Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea triennale in Informatica

Implementazione di un Voting System su Blockchain

Relatore:
Chiar.mo Prof.
Cosimo Laneve

Presentata da:
Andrea Scorza

Correlatore:
Dott.ssa
Adele Veschetti

II Sessione
Anno Accademico 2017-2018

Abstract

In questo documento si andranno ad analizzare i sistemi di voto, dai più antichi risalenti all'epoca romana, fino ad i più moderni utilizzati nei vari paesi del mondo ai giorni nostri. Parleremo delle varie tecnologie di voto ed innovazioni che si sono avvicendate nel trascorrere del tempo e di tutte le problematiche relative ad esse. Andremo ad analizzare nel dettaglio i più moderni sistemi di voto elettronici e la loro struttura. Si andrà quindi a definire una nuova e recente tecnologia, la blockchain e si andrà a spiegarne in dettaglio il funzionamento ed i maggiori algoritmi di consenso distribuito relativi ad essa. Infine verrà spiegato il progetto realizzato utilizzando la blockchain. Il progetto consiste in un innovativo sistema di voto elettronico decentralizzato, si andranno ad analizzare i vari componenti del sistema, le proprietà di voto mantenute nel sistema e i vari vantaggi e svantaggi che questa tecnologia se applicata potrebbe portare nel mondo moderno.

Indice

Capitolo 1

Introduzione

1.1 Sistemi di voto

Nel corso di questa tesi si andranno ad analizzare sotto vari punti di vista i diversi sistemi di voti utilizzati al mondo. L'idea principale è stata quella di risolvere un problema molto comune ma attualmente sottovalutato tramite una nuova tecnologia e provare a verificarne l'efficienza. Il problema in questione è quello del voto e dell'integrità e correttezza che questo antico sistema attualmente in uso manca nella maggior parte dei casi. Nel corso della storia sono stati inventati numerosi e diversi sistemi di voto, ma quello inventato dai romani, ancora in uso fino ad oggi, in Italia e non solo, sembra essere quello che va per la maggiore. Ovviamente sono state apportate modifiche nel tentativo di migliorarlo e colmare i difetti di questo sistema, ma a mio parere non si è ancora ottenuto un risultato soddisfacente.

I primi sistemi elettronici di voto furono inventati in America, macchine troppo costose e di dimensioni assurde, che cercavano di eliminare la principali possibilità di frodi, ma che risultavano, nella maggior parte dei casi, macchine totalmente inaffidabili che più che risolvere il problema, spesso lo amplificavano. Ad esempio la macchina di voto a leva inventata in America, con una leva simile a quella delle slot machine, che esprimeva tanta fiducia al pubblico, in verità era facilmente manipolabile, bastava che venisse impostata da un tecnico malintenzionato per poter smettere di contare i voti per un determinato partito o candidato dopo una determinata cifra, e l'impossibilità di poter ricontare i voti rendeva questa macchina totalmente un disastro dal punto di vista della prevenzione contro frodi elettorali. Per questo motivo è nata l'esigenza di un sistema elettronico che fosse in grado di mantenere intatte le proprietà e i diritti dei votanti.

In alcuni paesi sono già in uso sistemi elettronici di voto all'avanguardia, che comunque, come verrà spiegato successivamente non hanno ancora raggiunto un livello efficienza desiderato. Dopo l'analisi di questi nuovi sistemi, nasce quindi l'idea di creare completamente un nuovo sistema mai realizzato prima, tramite l'utilizzo della più nota e nuova tecnologia sul mercato, la blockchain. La blockchain è un registro elettronico distribuito, condiviso da tutti gli utenti che ne vogliano far parte, è decentralizzata, pubblica e immodificabile, tre proprietà che sembrano proprio far al caso nostro. La totale trasparenza della blockchain, unita alla sua fase di criptazione per mantenere l'anonimato degli utenti, è la piattaforma perfetta per una votazione. Nei prossimi capitoli spiegherò dettagliatamente il motivo della scelta di blockchain e i vari vantaggi che ne derivano.

Capitolo 2

Tecnologie di voto

Nella società di oggi, dove la tecnologia sta facendo passi da gigante, è difficile comprendere perché i governi non abbiano ancora convertito il sistema di elezione basato sulla carta in forma digitale in modo da eliminare frodi e corruzione.[13]

2.1 Il voto tradizionale

L'articolo 48 della costituzione italiana sancisce che : "*Il voto è personale ed eguale, libero e segreto.*". Il voto su carta venne introdotto per la prima volta a Roma nel 139 a.C. e per l'epoca fu un grosso passo avanti. Tuttavia questa antica tecnologia offriva un modesto rispetto della privacy ed era facilmente preda di varie forme di frodi elettorali. Il moderno sistema elettorale che prevede sempre l'utilizzo di carta venne utilizzato in Australia nel 1858 per la prima volta. La grande innovazione australiana fu quella di stampare schede di voto standard a spese del governo, distribuite ai votanti nei seggi elettorali e richiedeva che i votanti votassero in loco e le restituissero immediatamente. Il sistema australiano correttamente eseguito, aumentava lo standard di voto, garantendo privacy e assicurando un imparziale e corretto conteggio dei voti.[1]

2.1.1 I problemi

Le frodi

Questa tecnologia però poteva essere comunque soggetta a numerosi tipi di frodi, ad esempio se si deve effettuare un segno sulla carta, ci saranno sicuramente dei voti che saranno a metà tra il poter essere accettati e non. Il che verrebbe poi deciso al momento dello spoglio dei voti dal personale incaricato che potrebbe decidere di

invalidare voti anche qualora sia chiara l'intenzione del votante. Più nello specifico, un partito al potere potrebbe fare in modo che il personale dell'opposizione nei seggi sia poco qualificato mentre istruendo invece quelli dalla propria parte in modo che applichino aggressivamente le regole sui voti sfavorevoli in modo da manipolare le sorti dell'elezione. Secondo l'enciclopedia britannica del 1910, era comune per molte giurisdizioni che venissero eliminati fino ad un 40% di voti dal conteggio.

I costi

Un altro grosso problema risiede nel fatto che il processo di spoglio dei voti richiede moltissima mano d'opera, basti pensare al numero di edifici che devono essere convertiti a seggi elettorali in vista di un'elezione e quanto personale deve essere impiegato. Il tutto senza tener conto dell'esorbitante costo delle elezioni, nel 2013 il costo complessivo sostenuto dal Ministero dell'interno si aggirava intorno ai 315 milioni di euro Siamo tutto a conoscenza che il sistema di voti cartaceo sia fallato, e incline alla corruzione. Prendiamo ad esempio l'ultima elezione haitiana che venne invalidata a causa di schede elettorali fasulle prodotte a Dubai che furono inserite insieme alle altre schede elettorali per eleggere illegalmente il presidente. Per far fronte a questo danno lo stato haitiano ha dovuto pagare approssimatamente una cifra di 100 milioni di dollari, senza la sicurezza che ciò non possa riaccadere. Un altro esempio avvenne in America, quando finirono le schede elettorali e ne dovettero stampare altre, che stamparono su carta bianca invece che su quella apposita perchè non era presente. Le persone corsero ai seggi per compilare le schede e votare ma il tutto ovviamente non era tracciabile e quindi venne compromessa la veridicità della votazione.

Gli italiani all'estero

Anche noi in Italia abbiamo grossi problemi, soprattutto per quanto riguarda le votazioni dei cittadini italiani all'estero. Questi ricevono una busta contenente una scheda elettorale non timbrata, una busta per imbustare la scheda e le istruzioni. Già dal momento che queste buste vengono recapitate viene riscontrata la prima falla, essendo di dimensione maggiore di quella di una normale cartolina, i postini le lasciano notoriamente sporgere dalla buchetta il che le rende facili prede di organizzazioni che si occupano proprio della vendita di voti. A questo punto una persona qualunque può fingersi di esserne un'altra, compilare la scheda ed inviarla al consolato italiano, che la deve convalidare ed inviare in Italia. Se non vi erano state delle frodi precedenti, al consolato dovrebbe arrivare la busta correttamente, ma lui stesso potrebbe a questo punto invalidare la scheda, oppure utilizzandone

un'altra cambiare a proprio piacimento il voto. Il tutto considerando che bisogna essere fortunati che le varie spedizioni non sforino il limite di tempo entro il quale le buste devono tornare in Italia per essere considerate valide. Si conta che ad oggi vi siano 4,3 milioni di italiani all'estero aventi diritto di voto, quindi un numero che potrebbe in alcuni casi potrebbe far prendere una determinata piega alla votazione.

2.1.2 Per concludere

Per concludere, continuando ad usare il metodo antiquato della votazione su carta, risulta troppo facile corrompere il sistema, facendo in modo che la voce del popolo non venga chiaramente ascoltata, o annegata completamente dalle frodi. Se la voce del popolo non è il pilastro dell'elezione, allora l'elezione stessa non ha motivo di esistere. Le elezioni fraudolente e politici corrotti hanno portato diverse nazioni ad essere in regimi dittatoriali piuttosto che in democrazia, dove i fondi pubblici vengono utilizzati per scopi privati anziché utilizzati per migliorare la vita delle persone e costruire infrastrutture. Tutto questo spinge a pensare che i governi che sono in carico di dirigere sistema elettorale forse siano parte del problema.

2.2 Primi progressi verso la digitalizzazione

Durante la storia ci sono stati numerosi tentativi nel cercare di migliorare il sistema di voto, purtroppo nel tentativo di chiudere una falla ne venivano sempre aperte altre. Vi presento ora una serie di dispositivi che sono stati introdotti all'incirca durante l'ultimo secolo e rappresentavano l'avanguardia della tecnologia dell'epoca e il punto di partenza da cui verranno poi sviluppati sistemi molto più efficienti di votazione elettronica che sono attualmente in uso in determinati stati. [8]

2.2.1 Macchina di voto a leva

Le macchine di voto a leva vennero introdotte per la prima volta a New York nel 1892, e furono adottate in tutta la nazione, a discrezione dei governatori, ad esempio in stati con piccole città come l'Iowa, non vennero mai utilizzate. Furono molto utilizzate nella metà del ventesimo secolo e anche se fuori produzione dal 1982, vengono ancora largamente utilizzate. Hanno completamente eliminato gran parte degli approcci utilizzati in passato per manipolare il voto, offrono una discreta privacy e la leva rassicura il votante da un punto di vista psicologico. Sono però

macchine estremamente ingombranti, molto costose difficili da testare e complesse da mantenere. Ancora, con una macchina di voto a leva, non è possibile effettuare un secondo conteggio dei voti, in quanto i dati non viene lasciata una traccia per poter rieffettuare il conteggio, come invece si fa con le schede elettorali. Questi tipi di macchine non erano altro che una soluzione veloce al problema di un secolo fa, però introducendone nuovi, ad esempio, un tecnico poteva impostare una macchina in modo che dopo un determinato numero di voti a favore di un determinato partito, questa non registrasse più voti per quel partito, e questo stratagemma sarebbe risultato estremamente difficile da scoprire.

