale, è il mittente a firmare le transazioni, come se una banconota venisse firmata ogni volta che cambia proprietario. La blockchain non è altro che un registro distribuito delle diverse transazioni effettuate. Non è possibile trasferire la stessa banconota a più persone poiché ogni partecipante possiede una copia della blockchain. Per inviare e ricevere bitcoin, un utente deve creare un wallet, formato da una coppia di chiavi, una pubblica ed una privata. A ciascun wallet viene associato uno o più indirizzi, utilizzati per ricevere bitcoin. Una transazione è composta da un campo TxId, ovvero l'hash che identifica univocamente la stessa, una lista di input e una lista di output. Durante una transazione, gli input vengono consumati e vengono generati nuovi output. Il termine blockchain, letteralmente catena di blocchi, deriva dal fatto che le transazioni sono organizzate in una lista concatenata di blocchi. Ciascun blocco contiene il proprio identificativo, l'hash del blocco e l'hash del blocco precedente. Dato che non esiste un'autorità centrale che verifica e valida le transazioni, è necessario un meccanismo che determini quale nodo debba validare un blocco. Bitcoin utilizza la proof of work (PoW), ovvero un meccanismo in cui si cerca il consenso da parte della maggioranza dei nodi. L'obiettivo è quello di trovare un nonce (un valore numerico) tale per cui l'hash $(prevhash||Tx,...,Tx||nonce)$ appartenga ad un intervallo piccolo rispetto allo spazio degli output possibili. Dato che l'hash è una funzione one-way, l'unico modo per calcolare il nonce è provare iterativamente tutti i possibili valori (oppure tentare a caso fino a che non si trova un valore che vada bene), e, proprio per questo esistono i cosiddetti miner: nodi che in cambio di una ricompensa in bitcoin si sfidano per calcolare l'hash del blocco. Quando un blocco viene validato, esso viene accettato implicitamente da tutti gli altri miner dal momento che provano a costruire un nuovo blocco a partire da quello appena validato. Per assicurasi che una transazione sia andata a buon fine, è necessario attendere almeno 6 conferme (ovvero la validazione di sei blocchi successivi al blocco contenente la transazione).

Considerando la natura distribuita del sistema e il tipo di algoritmo di consenso, per alterare la blockchain di Bitcoin è necessario effettuare un attacco controllando il 51%

della potenza computazionale della rete. Risulta estremamente difficile, per non dire impossibile, controllare tutta questa potenza computazionale, quindi un qualsiasi agente economico razionale è incentivato a minare piuttosto che attaccare la rete. Anche in un ipotetico scenario d'attacco, non è possibile modificare il protocollo, rubare coin da un indirizzo esistente o rimuovere le transazioni dalla rete, ad eccezione di quelle recenti.

L'utilizzo della blockchain nella progettazione di un sistema di voto risulta particolarmente adatta poiché garantisce trasparenza, immutabilità e sicurezza. Zcash e Monero sono due blockchain note per la loro propensione all'anonimato, anche grazie all'utilizzo di zero knowledge proof. In crittografia il prover è l'entità che fornisce la prova, mentre il verifier è colui che attivamente verifica la veridicità di una particolare affermazione. Una dimostrazione zero knowledge è un protocollo attraverso il quale un prover può convincere un verifier di conoscere un valore segreto x, senza rivelare alcuna informazione riguardo al segreto, ad eccezione della semplice affermazione.
Dopo un'attenta analisi tra i due protocolli, è emerso che attualmente Monero risulta essere più adatto ad essere utilizzato in un sistema di voto. In primo luogo il protocollo di Monero è ben definito e, sebbene nel corso del tempo abbia subito delle evoluzioni, risulta essere stabile. Al contrario Zcash è più recente e deve essere ancora sviluppato per raggiungere la sua versione definitiva. In secondo luogo il protocollo di Zcash richiederebbe molte più modifiche rispetto a quello di Monero per essere utilizzato in un sistema di voto. Infine Zcash utilizza le succint non interactive argument of knowledge (ZK-SNARKs), un tipo di dimostrazione zero knowledge che, sebbene producano prove di lunghezza costante e richiedano un tempo di verifica ridotto, per utilizzarle è necessario creare una common reference string (CRS). Per generare una CRS è necessario un trusted setup che richiede un quantitativo di tempo, energia e potenza computazionale non indifferente per assicurarsi che tutto venga svolto in sicurezza. Invece Monero utilizza la bulletproof, una range proof senza alcun tipo di trusted setup.

Monero è una blockchain in continua evoluzione. Ogni 6 mesi viene rilasciata una nuova versione che apporta modifiche e miglioramenti al protocollo. In Monero esistono quattro diversi tipi di chiavi:

- **private view key** (k^v): utilizzata per verificare il saldo di un wallet
- **public view key** (K^v): utilizzata per creare indirizzi validi, stealth address
- **private spend key** (k^s): utilizzata per firmare le transazioni
- **public spend key** (K^s): utilizzata per verificare la firma delle transazioni

Diversamente da Bitcoin, l'indirizzo di un wallet non viene mai utilizzato come destinatario di una transazione, altrimenti un osservatore esterno che conosce gli indirizzi

pubblici potrebbe collegare gli output ai rispettivi destinatari. Per questo motivo bisogna creare uno stealth address per ogni output. In una transazione Monero il valore viene cifrato e si utilizza la bulletproof affinché un osservatore esterno possa verificarne la correttezza, cioè controllare che la somma degli output sia uguale alla somma degli input e delle fee e che i valori degli input e degli output siano positivi o nulli. Per celare il mittente di una transazione, Monero utilizza le ring signature. In particolare questo meccanismo permette di nascondere quali output vengono spesi in una transazione. Anziché firmare una transazione unicamente con la private spend key del mittente, la firma viene generata utilizzando anche un insieme di chiavi pubbliche scelte in maniera pseudocasuale. Per evitare che un output venga speso più volte, si calcola una key image che lo identifica univocamente mantenendo comunque l'anonimato.

