BAB II

TINJAUAN PUSTAKA

2.1. *Blockchain*

Blockchain adalah penemuan teknologi penyimpanan data oleh seorang atau grup yang bernama Satoshi Nakamoto. Sejak saat itu, *blockchain* telah berubah menjadi suatu yang lebih hebat. Dengan mengizinkan informasi untuk didistribusikan tapi tidak disalin, teknologi *blockchain* telah membuat pondasi untuk sebuah internet yang baru. Awalnya digunakan untuk mata uang digital atau *cryptocurrency* untuk Bitcoin, sekarang komunitas teknologi telah menemukan banyak potensi kegunaan teknologi tersebut. [1]

Informasi yang ada di dalam *blockchain* ada sebagai sesuatu yang disebarkan. Ini adalah kegunaan jaringan yang memiliki kegunaan yang sangat jelas. Database dari *blockchain* tidak disimpan dalam satu lokasi, yang berarti catatan informasinya yang disimpan sebagai informasi publik yang dapat diperiksa dengan mudah. Tidak ada penyimpanan yang terpusat untuk seorang hacker untuk merusak datanya. Datanya disebarkan oleh jutaan komputer pada saat yang bersamaan, sehingga datanya dapat diakses oleh semua orang yang terkoneksi dalam internet. [1]

Blockchain bisa juga disebut sebagai *public ledger* dari seluruh transaksi yang sama. *Blockchain* menyimpan transaksi tersebut dalam sebuah block. Block pertama dalam *blockchain* dinamakan "Genesis Block" atau "Block 0". Block pertama tersebut biasanya telah ditentukan

dikarenakan block tersebut tidak menunjuk pada *hash* milik block sebelumnya. [2]

Dikarenakan sistem *blockchain* yang bersifat terbuka, maka jaringan *blockchain* hidup dalam konsensus untuk mengurangi adanya kekurangan faktor akan kepercayaan, karena setiap pengguna yang terkoneksi dalam jaringan *blockchain* dapat menambahkan data ke dalam *blockchain*. Konsensus sangatlah dibutuhkan untuk memastikan pengguna yang lain setuju bahwa data tersebut adalah data yang sah sebelum data tersebut dimasukkan secara permanen ke dalam *blockchain.* Dikarenakan tidak ada yang bisa menjamin kepercayaan dari pengguna yang bersangkutan, maka konsensus adalah bagian yang vital di dalam *blockchain.* Untuk merusak data dari *blockchain* tersebut berarti membutuhkan kekuatan komputer yang sangat kuat yang dapat menguasai mayoritas dari jaringan *blockchain* yang ada. Berikut merupakan algoritma yang biasa digunakan untuk mencapai konsensus dalam *blockchain*: *practical byzantine fault tolerance algorithm (PBFT), the proof-of-work algorithm (PoW), the proof-of-stake algorithm (PoS), and the delegated proof-of-stake algorithm (DPoS).* [3]

Berikut merupakan komponen-komponen yang digunakan di dalam sistem *blockchain*:

2.1.1. Hash

Hash merupakan metode yang digunakan untuk mengubah data menjadi nilai hexadesimal yang memiliki panjang tertentu yang nilainya tetap (apapun nilainya jika di *hash* memiliki panjang yang

sama dengan hasil *hash* lainnya). *Hash* dikenal dengan istilah *One Way Encryption*, dimana *hash* hanya berlaku satu arah dan tidak bisa dibalikkan [6]. *Hash* memiliki *collision* yang memungkinkan beberapa nilai awal yang berbeda memiliki *hash* yang sama, hal tersebut merupakan kondisi yang tidak diinginkan, sehingga banyak algoritma *hash* yang menyatakan bahwa mereka memiliki *low collision* (kolisi rendah). Banyak juga kegunaan *hash* dalam sekuritas, yang paling umum digunakan adalah untuk membandingkan 2 data untuk meyakinkan bahwa kedua nilai tersebut adalah sama, yang paling umum digunakan untuk menyimpan password, sehingga password yang asli tidak disimpan ke dalam *database*.

2.1.1.1 SHA-256

SHA-256 adalah singkatan dari Secure *Hash* Algorithm – 256bit yang merupakan salah satu algoritma *hash* yang biasa digunakan di dalam *blockchain*. SHA-256 merupakan *hash* yang paling kompleks dan paling aman dibandingkan *hash* lain. SHA-256 merupakan lanjutan dari SHA-1 dan merupakan variasi dari SHA-2.