2.2.2 Schede perforate

La prima nuova tecnologia in grado di competere con la macchina di voto a leva, fu il famigerato Votomatic. Le schede perforate erano già state introdotte da IBM negli anni 90 dell'ottocento, ma il Votomatic non venne introdotto fino al 1964. Il beneficio principale risiedeva nel poter ricontare i voti in caso di problemi, ma, come succede sempre, vennero introdotti altri tipi di problemi. Noi tutti siamo in grado di interpretare segni sulla carta, siamo stati allenati a fare ciò sin da quando eravamo all'asilo, e questa abilità è un fattore chiave nello spoglio dei voti con il metodo tradizionale su carta che ci permetteva di riconoscere segni fatti apposta contro macchie o difetti della carta . Per quando riguarda le schede perforate, un foro non imperfetto, o un pezzo di carta che penzola equivale a quei difetti accidentali che si potevano avere su carta, ma non abbiamo la stessa esperienza per poterli riconoscere. Inoltre vi era un altro grosso problema, Votomatic era uno strumento che serviva per esprimere il proprio parere, e dopo averlo utilizzato la scheda che era anonima diventava anche illeggibile, senza lo strumento non si riusciva a verificare che i fori corrispondessero, quindi diveniva impossibile controllare che il voto fosse stato espresso correttamente. Questo problema era talmente grande che IBM nel 1970 abbandonò questa tecnologia e nel 1988 il National Burerau of Standards pubblicò un articolo di Saltman raccomandando l'immediato abbandono di questa tecnologia.

2.2.3 Scanner ottico

Questa tecnologia venne sviluppata negli anni '70 dall' American Information Systems of Ohama, e essenzialmente utilizzava la capacità di riconoscere i segni sulla scheda al posto dei fori delle precedenti schede perforate. Un grosso vantaggio, il che significava che non vi era bisogno di speciali macchine per poter votare, e quindi

un votante poteva verificare facilmente se aveva votato correttamente oppure no; le schede venivano poi inserite all'interno della macchina che si occupava di leggere i voti ed effettuare lo spoglio. Sfortunatamente la prima generazione di macchine era particolarmente sensibile ai tipi di penne utilizzate per segnare la scheda e come risultato molte macchine erano in difficoltà nel riconoscere segni corretti da altri segni accidentali sulla carta, il che creava confusione e o l'annullamento del voto. Le generazioni moderne di questo tipo di macchine ad oggi processano le immagini con sensori infrarossi diminuendo notevolmente la possibilità di errori.

2.3 E-voting

Con l'evoluzione della tecnologia diventa ovvio considerare l'utilizzo dei computer per le elezioni, in particolare sistemi di voto distribuiti che utilizzano internet per la realizzazione di queste elezioni (e-voting system). Per accedere ad un sistema di voto, gli utenti potranno usare computer, smartphone e tablet, e questi sistemi garantiranno l'anonimato durante il voto in modo da rispettare i diritti dei cittadini, più avanti parleremo di tutte le proprietà che dovranno essere rispettate da questi sistemi. I sistemi di voto elettronici devono essere facili da usare, sicuri, e cercano di eliminare l'errore umano. Questi sono obiettivi difficili da raggiungere, perché richiedono una forte criptazione per garantire sicurezza, integrità ed anonimato del voto. Il tutto deve inoltre avere un'interfaccia user-friendly che è spesso complicata da realizzare. Uno dei principali vantaggi dei sistemi elettronici di voto è la possibilità di ottenere un'elezione completamente verificabile, il che significa che tutti i votanti possono verificare se il proprio voto è stato contato correttamente e lo spoglio dei voti effettuato correttamente. Alcune nazioni utilizzano macchine per votare nei seggi, (mi riferisco a dei dispositivi elettronici che non utilizzano internet e sono dei terminali con un display touch-screen), queste macchine sono utilizzate esclusivamente per il voto e sono in grado di contare direttamente il voto, oppure creare una ricevuta che andrà successivamente contata. Solitamente non è possibile verificare i passaggi che eseguono queste macchine perché la case produttrici non rilasciano i dettagli dell'implementazione, e non si sa come queste macchine operino in realtà. Dopo l'analisi di numerose macchine da parte del Chaos Computer Club (CCC), la più grande organizzazione di hackers europea, hanno riassunto il risultato della ricerca in una frase: *"Trust is a good thing, control not possible"* il che significa che queste macchine sono state ritenute da esperti di sicurezza inaffidabili in quanto avevano lacune nella sicurezza e nella verificabilità del voto, e che queste macchine dovevano essere bandite dalle elezioni. La mancanza di verificabilità ha fatto si che

queste macchine fossero proibite per le elezioni in Germania, e dal momento che il voto di un cittadino non possa essere verificato, queste macchine sono state proibite per le elezioni parlamentari. [11]

2.3.1 Proprietà

Gli e-voting system devono essere sicuri almeno quanto quelli tradizionali su carta. Come abbiamo visto in precedenza i metodi tradizionali però hanno numerose falle che nei sistemi elettronici online, grazie all'uso della criptografia vengono eliminati, il che sarebbe un grosso punto a favore per gli e-voting systems. [10] Vediamo ora una serie di proprietà che questi sistemi devono rispettare:

- **Disponibilità**: Un e-voting system deve rimanere disponibile per l'intera durata dell'elezione, e deve essere a disposizione dei votanti che si connettono tramite l'uso dei loro dispositivi

- **Idoneità**: Solo i votanti idonei hanno la possibilità di esprimere un voto, e solamente un voto per persona può essere espresso. Se in alcuni casi particolari vi fosse la possibilità di votare più di una volta, l'ultimo voto sarebbe quello ritenuto valido.

- **Integrità**: L'integrità del voto deve essere garantita, gli e-voting devono garantire che i voti non vengano alterati durante nessun passaggio delle elezioni, altrimenti il sistema non potrebbe essere considerato affidabile.

- **Segretezza**: La connessione tra il voto e l'utente che ha votato non deve poter essere ricostruibile senza l'aiuto del votante.

- **Correttezza**: Lo spoglio dei voti deve essere effettuato correttamente, e il risultato pubblicato deve essere quello corretto.

- **Robustezza**: Il sistema dovrebbe essere in grado di tollerare alcuni voti nulli. Deve inoltre venir considerata la possibilità di utenti malintenzionati che proveranno ad inserire voti maligni, i quali devono essere identificati. Un sistema di voto deve riconoscere questo tipo di voto per prevenire la manipolazione dei voti o attacchi ai servers.

- **Verificabilità**: Dopo il processo di spoglio dei voti i risultati devono essere pubblicati e poter essere verificabili da tutti, ovvero la piattaforma deve consentire di poter verificare il risultato dell'elezione. Inoltre il votante stesso

deve avere la possibilità di verificare che il proprio voto sia arrivato a destinazione, il che garantisce che il votante sia sicuro che il proprio voto non sia stato modificato e sia venuto contato.

- **Equità**: I sistemi di voto devono garantire che non vengano presentati risultati parziali prima della fine delle elezioni. Altrimenti i votanti potrebbero essere influenzati dai risultati e votare differentemente.

- **Libertà di scelta**: Il sistema deve contenere sistemi di sicurezza in grado di evitare che il votante sia costretto a votare per uno specifico partito, candidato etc. Il sistema di voto deve essere costruito in modo da garantire che il votante possa votare liberamente anche nel caso in cui venga costretto. Anche la vendita del voto deve risultare poco attraente o troppo costosa. La coercizione è ancora un grosso problema tra i sistemi di voto.

Queste proprietà sono necessarie per un corretto e sicuro sistema e-voting ed aggiungono complessità e rendono lo sviluppo di un design sicuro e di un'interfaccia user-friendly più complicata. La grande sfida per i sistemi di voto consiste nel soddisfare più proprietà possibili, e creare un sistema di voto sicuro facile abbastanza da essere compreso ed utilizzato da tutti.

2.4 Il sistema I-voting dell'Estonia

L'Estonia è una nazione moderna che fa largo uso dell'internet anche per scopi burocratici, al contrario dell'Italia. È praticamente possibile fare qualsiasi operazione grazie alla combinazione di internet e della loro carta d'identità elettronica, oppure del mobile-id tramite smartphone. Queste ID sono anche utilizzate per effettuare l'e-voto e l'elezione del governo del 2005 fu la prima elezione dove i cittadini poterono votare tramite internet. [5, 4]

2.4.1 ID

Le carte d'identità elettroniche vengono realizzate sulla Java chip platform e contengono 2048 bit, protette da pin, e tramite criptografia RSA possono creare firme SHA1 , SHA2. Quindi sono conformi alle comuni pratiche di sicurezza adottate sul web e permetto di autenticare, criptare e firmare. Dal momento che è il governo a distribuire questi ID, il governo tiene traccia della chiave pubblica dei cittadini,

quindi l'autenticazione al sistema di voto elettronico è facile perché il votante ha solo bisogno di creare la sua firma digitale tramite la tessera, inviare la firma al server di autenticazione dell'applicazione e viene autenticato tramite la PKI (Public Key Infrastructure) del governo.

2.4.2 La piattaforma

Il client I-voting è stato sviluppato per la maggior parte dei sistemi operativi tra cui Windows, Linux, Mac OS X, e l'applicazione guida il votante durante il processo di voto. La versione pubblicata del sistema include la chiave pubblica dell'elezione e la comunicazione con il data-center dell'elezione viene effettuata tramite connessione HTTPS. Il codice del nucleo del server dell'e-voting estone è stato reso open-source, mentre il client 'I-voting, gli script per inserire un voto e i driver per il modulo di sicurezza hardware (HSM) rimangono segreti. L'HSM è utilizzato per decriptare e contare i voti e pubblicare il risultato finale. Quindi gran parte dell'applicazione può essere testata per problemi relativi alla sicurezza, ma senza poter controllare completamente l'intero sistema la totale sicurezza non è garantita. Uno snapshot del codice del nucleo del server viene pubblicato su git-hub prima dell'inizio dell'elezione. I tecnici non vogliono pubblicare il codice del client I-voting per ragioni di sicurezza, secondo loro diventerebbe troppo facile per gli attaccanti creare una finta applicazione di voto identica all'originale.