Dato che la blockchain è una tecnologia complessa, si è deciso di considerare la tipologia di votazione più importante, cioè quella inerente alle elezioni politiche.
L'espressione di una scelta di voto in un sistema tradizionale viene sostituita da una transazione sulla blockchain. Per convenzione, 1 token di voto corrisponde a 1 monero. Si suppone che le proprie chiavi private generate dal wallet non siano cedibili. Inoltre, ciascuna sessione di voto è indipendente dalle altre e non condivide alcun dato. Nel sistema sono presenti diversi attori: gli elettori, coloro che hanno diritto di partecipare alla votazione; i candidati, cioè le scelte esprimibili nella votazione, ed infine un amministratore, ovvero una persona che si occupa di gestire l'elezione. I wallet dei candidati sono di tipo view only, cioè possono solo ricevere fondi senza mai trasferirli. Per quanto riguarda la blockchain, la rete è costituita da diversi nodi certificati e gestiti dall'ente organizzatore. Non è possibile aggiungere nodi a piacere poiché potrebbe compromettere la privacy del sistema.
Per utilizzare Monero in un sistema di voto, è necessario effettuare alcune modifiche al protocollo. Come prima cosa si è scelto di utilizzare la versione 14.01 di Monero fin dal primo blocco. Questo poiché questa versione richiede una ring signature di almeno 11 indirizzi, obbliga ad utilizzare la bulletproof al posto della vecchia versione della ring confidential transaction. In seguito si è limitata la trasferibilità dei token. Tutti i nodi della rete conoscono l'indirizzo e la private view key dell'amministratore. Questo comporta un certo grado di trasparenza poiché tutti possono riconoscere le transazioni prodotte dall'amministratore. In questa rete un token può appartenere a una delle categorie: spendibile o valido. Se il token è prodotto dall'amministratore, esso è spendibile. Dal momento che un elettore riceve un token dall'amministratore e lo spende, la transazione genera un token valido. Il protocollo prevede che se un token valido viene utilizzato nella ring signature, la transazione non è valida e quindi viene rigettata. In questo modo un token in possesso di un elettore è trasferibile una sola volta. Si osservi che un token valido può essere trasferito ad un qualsiasi partecipante della rete, potenzialmente anche ad un indirizzo appartenente ad un altro elettore. Questo token non potrà più essere speso e quindi diventa inutilizzabile. Con questa strategia si evita che un qualsiasi miner possa spendere la propria ricompensa. Prima dell'apertura della

votazione, l'amministratore distribuisce i token agli elettori.

L'implementazione del sistema è composta da un server NodeJs che si occupa del mining e della gestione dei diversi wallet, da MongoDB che memorizza le informazioni inerenti alla votazione e da quattro nodi che gestiscono la blockchain. Il tutto viene eseguito in cloud, tramite il servizio di AWS. Gli utenti possono partecipare alla votazione tramite una applicazione web, in cui devono inserire il codice fiscale prima di effettuare il voto. Al termine della votazione, ciascun elettore riceve un transaction Id tramite il quale può verificare che il voto sia stato conteggiato. Al termine della votazione è possibile effettuare un'operazione di notarizzazione includendo l'hash della blockchain in una blockchain pubblica.

Analizzando i risultati ottenuti dall'esperimento, possiamo concludere che la proprietà di autenticità non è garantita. Il problema dell'autenticazione degli elettori è strettamente collegato al problema dell'identità digitale e rimane una questione aperta. Il sistema di voto può essere open source oppure può essere certificato da un operatore esterno. In questo modo è possibile verificare le operazioni svolte dall'amministratore (ovvero il server Nodejs). Questo unito all'utilizzo della blockchain comporta che le proprietà di anonimato, integrità, immutabilità, verificabilità, auditabilità e trasparenza siano garantite. Per quanto riguarda la proprietà di disponibilità, essa viene garantita dall'utilizzo di AWS. Dato che tramite il sistema di voto da remoto è possibile votare con il proprio dispositivo da qualsiasi luogo, vengono garantite anche le proprietà di mobilità e accessibilità. La capacità di controllo e ripristino del sistema viene assicurata dal protocollo rigido e dal sistema decentralizzato. L'unico problema riscontrato oltre l'autenticità è la non coercibilità. Infatti in quanto sistema da remoto non è possibile garantire che l'utente non sia influenzato da persone o agenti esterni al momento del voto.
Per creare un sistema completo, installabile ed utilizzabile, come prima cosa sarebbe necessaria la creazione di un wallet Monero multipiattaforma. Inoltre sarebbe necessario integrare nel sistema di voto un servizio di autenticazione digitale sicuro e un meccanismo che garantisca la non coercibilità.

In conclusione, considerando che il protocollo di Monero è in continua evoluzione e che i problemi mostrati potrebbero essere risolti in un futuro prossimo, il protocollo descritto in questo elaborato risulta essere un buon punto di partenza per la costruzione di un sistema di voto da remoto sicuro e affidabile.