2.4.3 Processo di voto

Il votante deve scaricare l'applicazione tramite internet da uno dei siti web autorizzati. Come primo passo deve autenticarsi tramite la propria ID, e se è idoneo gli verrà presentata una lista di candidati tra cui scegliere. Il voto viene criptato con la chiave pubblica dell'elezione, firmato con la propria chiave privata e mandato al server incaricato dell'inoltro dei voti che controllerà se il voto è stato criptato correttamente e provvederà ad eseguire l'inoltro verso il server che si occupa di tenere i voti e scriverà un log in un server apposito che detiene i registri di log. Questi tre server sono all'interno del data-center controllato dalle autorità dell'elezione. Per la verifica del voto, il client I-voting genera un token che non può essere indovinato, impacchettato all'interno di un QR-code, che potrà essere letto tramite l'applicazione installata sullo smartphone del votante. Scannerizzando il QR tramite l'applicazione del votante, rivelerà il candidato per cui ha votato e questa operazione è solamente disponibile entro 30 minuti dall'invio del voto al data-center. Il votante ha la possibilità di votare più di una volta, e solamente l'ultimo voto sarà quello considerato

valido, per evitare coercizione e vendita di voti. È anche possibile votare tradizionalmente utilizzando la carta, recandosi ad un seggio elettorale, il che invalida la votazione elettronica, perché alla votazione su carta viene data la priorità.

2.4.4 Spoglio dei voti

I voti sono composti come se avessero una doppia custodia, quindi la connessione tra il votante e il voto è ancora presente. Come primo passo questa connessione deve essere rimossa prima che il voto venga decriptato, quindi la firma del votante deve essere cancellata dal voto. Questo processo viene eseguito sul server che si occupa di detenere i voti e quindi quest'ultimi vengono resi anonimi, quindi scritti su un DVD e trasferiti tramite air-gap (un'ulteriore misura di sicurezza) al server incaricato di effettuare lo spoglio dei voti che non ha connessione a internet e quindi diminuisce notevolmente la possibilità di essere compromesso o che venga infettato con del codice maligno. Quindi questo server viene connesso al modulo HSM che è incaricato di decriptare i voti. La chiave privata dell'elezione viene distribuita tramite più autorità che hanno il compito di cooperare e creare la chiave privata. Tramite questa chiave i voti possono essere decriptati e contati. Per ultimo, il risultato dell'elezione e le varie statistiche vengono rese pubbliche tramite il sito ufficiale.

2.4.5 Sicurezza

Il sistema estone utilizza numerose primitive crittografiche, ma presenta comunque numerose falle, che andrò a brevemente a descrivere.

Sicurezza delle operazioni

Alex Halderman insieme a tre membri del suo team, dell'università del Michigan venne nominato ufficialmente come controllore di un'elezione nel 2013, e il team pubblicò il risultato dello studio online i problemi di sicurezza procedurali e operazionali:

- Venivano utilizzati dei personal computer per preparare il software per l'elezione
- Erano presenti delle telecamere di sicurezza per controllare il personale addetto alla creazione del software ma la sorveglianza non era 24/7
- Le password del wifi erano appese al muro e venivano registrate dalla video camera, le telecamere erano in grado di vedere cosa stessero scrivendo i tecnici

e una delle telecamere fu persino in grado di vedere la password di root per accedere ad uno dei server.

Dal momento che i developer del software utilizzavano il loro computer per sviluppare, il quale aveva fatto download di software da canali non sicuri, poteva essere possibile per un attacker inserire codice che veniva scaricato da una fonte sconosciuta. Questa falla poteva essere utilizzata da un attacker per prendere controllo della macchina di un developer e compromettere i risultato di un'elezione, compromettendo i voti. Dal momento che l'interno sistema non è open source, vi è la possibilità che codici maligni risiedano nella parte privata del codice. Un altro grande problema consiste nel fatto che gli amministratori erano spesso da soli con i server, anche se il regolamento prevedeva tassativamente la presenza di almeno due persone per lavorare sui server, il che rendeva il sistema potenzialmente a rischio di un attacco interno.

Sicurezza tecnica

Il sistema è vulnerabile ad attacchi di livello di stato, come compagnie di intelligence, queste compagnie hanno accesso a gran parte del traffico di internet, abbastanza capacità da poterlo salvare ed analizzare ed effettuare un attacco temporale. Quindi un attacker potrebbe misurare il tempo che un pacchetto impiega per comunicare con il server, e identificare con una certa percentuale di riuscita che un determinato individuo ha piazzato il proprio voto.

Infrastrutture centralizzate

Tutti i server sono all'interno dello stesso data-center, e quindi il sistema è vulnerabile ad attacchi DDoS o simili. Rendendo il server distribuito, si avrebbe un più alto livello di disponibilità, ma sarebbe più complicato e costoso rispetto a tenere tutti i server in una sola location. Inoltre sarebbe anche più complicato rendere sicuri server distribuiti e le loro comunicazioni.

Attacchi Client-side

Come in tutte le applicazioni eseguite sui computer dei votanti, gli attacchi client-side sono possibili, questi mirano a manipolare il computer del votante. Agenzie di intelligence, come la BND in Germania, hanno un budget separato solo destinato all'acquisto di zero-day-exploits per avere il controllo dei sistemi operativi, quindi la manipolazione del voto dal computer del votante sarebbe possibile e non verrebbe rilevata dal votante stesso.

Conclusione

Le tessere ID utilizzano funzioni crittografiche sicure, con PKI controllata dal governo, il che semplifica il processo di autenticazione al sistema di voto da parte dei votanti. Non vi sono credenziali spedite via posta o tramite altri mezzi non sicuri, il che è un punto a favore di questo sistema. Usano primitive crittografiche molto comuni in modo che il sistema possa essere realizzato tramite le conoscenze tecnologiche presenti in Estonia il che rappresenta un enorme vantaggio per il governo in quanto non si è dovuto affidare ad altri stati o compagnie per lo sviluppo del sistema di voto. La trasparenza è stata ottenuta tramite un processo di voto ben documentato ed il codice open-source. La verificabilità del voto viene ottenuta tramite lo scan di un codice QR dopo l'effettuata votazione che mostra la scelta effettuata e il corretto adempimento della votazione. Permettendo voti multipli si limita la coercizione, tuttavia il sistema non è protetto da attacchi temporali con la conseguente possibilità di osservare un gruppo di elettori e dimostrare che hanno votato, indipendentemente da quale partito.

2.5 Il sistema iVote del South Wales

L'Australia iniziò il più grande utilizzo di sistemi e-voting della storia, circa il 5% dei votanti utilizzo questo nuovo sistema per le elezioni di stato nel 2015 nel South Wales. Il sistema è stato implementato con l'aiuto della piattaforma Scytl. [14]

2.5.1 Sistema di voto

iVote è un sistema interamente closed source fornito da un sito web Java-script. I votanti devono registrarsi prima della votazione per ricevere le credenziali, un ID ad otto cifre e impostare il loro pin di sicurezza a sei cifre. Con le credenziali possono a quel punto identificarsi sul portale https://cvs.ivote.nsw.gov.au e piazzare il loro voto durante l'elezione. Questo sistema era stato pensato per votanti che non erano in Australia al momento della votazione o persone incapaci di raggiungere i seggi elettorali. Per fare un test di prova, la commissione elettorale del South Wales preparò una finta elezione raggiungibile tramite un diverso indirizzo utilizzando però gli stessi software che saranno poi stati utilizzati nelle elezioni reali. Ci sono tre possibilità per votare con iVote, si può usare il telefono, si può usare internet, oppure si possono utilizzare i computer predisposti ai seggi elettorali. Il voto viene criptato localmente tramite una libreria JavaScript e inviato al server di verifica. A questo punto il votante riceve una ricevuta per verificare il proprio voto con sistema

telefonico automatico, oppure online tramite il server incaricato. Il votante deve a quel punto inserire il proprio ID di voto il Pin e il numero della ricevuta e potrà verificare che il proprio voto sia stato regolarmente contato. La verifica tramite telefono si ferma quando l'elezione termina, mentre la verifica online rimane attiva anche ad elezione conclusa. Essere capace di dimostrare per quale candidato o partito si ha votato è simile ad ottenere una ricevuta e questo meccanismo è quindi suscettibile a coercizione. Questa non è una buona soluzione in quanto coercizione e contrabbando di voti sono un grosso problema dei sistemi di voto. Anche la descrizione del sistema stesso è inconsistente, ad esempio esistono varie descrizioni di come vengono criptati i voti, alcuni affermano di utilizzare AES simmetrico con il numero di ricevuta per criptare il voto, oppure ancora ElGamal con la chiave pubblica dell'elezione. Halderman ed il suo team scoprirono che entrambi i sistemi venivano utilizzati, in poche parole non è una descrizione che un sistema di voto degno di fiducia dovrebbe avere, anzi dovrebbe essere il più chiaro possibile.

2.5.2 Processo di spoglio

Analizzare il processo di spoglio dei voti non è possibile, perché non ci sono pubblicazioni in merito e non è stato reso pubblico il source code. L'ufficio della commissione elettorale del South Wales descrive il processo nella home-page come : *"The ballot is decrypted, audited and counted"*, ovvero il voto viene decriptato, controllato e contato.

2.5.3 Problemi relativi alla sicurezza

Closed source

Non è possibile fare peer-review del codice in quanto non è stato reso pubblico. Questo non è un buon modo di operare, perché in questo modo solo un piccolo numero di persone hanno accesso al source-code e sono in grado di verificare che il codice sia privo di bugs o codice maligno. Creare un sistema di voto open-source è indispensabile per un sistema di cui ci si deve fidare durante un'elezione.

Coercizione

In questo sistema non vi è nessun meccanismo in grado di proteggere i votanti dalla coercizione, un votante ha solo bisogno di alcuni credenziali ed è capace di votare. Quindi la vendita dei voti e la coercizione possono essere un grandissimo problema da non sottovalutare in questo sistema di voto.

Anonimato ed attacchi temporali

Questo sistema ancora è suscettibile ad attacchi network-level, in quanto non sono stati resi disponibili meccanismi per rendere i votanti anonimi dagli sviluppatori di iVote. Per l'elezione del 2015, Halderman e Vanessa Teague iniziarono la loro indipendente analisi di sicurezza del sistema iVote e resero pubblici i risultati. Dal momento che iVote è closed-source, Halderman et al. poterono solo analizzare la web-app, ma non potevano votare quindi si limitarono ad analizzare solamente il codice HTML e JavaScript della web-app e riscontrarono un problema grave.

FREAK attack

La web-app usa, come avviene comunemente, più server per caricare i file JavaScript che servono all'applicazione. Due settimane prima che l'elezione iniziasse ci fu il FREAK attack (Factoring RSA Export Keys) che fece molto scalpore: era possibile effettuare il downgrade della criptazione SSL/TSL a 512 bit RSA su alcuni web-server vulnerabili oppure vecchi browser. Questo attacco rendeva possibile fattorizzare la chiave RSA in meno di sette ore grazie al potere computazionale noleggiabile su Amazon per circa 100 dollari. Come risultato di questo downgrade, diveniva possibile impersonare un web-server ed effettuare attacchi man-in-the-middle. Nel nostro caso iVote scaricava un file JavaScript dal Piwik's enterprise service i cui server erano vulnerabili all'attacco FREAK. Halderman et al. scoprirono questa falla e la comunicarono ai tecnici di iVote. L'ufficio della commissione elettorale del South Wales reagì e scartò il file JavaScript dal web-server non sicuro, ma durante questo lasso di tempo era stato teoricamente possibile manipolare i 66 mila voti che erano già stati piazzati. Utilizzando questo attacco era possibile impersonificare i server di Piwik e manipolare codice JavaScript ad esempio per modificare o scartare dei voti. Il votante non si sarebbe mai accorto che il suo voto non era stato realmente piazzato perché modificando il codice JavaScript sarebbe stato facile copiare il sistema telefonico automatico di verifica, cambiare il numero di telefono che il votante avrebbe visualizzato dopo la votazione sul display e confermare al votante che il voto era stato piazzato correttamente. Cambiare i contenuti di un sito web è molto semplice quando si ha accesso ai file JavaScript. Quindi il votante potrebbe non essere in grado di notare che il proprio voto sia stato manipolato. Il bug FREAK venne chiuso durante l'elezione dopo che Halderman contattò le persone responsabili.

Conseguenze

La vulnerabilità FREAK rende possibile l'idea che un attacker abbia potuto manipolare i voti di 66 mila persone che sono stati venuti contati durante l'elezione. Questa era una vulnerabilità di livello critico in quanto solo 3177 voti erano necessari per decidere ci avrebbe ottenuto l'ultimo posto disponibile nel Consiglio Legislativo. Quindi l'attacco potrebbe aver avuto un impatto sul risultato dell'elezione, ma non vi è purtroppo la possibilità di controllare retroattivamente se la votazione fu compromessa dalla vulnerabilità.

Conclusione

Questo sistema di voto è puramente web-based, che è un vantaggio, perché l'utente non deve installare nessun software sul proprio terminale. La criptografia viene completamente realizzata tramite JavaScript nel Web-browser, il che non è un problema in quanto queste tecnologie sono abbastanza potenti per questo compito. La mancanza di descrizione del sistema porta ad una mancanza di fiducia nel voto, non vi è possibilità di verificare che il processo di voto sia corretto. In alcuni casi iVote, si affida al telefono per effettuare il voto e per la verifica dei votanti. Non vi è però descrizione riguardo la crittografia della telefonata, quindi si assume che non sia presente il che è una potenziale falla nella sicurezza. Riassumendo, i tecnici del sistema sembrano ignorare i progressi e le buone pratiche contemporanee utilizzate in altri sistemi.

Capitolo 3

Blockchain

3.1 Introduzione

Blockchain al momento è una delle principali buzzwords nel mondo della tecnologia e della finanza. La principale applicazione della blockchain fu nel 2009 per Bitcoin, che è una cryptocurrency e blockchain è la tecnologia che sta alle sue spalle. Il termine cryptocurrency si riferisce ad una moneta virtuale che funziona tramite una blockchain. Bitcoin nasce dal genio di una misteriosa persona o di un gruppo di persone conosciuta come Satoshi Nakamoto. Nessuno conosce l'identità di Nakamoto ma la loro visione fu svelata nel 2009 su un whitepaper chiamato *"Bitcoin: A Peer-to-Peer Electronic Cash System."*[9]

Con il termine Blockchain si intende un metodo digitale di registrazione di transazioni che rende le informazioni in esse contenute accessibili, visibili e, soprattutto non alterabili, con la conseguenza che non c'è più bisogno di una autorità centrale che tenga sotto traccia tutti gli stadi di una transazione.

Attualmente Bitcoin è utilizzato per il più grande sistema di pagamento peer-to-peer e fu sviluppato come alternativa alla moneta tradizionale, troppo centralizzata e regolata, secondo i suoi creatori.[12]

3.1.1 Funzionamento

Blockchain è un database distribuito dove tutti i dati sono condivisi tra i partecipanti della rete. I dati che dovrebbero essere salvati all'interno di questo database sono impacchettati in blocchi con una dimensione massima predefinita e verificati con uno specifico hash. Questo hash deve iniziare con un numero specifico di zero che dipenderà dal numero di partecipanti sulla rete. Per ottenere ciò i partecipanti

aggiungono dei nonce ai dati del pacchetto cercando di trovare l'hash corrispondente modificando questo nonce. Questa proof-of-work viene chiamata mining. Il mining è utilizzato per generare bitcoin. A colui che riuscirà a trovare l'hash corretto per un determinato pacchetto sarà corrisposta una determinata cifra di bitcoin. Il numero di bitcoin di remunerazione per blocco viene regolata dal protocollo bitcoin e di media vengono richiesti 10 minuti per scoprire questo hash. Generalmente gli hash vengono scoperti da pool di miner, ovvero agenzie con un potere computazionale inimmaginabile che raggruppano all'interno svariate unità di miner.

I dati all'interno di bitcoin vengono rappresentati come transazioni tra uno o più utenti. Dal momento che le transazioni sono pubbliche, ogni utente conosce il capitale in bitcoin di tutti gli altri utenti. Prima che le transazioni vengano aggiunte alla catena, queste vengono controllare in modo da verificare che i capitali non siano già stati spesi precedentemente ed evitare double-spending. Questa verifica è resa possibile dal fatto che le transazioni sono salvate pubblicamente all'interno della blockchain.

Ci sono due modi di partecipare alla blockchain:

- Si può diventare un nodo della blockchain, il che risulterebbe nell'avere salvata localmente sul proprio terminale la blockchain. Questi nodi verificano gli hash dei blocchi, per garantire integrità alla catena, e si scambiano la blockchain tra di loro in modo da mantenere uno stato comune.

- Oppure si può diventare miners, ovvero vengono collezionate transaction da una transaction pool e si inizia la ricerca dell'nonce per generare l'hash corrispondente. Se l'hash viene trovato, la scoperta viene trasmessa a tutta la rete in modo che i nodi possano verificare il blocco e il miner verrà remunerato.

Questa è l'idea generale della blockchaine del primo protocollo che l'ha utilizzata (Bitcoin). Dal momento che la blockchain è open source gli sviluppatori possono utilizzare approcci differenti per verificare i blocchi che andranno salvati all'interno della blockchain vengono anche utilizzate proof di verifica differenti. Nel protocollo bitcoin la blockchain è utlizzata per condividere transazioni tra gli utenti. Ogni utente ha un portafoglio privato ed è in grado di acquistare bitcoin che poi potrà di spendere.

Tutte le transazioni sono pubbliche e disponibili e la blockchain comincia con il blocco genesi che è il primo blocco mai minato. Il blocco successivo viene collegato

al blocco genesi e così via. Questo procedimento crea una lunga catena di blocchi per questo viene chiamata blockchain.

In alcuni casi è possibile che due blocchi vengano minati esattamente allo stesso momento, e per via del lag di rete, in due parti del mondo diverse venga percepita una blockchain diversa, il così detto soft-fork. Generalmente questi fork vengono richiusi al blocco successivo, perché nel primo istante in cui ad uno dei due rami viene aggiunto un altro blocco, questo diventa il ramo più lungo e quindi il ramo più corto viene scartato. La probabilità che ciò avvenga è pressoché nulla, ma in tal caso le transazioni all'interno del blocco del ramo che viene scartato vengono annullate e reinserite nel pool delle transazioni, motivo per cui si aspetta solitamente sei blocchi prima di considerare una transazione verificata.

3.2 Algoritmi di consenso

Blockchain è un sistema peer-to-peer decentralizzato senza alcuna autorità centrale. Questo sistema previene la corruzione ma crea però dei problemi, ad esempio come vengono prese le decisioni. Si pensi ad esempio ad una organizzazione centralizzata, tutte le decisioni vengono prese dal capo, o da un gruppo di persone in incaricate di prendere decisioni, ma questo non è il caso di Blockchain perché blockchain non ha leader. Per Blockchain per prendere decisioni vi è bisogno di consenso ottenuto mediante meccanismi di consenso.[6]

Il consenso è un metodo dinamico di raggiungere un accordo all'interno di un gruppo. Mentre con il voto si utilizza la maggioranza per prendere una decisione, andando a scapito della minoranza, con il consenso si ha la certezza che l'intero gruppo beneficerà dall'accordo a cui si è arrivati. Da un punto di vista idealistico il consenso può essere utilizzato da un gruppo di persone sparse per il mondo per creare una società più equa e giusta. Un metodo che consente di prendere decisioni tramite il consenso viene chiamato meccanismo di consenso. Vediamo ora gli obiettivi di un meccanismo di consenso:

- **Ricerca dell'accordo**: Un meccanismo di consenso dovrebbe trovare l'accordo del maggior numero di persone all'interno del gruppo
- **Collaborazione**: Tutti i partecipanti devono lavorare insieme per ottenere un risultato che mette per primo l'interesse dell'intero gruppo
- **Cooperazione**: Tutti i partecipanti devono mettere i loro interessi da parte e lavorare come un team al posto che come individui.

- **Egualità**: Un gruppo che cerca di ottenere il consenso deve essere il più egualitario possibile, ovvero il voto di una persona non può essere più importante di quello di un'altra.
- **Inclusività**: Più persone possibili dovrebbero essere incluse nel processo di consenso, non dovrebbe essere come le normali votazioni dove le persone non se la sentono di votare perché pensavo che il loro voto conti poco
- **Partecipazione**: Il meccanismo di consenso dovrebbe essere fatto in modo che chiunque debba partecipare attivamente nell'intero processo.

Ora che abbiamo definito che cosa sono i meccanismi di consenso, e a che cosa dovrebbero puntare, andremo ad analizzare i meccanismi di consenso più famosi ed utilizzati ai giorni nostri.

3.3 Proof of Work

Proof of work è un protocollo il cui obiettivo primario è quello di funzionare come deterrente per attacchi DDoS (Distributed Denial of Service) che hanno lo scopo di esaurire le risorse di un computer inviando multiple richieste fasulle. Il concetto di Proof of Work esisteva ancora prima di Bitcoin, ma fu Satoshi Nakamoto che applicò questo protocollo alla sua criptovaluta rivoluzionando il modo in cui le transazioni venivano eseguite. Il PoW è probabilmente la più grande idea del white paper di Nakamoto ([12]) perché permetteva di ottenere il consenso distribuito anche in mancanza di fiducia tra le parti. Un sistema di consenso distribuito trustless (trustless and distributed consensus system) significa che se vogliamo inviare o ricevere denaro da qualcuno non dobbiamo affidarci a servizi di terzi per avere certezza della validità dell'operazione. Quando usiamo metodi di pagamento tradizionali dobbiamo affidarci a terzi per validare la nostra transazione (es Visa, Mastercard, PayPal, banche ecc). Loro posseggono il loro registro privato con all'interno lo storico delle transazioni e il saldo di ogni conto. Con Bitcoin ed altre digital currency, tutti hanno una copia del libro mastro, quindi non c'è bisogno di affidarsi a terze parti, perchè ognuno può direttamente verificare le informazioni che vi sono scritte [7].

3.3.1 Mining

Andando più in profondità, il PoW è un requisito per definire un calcolo computazionale molto costoso, il mining, che deve essere effettuato per creare un gruppo di transazioni trustless (chiamato blocco) su un distribuited ledger che è blockchain. Il mining ha due scopi principali:

- Verificare che una transazione sia legittima, per evitare il double-spending (che un utente usi due volte gli stessi fondi).

- Creare nuova moneta digitale, remunerando in miners che hanno svolto il compito precedente.

Quando si esegue una transazione vengono compiuti diversi passaggi:

- Le transazioni vengono raggruppate assieme in un blocco

- I miners verificano che le transazioni all'interno del blocco siano legittime risolvendo un puzzle matematico chiamato problema del Proof of Work

- Una ricompensa in forma di moneta digitale viene assegnata al primo miner che risolve il problema

- Le transazioni verificate sotto forma di blocco vengono quindi salvate nella catena (il blocco viene collegato all'ultimo blocco della catena).

Questo problema matematico ha come elemento chiave l'asimmetria. Il lavoro infatti deve essere complicato per il miner ma facile da testare per il network. Questa idea è anche nota come CPU cost function o CPU pricing function.

Tutti i miners della rete competono per essere i primi a trovare una soluzione per il problema, un problema che non può essere risolto in altri modi che utilizzando brute force ovvero la risoluzione del problema richiede un elevatissimo numero di tentativi. Quando un miner risolve il problema lo comunica all'intero network e successivamente riceverà un reward dal protocollo.

Da un punto di vista tecnico il mining è un'operazione di hash inversa, il miner deve trovare un numero (nonce) in modo che la l'algoritmo crittografico hash su un blocco di dati, ritorni un valore inferiore ad una determinata soglia. Questa soglia viene chiamata difficulty ed è ciò che determina la natura competitiva del mining. Maggiore è la potenza computazionale presente sul network e maggiore sarà la difficulty, aumentando anche il numero medio di tentativi che bisogna intraprendere per creare un nuovo blocco. Questo metodo aumenta anche il costo della creazione di un blocco, spingendo i miner a migliorare la propria efficienza del sistema di mining per avere un bilancio economico positivo. L'aggiornamento di questo parametro avviene all'incirca ogni 14 giorni, e un nuovo blocco viene generato ogni 10 minuti.

Proof of Work non è solamente utilizzato da Bitcoin ma anche da Ethereum e molte altre blockchain. Non tutte le funzioni dei sistemi PoW sono uguale in quanto sono state create specificatamente per diverse blockchain, ma in linea generale il funzionamento è lo stesso.

3.4 Proof of Stake

L'alternativa più comune al PoW è il Proof of Stake. In questo tipo di algoritmo di consenso, al posto di investire in computer costosi per gareggiare per minare blocchi, i "validator" investono in monete del sistema. Si usa il termine validato al posto di miner perchè nella Proof of Stake non vi è la creazione di nuova moneta. [2]

Proof of Stake è un metodo differente di validare le transazioni ed ottenere il consenso distribuito. È sempre un algoritmo, e lo scopo è lo stesso del PoW, ovvero ottenere il consenso distribuito, ma il processo per ottenere questo obiettivo è abbastanza diverso.

La prima idea di Proof of Stake fu suggerita sul forum bitcointalk nel 2011, ma la prima criptovaluta ad usare questo metodo fu Peercoin nel 2012, insieme successivamente a ShadowCash, Nxt, BlackCoin, NuShares/NuBits, Qora and Nav Coin. Al contratio di PoW, dove l'algoritmo remunera il miner che ha risolto il problema matematico con lo scopo di validare transazione e creare un nuovo blocco, nella PoS il creatore di un nuovo blocco viene scelto in maniera deterministica dipendentemente alla sua ricchezza, denominata stake.

Come dicevamo prima, nella PoS non vi è creazione di moneta, in quanto tutto il capitale viene creato inizialmente e questo numero non cambierà mai, quindi non vi è un processo di mining, per questo motivo vi sono i validator, che non ricevono un reward per la validazione di un blocco ma parte delle commissioni della transazione. In PoS la possibilità di essere scelto come validator per creare il nuovo blocco dipende dalla frazione di moneta che si possiede rispetto a quella dell'intero sistema. Un valodator con 200 coin sarà due volte più probabile che venga scelto rispetto ad un validator con 100 coin.

Una volta che un validator crea un blocco, questo blocco deve essere sottomesso alla blockchain. PoS diversi hanno diversi metodi per effettuare la sottomissione. In Tendermint per esmepio ogni nodo del sistema deve firmare un blocco finché non si è

raggiunta una maggioranza, in altri sistemi per firmare invece viene scelto un gruppo casuale di nodi. A questo punto però vi è problema, cosa scoraggia un validator dal creare due blocchi ed ottenere le commissioni transazione di entrambi i blocchi, e allo stesso modo cosa scoraggia un nodo che deve firmare dal firmare entrambi i blocchi ? Questo problema si chiama "nothing at stake" ovvero niente da perdere e quindi nessuna ragione per non comportarsi correttamente.

Gli ingenieri blockchain stanno cercando un modo per risolvere questo problema e la prima risposta è quella di far bloccare i fondi ad un validator all'interno di una cassaforte virtuale al momento della validazione. Nel caso un validator provasse di firmare due volte o provasse a creare una fork (ovvero due blocchi) le sue monete verrebbero eliminate.

Nei sistemi di consenso distribuiti dove viene utilizzata la PoW i miners hanno bisogno di tantissima energia. Secondo dati del 2015, una transazione bitcoin richiedeva la stessa quantità di corrente elettrica di 1,57 case americane per un giorno. Inoltre questi costi dell'energia vengono pagati con moneta a corso forzoso, portando ad una costante pressione al ribasso sulla moneta digitale. In una ricerca recente, gli esperti affermano che nel 2020 il consumo di energia elettrica delle transazioni bitcoin sarà paragonabile al consumo di elettricità dell'intera Danimarca. I developer sono preoccupati da questo problema e la PoS è un ottima alternativa per una forma di consenso più economica ed ecologica.

Capitolo 4

Voting system su blockchain

Lo scopo di questo progetto è stato quello di implementare una votazione tramite blockchain, ovvero di testare una nuova tecnologia al posto di quella tradizionale, cercando di migliorarla utilizzando i benefici che questa nuova tecnologia ci mette a disposizione. L'aspetto principale di cui mi sono occupato non riguarda tanto la piattaforma in se che ha bisogno di essere migliorata per essere utilizzata in un ambiente reale, ma di verificare la possibilità e l'usufruibilità di cosa le blockchain possano offrirci, in questo caso utilizzarle come backbone per una votazione. In questo progetto verrà utilizzata una macchina che funzionerà come server e creerà la blokchain. Una volta creata la blockchain, questa verrà resa pubblica e accessibile a tutti coloro che desiderano partecipare alla votazione. Quest'ultima sarà completamente trasparente e tutti coloro che lo desiderino potranno vederne le transazioni all'interno senza pregiudicare l'anonimato dei votanti. Per migliorare l'interazione con la blockchain è stata sviluppata una piccola piattaforma che garantisca alcuni principi di base delle votazioni, come l'univocità del voto e il fatto che una persona possa votare una sola volta; e faciliti anche il lavoro che l'utente medio dovrà compiere per effettuare una votazione. L'utente quindi dovrà prima collegarsi alla blockchain, che come ho preannunciato sarà pubblica, effettuare il login utilizzando le proprie credenziali, ottenere il proprio token di voto e successivamente consultando la pagina dei candidati con i rispettivi indirizzi di voto, esprimere il proprio voto tramite l'ambiente blockchain sul proprio terminale.

4.1 Vantaggi

Conosciamo tutti i problemi delle votazioni tradizionali, ovvero che il sistema di ballottaggio può essere manipolato da potenti ed organizzazioni criminali per far si che la votazione prenda la piega desiderata. Il sistema di spoglio dei voti è ancora

troppo macchinoso, richiede molta mano d'opera e non sempre può venire considerato affidabile, senza tener conto dell'esorbitante costo delle elezioni, nel 2013 il costo complessivo sostenuto dal Ministero dell'interno si aggirava intorno ai 315 milioni di euro.[3] L'utilizzo di una blockchain potrebbe risolvere gran parte di questi problemi, a partire dal fattore legato alla sicurezza. Il sistema di votazione corrente garantisce anonimato ai votanti, ma il processo di spoglio non è trasparente. Le persone devono fidarsi dei risultati affidati alle commissioni elettorali. Blockchain permetterebbe di tracciare i voti, quindi garantendone la totale trasparenza, ma proteggendo la privacy grazie al fatto che le transazioni sulla rete restano anonime. Sarebbe impossibile per un utente votare più di una volta perchè sulla catena si ha un record permanente del voto collegato all'id che viene salvato sotto forma di transazione, una volta che una transazione è stata inserita all'interno di un blocco e questo blocco dopo essere stato verificato viene aggiunto alla catena quest'ultima non può più essere modificata, quindi impedirebbe la cancellazione di voti. Il tutto sarebbe completamente trasparente, perché la blockchain in questione sarebbe pubblica e può essere consultata in qualsiasi momento da qualsiasi utente. I risultati o l'andamento delle elezioni sono immediatamente disponibili, rendendo il processo di votazione non solo più veloce ma largamente più efficiente del vecchio sistema tradizionale. L'errore umano sarebbe eliminato dallo spoglio dei voti e si otterrebbe il risultato di un'elezione già pochi istanti dopo la chiusura delle urne. La blockchain in generale, essendo decentralizzata, garantisce maggiore democraticità, e in un contesto come una votazione, potrebbe essere la chiave di volta per risolvere i numerosi conflitti che avvengono con l'interferenza di governi, come succede in alcuni paesi, nelle elezioni.

4.2 Implementazione

4.2.1 Multichain e Multichain-explorer

Per questo progetto ho utilizzato Multichain, che è una piattaforma libera che permette di creare blockchain private che possono essere utilizzate da organizzazioni o privati per operazioni finanziarie e ogni genere di utilizzo cui può essere utilizzata una blockchain. La piattaforma mette a disposizione API che a linea di comando permetto di eseguire numerose operazioni, dalla creazione della blockchain, all'esecuzione di transazioni, al settaggio dei parametri ecc. Questa piattaforma è stata quindi utilizzata per la realizzazione, lo sviluppo e il testing del progetto. Durante la realizzazione del progetto ho anche testato ed utilizzato Multichain-explorer, che

è un web-based explorer per blockchain costruite con Multichain. Ho trovato questo strumento particolarmente utile perché consente di prendere visione in modo facile e intuitivo di come sia composta la blockchain, e di ottenere tutte le informazioni necessarie riguardanti la blockchain. Molto utile inoltre anche per andare a scomporre i blocchi e vedere le transazioni all'interno degli stessi.

4.2.2 Creazione della blockchain

Il primo passo fondamentale del progetto è stato quello di creare tramite la piattaforma Multichain la mia blockchain su cui sarò poi andato a costruire la votazione. Ho dovuto impostare i parametri necessari per consentire a qualsiasi user di potersi connettere, in modo da rendere pubblica la votazione, e successivamente i permessi per consentire agli users di poter inviare assets, cosa che poi sarebbe stata indispensabile per portare a termine le transazioni. Una volta creata la blockchain, Multichain mi fornisce un indirizzo ip ed un numero di porta per consentire a qualsiasi utente di potersi connettere alla catena. A questo punto ho richiesto un address, collegato alla macchina (che d'ora in avanti chiamerò poll server) in modo da poterla identificare e tramite questo indirizzo ho istanziato sulla macchina un numero finito di asset, indivisibili. Questi asset che chiamerò token, sono una vera e propria valuta e saranno utilizzati durante la votazione come voti virtuali, un token corrisponderà ad un voto. Durante la votazione, tramite la piattaforma che più avanti illustrerò, i voter, potranno richiedere un token al poll server, e successivamente inviarlo al candidato di loro scelta. In questo modo si potrà avere traccia della transazione tramite la catena, e il voto espresso non potrà più essere modificato. A questo punto ho dovuto creare i rispetti indirizzi per i candidati. Ho ipotizzato di avere per semplicità solamente due candidati, ma il numero di indirizzi possibili e di conseguenza il numero di candidati è teoricamente infinito. Questi due indirizzi avranno il permesso in ricezione, significa che qualsiasi users potrà inviare a loro token. Gli users tramite la piattaforma che ho realizzato potranno prendere visione degli indirizzi dei vari candidati e tramite multichain potranno inviare loro il proprio token o voto. In qualsiasi momento sarà possibile vedere quanti voti sono stati assegnati a quale indirizzo. Per quanto riguarda i votanti, o voter, la loro procedura è molto semplice, devono aver installato sulla propria macchina Multichain, e tramite un comando insieme ad indirizzo ip ed un numero di porta, che verrà reso noto, potranno collegarsi alla blockchain. Una volta connessi alla catena, utilizzeranno la mia piattaforma per ottenere il token e successivamente esprimeranno il proprio parere tramite una primitiva di multichain.

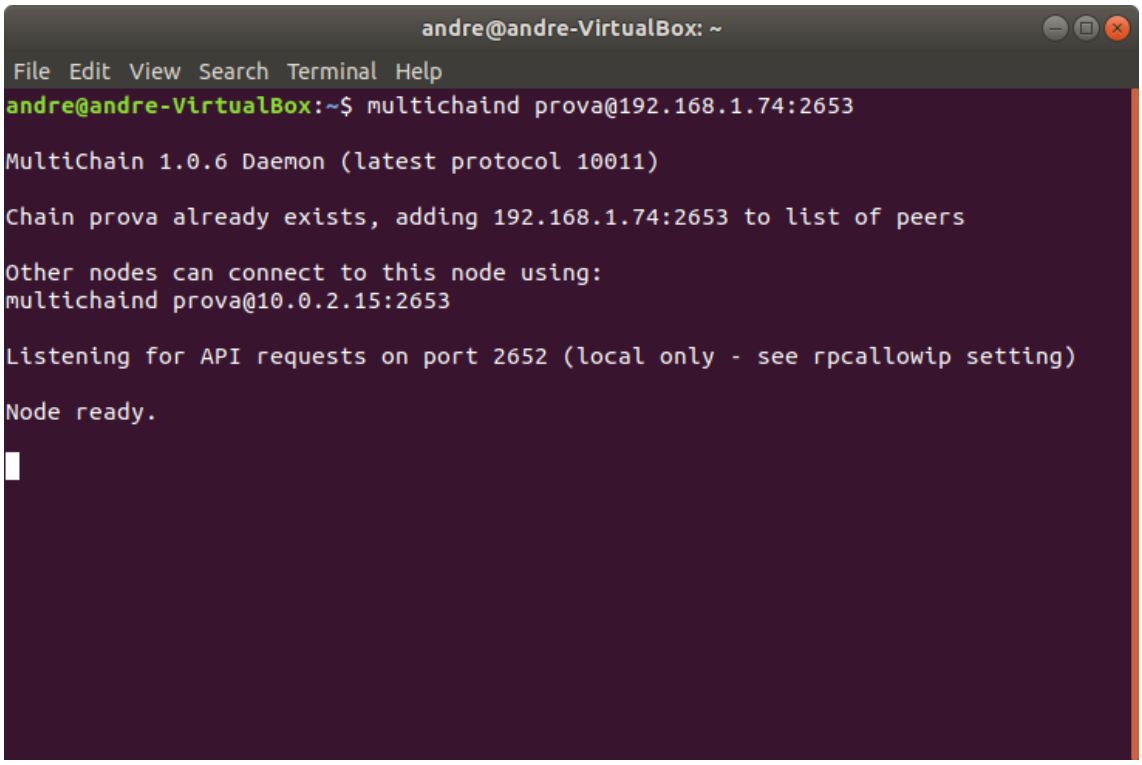

Figura 4.1: Collegamento alla blockchain

4.3 La piattaforma

La piattaforma che ho creato non è ancora adatta ad essere utilizzata per una votazione a livello nazionale, è un semplice strumento utilizzato per garantire i controlli di base necessari per una corretta votazione. La piattaforma è stata implementata utilizzando vari linguaggi, tra cui JavaScript, PHP, JSON e si occupa principalemte di distribuire token e di verificare che un utente non richieda più token di quanti gliene siano dovuti. Per connettersi alla piattaforma l'utente dovrà inserire l'indirizzo ip contenuto nel comando per connettersi alla blockchain seguito dal nome della pagina web a cui vorrà collegarsi. Sono state create due pagine statiche che consentono all'utente di ottenere informazioni riguardanti la blockchain e i candidati. Abbiamo la pagina info.php dove vengono visualizzate tutte le informazioni riguardanti la blockchain, come il nome, la descrizione, il protocollo, la porta utilizzata, il numero dei blocchi ecc, e la pagina candidates.html che mostra gli indirizzi a cui gli utenti possono inviare token per esprimere il proprio voto a favore di un candidato.

4.3.1 Login

Uno dei maggiori problemi nell'ambito delle votazioni, che viene riscontrato anche tramite blockchain consiste nel riconoscimento del votante. Nel Marzo 2018 in West

Virginia è stata consentita la possibilità ai militari in territori stranieri di votare tramite un'applicazione collegata ad una blockchain. Per identificare i votanti hanno utilizzato una combinazione di riconoscimento facciale, impronta digitale e documenti. Il che però non riesce ancora a convincere il pensiero dei più ostici. Io come avevo preannunciato non ho cercato di raggiungere questo livello di autenticazione, mi sono servito di una pagina di login, dove viene verificato username e password tramite php. I controlli vengono effettuati temporalmente, e una persona non si può connettere due volte entro un determinato periodo di tempo, che potrebbe essere stabilito a tempo debito in base alle necessità dell'elezione. Questo impedisce che un votante richieda più indirizzi per poi avere più di un voto, spiegherò meglio più avanti il funzionamento degli indirizzi e dei token.

4.3.2 Vote

Dopo aver effettuato l'accesso tramite la pagina di login, l'utente verrà automaticamente reindirizzato alla pagina vote che permetterà all'untente di richiedere il proprio token. All'interno della blockchain sono stati inseriti durante la fase di configurazione un determinato numero di asset. Questi asset come avevo preannunciato sono una specie di moneta virtuale, e possono essere scambiati tra indirizzi come transazioni. Tutte le transazioni vengono registrate e sono salvate permanentemente all'interno della catena. Per votare l'utente dovrà semplicemente richiedere un indirizzo a Multichain dal proprio terminale, questo indirizzo varierà di volta in volta e cambia a seconda dell'utente, verrà utilizzato anche in seguito per impedire che un utente richieda più di un token. Questo indirizzo dovrà essere inserito nel campo apposito nella pagina vote, e cliccando il pulsante "Get Token" si verrà reindirizzati nella pagina più importante che eseguirà altri controlli e lo script.

4.3.3 Pay

La pagina Pay o pagina di pagamento è forse la pagina più importante di tutta la piattaforma e si occupa di varie funzioni. Per prima cosa al momento dell'invio dell'indirizzo verrà eseguito uno script che controllerà la presenza o meno dell'address all'interno di un fil Json. Questo controllo precluderà l'utente dal ricevere un token, se l'indirizzo verrà riscontrato all'interno del file. Serve ad evitare anche in questo caso che un utente possa utilizzare lo stesso indirizzo più di una volta per poter ottenere più di un token. Nel caso l'address sia già presente all'interno del file, il processo di richiesta del token verrà fermato e l'utente visualizzerà la scritta "Address already used". In caso contrario invece, l'utente visualizzerà una pagina

che lo informa che il processo di invio del token è andato a buon fine e a breve sarà in grado di vedere aumentare il suo conto. Per lo script di invio token, progettato in php, vengono utilizzate le primitive fornite da Multichain, e si divide in due parti. Nella prima parte viene concesso il permesso all'address inserito all'interno della schermata precedente (la pagina Vote) di riceve e inviare assets. La seconda parte dello script si occupa invece si eseguire il trasferimento dell'asset dall'indirizzo originario sul quale erano stati creati gli asset, all'indirizzo del voter. A questo punto come avevo preannunciato precedentemente il votante in totale autonomia, tramite Multichain, potrà andare a controllare il proprio saldo che nel giro di pochi istanti dovrebbe essere aumentato. Non è un trasferimento istantaneo proprio perché stiamo utilizzando una blockchain e la transazione deve essere inserita all'interno di un blocco e lo stesso deve essere prima approvato. In ogni istante, un utente che lo desideri può consultare il numero di token associati al proprio indirizzo i quali non possono essere maggiori di 1 e minori di 0.

Questo è lo script in php che si occupa di verificare che l'address non sia già stato utilizzato. Ogni volta che un address viene utilizzato viene salvato all'interno di un file json, accessibile da tutti i nodi della rete. Se l'indirizzo viene trovato all'interno del file, l'utente sarà bloccato e non potrà procedere con la richiesta di token. Nel caso invece l'indirizzo non fosse già stato utilizzato precedentemente l'utente può continuare la procedura di richiesta token, e l'address verrà salvato all'interno del file per poter evitare operazioni fraudolente.

```
1  try
2    {
3          $jsondata = file_get_contents($myFile);
4          $arr_data2 = json_decode($jsondata, true);
5          if (strpos($arr_data2, $address) !== false) {
6                  echo "<body bgcolor='#cccccc'>";
7                  echo "<h1>";
8                  echo "<font color = 'red'>";
9                  echo "<center>";
10                 echo "<br><br><br>";
11                 echo "ADDRESS ALREADY USED";
12         }
13         else {
14         $arr_data2 .= $_POST['address'];
15         $jsondata = json_encode($arr_data2, JSON_PRETTY_PRINT);
```

Questa parte del codice sottostante, è forse il cuore della piattaforma e serve per comunicare con multichain e far accreditare un token al votante con un address legittimo. Come prima cosa viene salvato l'address con il metodo POST, che servirà per sapere a chi accreditare il token. Dopodichè viene garantito il permesso a questo address di ricevere e mandare token, in modo da poterlo abilitare alla votazione. Infine viene spedito, dall'indirizzo iniziale della blockchain dove risiedono gli asset, un token all'indirizzo cui avevamo abilitato precedentemente l'invio e la ricezione di token, ovvero l'indirizzo che il votante aveva precedentemente inserito nella piattaforma online.

```
1  $addr = $_POST["address"];
2
3  $a = 'curl -s --user multichainrpc:
4  3n18XKBt4j1bQfr1unmR2qS8gXHovsv4YqfDCKJCZGUu --data-binary \'';
5  $b = '{"jsonrpc": "1.0", "id":"curltest", "method": "grant",
6  "params": ["';
7  $c = '", "receive,send"';
8  $d = '] }\' -H "content-type: text/plain;" http://127.0.0.1:2652/';
9  $cmd = $a . $b . $addr . $c . $d;
10 $ret=system($cmd);
11
12 $a = 'curl -s --user multichainrpc:
13 3n18XKBt4j1bQfr1unmR2qS8gXHovsv4YqfDCKJCZGUu --data-binary \'';
14 $b = '{"jsonrpc": "1.0", "id":"curltest", "method":
15 "sendassetfrom", "params": ["1Vk8K11nFZb9cbA6LUZGkKyiitJv7ahye95AVq","';
16 $c = '", "token", 1';
17 $d = '] }\' -H "content-type: text/plain;"
18 http://127.0.0.1:2652/';
19 $cmd = $a . $b . $addr . $c . $d;
20 $ret=system($cmd);
```

4.3.4 Asset

Ogni votante che voglia poter votare deve richiedere un asset alla blockchain tramite la piattaforma e successivamente inviarlo ad uno dei candidati. Il sistema di occupare del fatto che un votante possa richiedere al massimo un asset con due controlli, il primo viene effettuato al momento del login sulla pattaforma, che sarà ad accesso limitato a seconda del numero di votazioni possibili e il secondo avviene al momento della richiesta del token, dove non verrà rilasciato più di un token per lo stesso indirizzo.

Con lo screenshot sottostante vorrei mostrate tre processi fondamentali del sistema di voto.

Con il primo comando l'utente ottiene un nuovo address che inserirà all'interno della piattaforma e gli permetterà di ricevere un token.

Con il secondo comando interroga multichain sul suo balance, ovvero sul proprio saldo. Una volta che l'address inserito è stato verificato, viene creata la transazione di invio token, una volta che questa transazione è stata inserita all'interno di un blocco, e questo blocco verificato ed aggiunto alla catena, l'utente vedrà il proprio saldo aumentare ad uno.

Il terzo comando rappresenta la votazione vera e propria, ovvero l'utente invia il proprio token all'indirizzo di uno dei due candidati, che si trova nella pagina web dedicata. Il codice in basso rappresenta l'id della transazione e significa anche che la transazione è andata a buon fine.

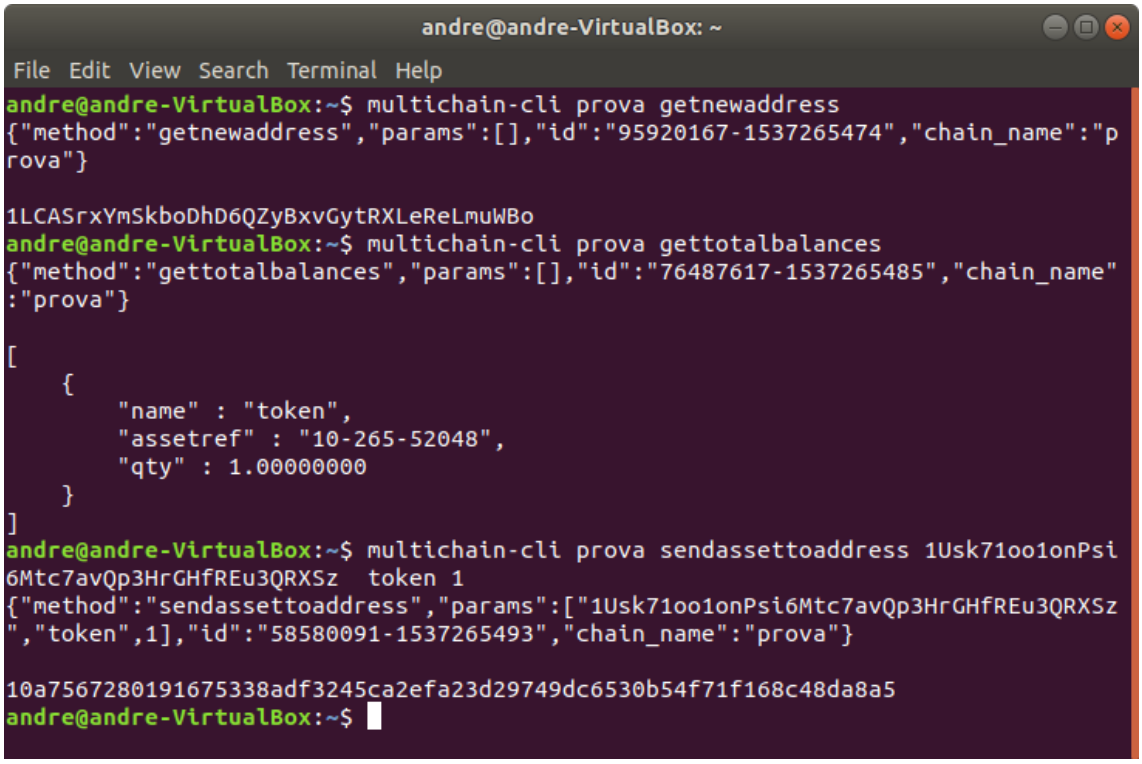

Figura 4.2: I 3 comandi sopra citati

4.3.5 Spoglio dei voti

Uno dei maggiori punti a favore della votazione tramite blockchain risiede nello spoglio dei voti. Oltre ad eliminare l'errore umano commesso durante il conteggio, non bisognerebbe più aspettare ore dopo la fine della votazione per avere un risultato ma tramite un semplice comando si potrebbe ottenere istantaneamente l'andamento della votazione, nel caso non sia ancora finita, o il risultato finale. L'andamento della votazione può essere controllato in ogni momento utilizzando vari strumenti. Nel caso della mia piattaforma, se siamo connessi tramite il terminale che ha creato la votazione, abbiamo diversi metodi. Per prima cosa si possono usare le primitive di Multichain, che ci consentono non solo di vedere quanti token sono stati assegnati a quali candidati, ma anche di tenere sotto controllo i nostri asset e vedere quanti token sono in mano ai voter in attesa di essere utilizzati. Ho inoltre realizzato un piccolo scipt Python che mi consente di tenere sotto controllo velocemente l'andamento della votazione restituendomi i punteggi di ogni candidato. E' possibile inoltre controllare l'andamento della votazione tramite un altra interfaccia, Multichain-explorer. Questo web-based explorer per Multichain consente di visualizzare la catena in maniera grafica ed ottenere informazioni dettagliate sulle transazioni e sui voti di ogni candidato. Dal punto di vista dei voter, abbiamo sempre a disposizione le primitive di multichain, e inoltre essendo la votazione tramite blockchain, non vi è nulla di nascosto, tutti i dati sono a disposizione di tutti e gli utenti sono liberi di interrogare la blockchain sulle varie transazioni all'interno di ogni blocco, in modo da controllare che il proprio voto sia andato a buon fine e tenere sotto controllo l'andamento della votazione, senza ovviamente compromettere l'anonimato dei votanti.

Qui vi presento le funzioni più interessanti dello script da me realizzato in python per effettuare lo spoglio dei voti che interroga multichain sui voti ottenuti dai candidati, e restituisce il valore dentro headQuery. A questo punto trova la stringa corrispondente al candidato con il numero di voti ottenuti che verrà passata alla funzione valore. Valore a questo punto restituirà il numero esatto di voti che andrà confrontato poi all'interno del main. A seconda di quale dei due candidati abbia un voto maggiore, questo script restituisce l'id del candidato vincente, o in caso di parità comunica il pareggio.

```
1 import os
2 import subprocess
3 import json
```

```
4
5  def main():
6      headQuery = subprocess.run(['multichain-cli', 'prova',
7      'getaddressbalances',
8      '1KBT2wdkFQwkk9o5Be4V2CWszDQfPxxrxL7kc9'], stdout =
9      subprocess.PIPE)
10     headQuery2 = subprocess.run(['multichain-cli', 'prova',
11     'getaddressbalances',
12     '1Usk71oo1onPsi6Mtc7avQp3HrGHfREu3QRXSz'], stdout =
13     subprocess.PIPE)
```

```
1  def valore(bytes):
2      prova = bytes
3      ritorno1 = find_str(str(prova), "qty")
4      ritorno1 = ritorno1 - 1
5      prova2 = prova[ritorno1:]
6      prova3 = str(prova2).split();
7      x = prova3.pop()
8      singleitem = prova3.pop()
9      val1 = float(singleitem[:-2])
10     return val1
11
12
13 def find_str(s, char):
14     index = 0
15
16     if char in s:
17         c = char[0]
18         for ch in s:
19             if ch == c:
20                 if s[index:index+len(char)] == char:
21                     return index
22
23             index += 1
24
25     return -1
```

Le due stringhe che trovate all'inizio all'interno del main, sono gli id dei candidati cui i votanti hanno inviato il proprio voto.

4.4 Proprietà

La votazione tramite blockchain rispetta la maggior parte delle proprietà, garantendo sicurezza affidabilità ed anonimato al votante. Vi sono però alcuni problemi

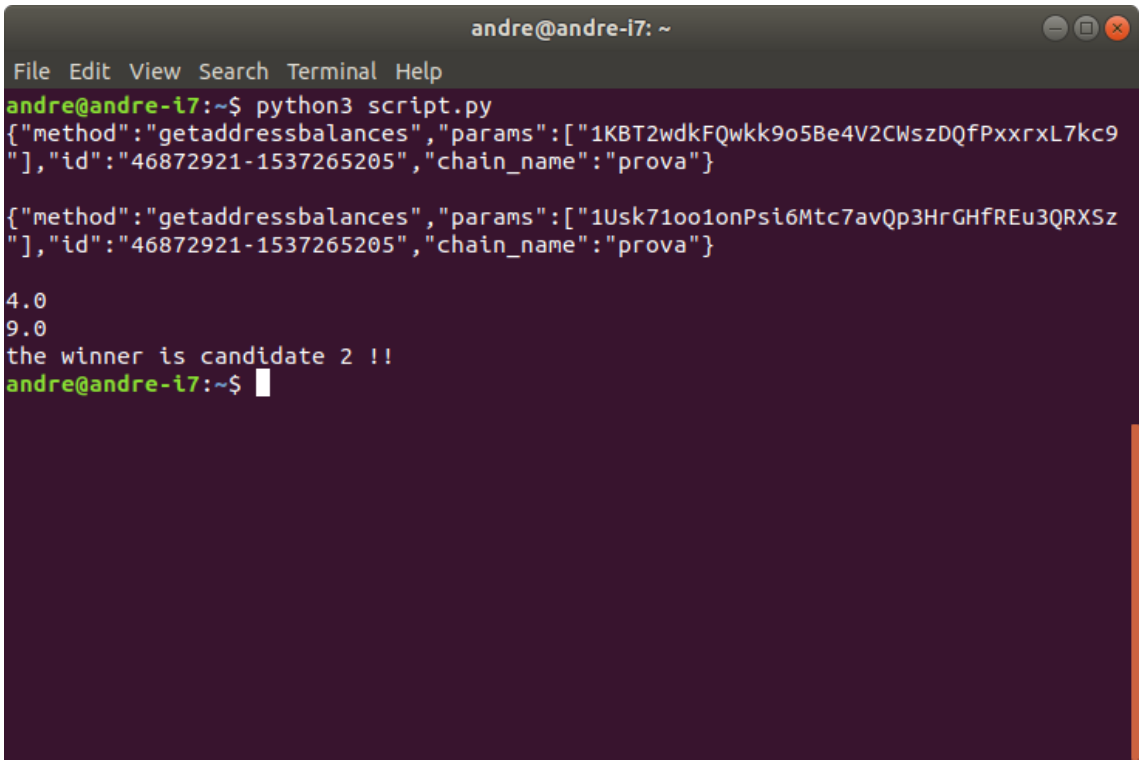

Figura 4.3: Risultato dello script in python

riguardanti uno degli aspetti fondamentali su cui blockchain si basa.

4.4.1 Equità

Questa proprietà non viene rispettata in ambito blockchain, stiamo parlando della proprietà che impedisce risultati parziali dell'elezione prima che essa sia terminata, in modo da non influenzare i votanti. Essendo la blockchain pubblica, ogni individuo può verificare i voti che ciascun candidato o partito ha ottenuto, quindi per esempio, un partito che nella fase iniziale dell'elezione ha ottenuto pochissimi voti potrebbe risultare svantaggiato da questo aspetto in quanto risulterebbe magari più difficile per un votante votare per un partito cui non crede possa vincere l'elezione.

4.4.2 Libertà dalla coercizione

Il secondo problema risulta un problema comunque a tutti i sistemi di voto, sia elettronici che non, sia centralizzati che come in questo caso decentralizzati, ovvero la coercizione e la compravendita di voti. Tramite blockchain io posso avere una ricevuta di quello che ho votato, e questo mi serve per poter controllare di aver votato correttamente, ovvero viene soddisfatta la proprietà della verificabilità. Tramite questa ricevuta però posso vendere il mio voto, non solo, anche rendendo pubblico il mio indirizzo privato, potrei dimostrare il mio voto. La coercizione invece direi che

risulta molto più complicata in quanto non vi è modo di collegare la persona fisica all'indirizzo, in quanto l'anonimato viene garantito da crittografia asimmetrica. Una persona però se costretta rivelerebbe il proprio indirizzo e quindi sarebbe possibile manipolare il voto delle persone, ma questo è un problema comunque a qualsiasi sistema di voto. In altre parole possiamo dire che principalmente l'unico problema risiederebbe nella troppa semplicità con cui si potrebbe vendere il voto. Non esiste sistema al mondo che non sia vulnerabile alla compravendita di voti, ma alcuni sistemi lo rendono un po' più complesso.

4.4.3 Soluzione

Una possibile soluzione parziale alla compravendita di voti sarebbe dare la possibilità di poter votare più volte, come avevamo visto precedentemente il altri sistemi. Questo non eliminerebbe il problema alla base, ma renderebbe la compravendita sicuramente più complicata. L'idea di base sarebbe quella di tenere in considerazione solamente l'ultimo voto in linea temporale in modo da poter dare la possibilità ad un utente di cambiare voto fino all'ultimo istante, rendendo la compravendita più macchinosa e insicura.

Capitolo 5

Conclusione

Blockchain potrebbe essere un buon approccio per garantire un voto elettronico sicuro. Sono stati riportati buoni risultati, ma vengono riscontrati gli stessi problemi che si hanno i migliori sistemi di voto elettronici centralizzati. Il maggior problema come preannunciato risiede nel fatto che essendo la blockchain pubblica, un utente potrebbe rendere pubblico il proprio indirizzo privato, risultando in un sistema non libero da coercizione, pertanto questo sistema risulta vulnerabile alla compravendita di voti e all'estorsione.

Sono soddisfatto dei risultati ottenuti in quanto questa idea potrebbe senza dubbio competere con i più moderni sistemi di e-voting attualmente sul mercato. Ricordo che i problemi riscontrati su blockchain sono i comuni problemi riscontrati anche sui sistemi più moderni e se volessimo confrontare la votazione tramite blockchain con l'e-voting system Estone, attualmente a mio parere il più evoluto ed il più sofisticato, non ci sarebbe un grosso divario.

Ringraziamenti

Vorrei ringraziare il Professor. Laneve per avermi dato la possibilità di esplorare l'ambiente blockchain e mettere a punto un sistema di voto elettronico decentralizzato che funzioni tramite questa nuova tecnologia.

Non sempre è stato facile, soprattutto all'inizio, essendo relativamente una nuova tecnologia non era presente molto materiale su cui poter studiare, ma il Professor. Laneve e la sua collaboratrice Adele Veschetti sono sempre stati disponibili per chiarimenti e delucidazioni.

Un ringraziamento particolare va ad Adele Veschetti che mi è sempre stata vicino durante il percorso di tesi e mi ha aiutato nella ricerca e nella sperimentazione della tesi di laurea.

Bibliografia

[1] Thomas Bronack. "The problems with a paper based voting system". In: *White Paper* (2010).

[2] Amy Castor. *A (Short) Guide to Blockchain Consensus Protocols*. March 4th 2017. URL: https://www.coindesk.com/short-guide-blockchain-consensus-protocols/.

[3] Alessandro Cipolla. *Costi elettorali italiani*. May 28 2018. URL: https://www.money.it/elezioni-anticipate-quanto-costa-voto.

[4] Estonian National Electoral Committee. *Statistics - Inter- net Voting - Voting methods in Estonia.* April 2015. URL: http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics/.

[5] Maaten Epp. "Towards remote e-voting : Estonian case". In: *Proceedings of the 1st Conference on Electronic Voting* (2004).

[6] Block Geeks. *Basic Primer: Blockchain Consensus Protocol*. 2018. URL: https://blockgeeks.com/guides/blockchain-consensus/.

[7] Block Geeks. *Proof of Work vs Proof of Stake: Basic Mining Guide*. 2017. URL: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.

[8] Douglas W. Jones. "Problems with Voting Systems and the Applicable Standards". In: *Testimony before the U.S. House of Representatives' Committee on Science* (Washington D.C. May 22 2001).

[9] Arjun Kharpal. *Everything you need to know about the blockchain*. 18 June 2018. URL: https://www.cnbc.com/2018/06/18/blockchain-what-is-it-and-how-does-it-work.html.

[10] Delaune Stéphanie; Kremer Steve; Ryan Mark. "Verifying privacy-type properties of electronic voting protocols: A taster". In: *Towards Trustworthy Elections* (Springeri 2010).

[11] Christian Meter. "Design of Distributed Voting Systems". In: (24th September 2015).

[12] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”. In: (mar. 2009).

[13] Erica Naone. *Voting with (Little) Confidence*. January 29 2008. URL: `https://www.technologyreview.com/s/409453/voting-with-little-confidence/`.

[14] Halderman J A.; Teague Vanessa. “The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election”. In: *arXiv preprint arXiv:1504.05646* (March 2015 pp. 1–18).