Dari dahulu SSL (Secure Socket Layer) menggunakan algoritma SHA sebagai kunci dari algoritma *digital signature* miliknya. Dari 2011 sampai 2015, SHA-1 adalah algoritma yang utama untuk keamanan. Dikarenakan banyaknya penelitian yang mengacu pada kelemahan dari

SHA-1, maka adanya perombakan dalam standart keamanan yang membuat SHA-2 sebagai standart minimal untuk *digital signature*. [4]

2.1.2. Konsensus

Konsensus adalah masalah yang mendasar di sistem yang terdistribusi. Konsensus melibatkan beberapa anggota dari suatu grup untuk menyetujui sesuatu nilai. Setelah mereka sudah menyetujui nilai tersebut, maka keputusan tersebut adalah final. Algoritma konsensus yang biasa digunakan adalah keputusan mayoritas. [5]

2.1.2.1 Raft

Raft adalah algoritma konsensus untuk mengatur sebuah catatan replikasi. Hasil dari Raft setara dengan Paxos dan sama efisien dengan Paxos, namun strukturnya berbeda dengan Paxos. Hal tersebut yang membuat Raft lebih mudah dimengerti dibandingkan Paxos dan juga memberikan pondasi untuk membangun sistem yang dapat dikembangkan. Untuk meningkatkan kemudahan pengertian, Raft memisahkan elemen kunci dari konsensus, seperti pemilihan pemimpin, replikasi catatan, dan keamanan. Hal-hal tersebut dapat mengurangi beberapa keadaan yang harus dipertimbangkan. Hasil dari cerita pengguna menunjukkan bahwa Raft dapat lebih mudah dimengerti untuk dipelajari dibandingkan Paxos. Raft juga

memiliki beberapa mekanisme untuk mengganti keanggotaan dalam suatu cluster yang menggunakan mayoritas untuk menjamin keamanan. [6]

Raft bekerja dengan memilih pemimpin yang ditunjuk untuk melakukan replikasi *log* dalam suatu kelompok. Jika ada suatu konsensus yang terjadi, maka pemimpin tersebut yang menentukan apakah hasil tersebut akan dikerjakan atau tidak sesuai dengan hasil musyawarah dari seluruh anggota kelompok yang ada. Pemimpin tersebut juga akan mengirimkan *heartbeat* kepada seluruh anggota kelompok yang ada, dan jika ada anggota kelompok yang tidak menerima *heartbeat* tersebut dalam suatu kurung waktu tertentu, maka anggota tersebut akan mencalonkan diri untuk menjadi pemimpin dan menyebarkan informasi tersebut ke seluruh anggota kelompok untuk mendapatkan jawaban apakah ia akan menjadi pemimpin atau tidak. [5]

2.1.3. Asymmetric Cryptography

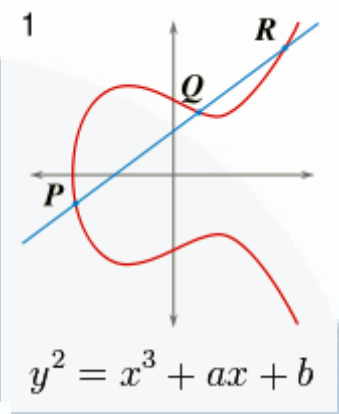
Asymmetric cryptography merupakan salah satu metode untuk melakukan enkripsi dan dekripsi data menggunakan *public key* dan juga *private key*, biasa disebut sebagai *public key cryptography* dan digunakan sebagai *digital signatures*. *Public key* dan *private key* merupakan kumpulan angka yang dipasangkan satu sama lain, namun tidak memiliki nilai yang sama. *Public key* adalah kunci yang boleh untuk disebarkan ke semua orang. Sedangkan

private key adalah kunci yang hanya boleh dimiliki dan disimpan secara rahasia oleh pemilik yang sah. Kunci tersebut dapat melakukan dekripsi dari hasil enkripsi dari kunci yang berlawanan. [7] Dengan kata lain, pesan yang di enkripsi menggunakan *private key* dapat di dekripsi menggunakan *public key* dan juga sebaliknya.

2.1.3.1 ECC

ECC (Elliptic Curve Cryptography) merupakan algoritma *asymmetric cryptography* yang mulai populer di kalangan ahli keamanan. ECC menggunakan teknik enkripsi yang berdasarkan teori kurva elips yang dapat membuat kunci yang lebih cepat, kecil, dan lebih effisien dibandingkan *asymmetric cryptography* lainnya. Untuk meretas ECC, peretas harus menghitung logaritma diskrit dari kurva eliptik yang ternyata terbukti lebih susah dipecahkan dibandingkan faktorisasi dari RSA. Hasil dari kunci ECC lebih kecil dari RSA dan menggunakan *power* yang lebih kecil, sehingga lebih cocok untuk digunakan pada aplikasi mobile dibandingkan RSA [7]. Pada penelitian ini, peneliti menggunakan algoritma ECDSA berdasarkan ECC.

Secara garis besar ECC menggunakan rumus matematika berdasarkan grafik sebagai berikut:



Gambar 2.1 Grafik kurva ECC [8]

2.2. React Native

React Native adalah *framework* milik Facebook yang dimulai dari Facebook international hackathon project pada musim panas 2013. Pertama diumumkan pada Januari 2015. Pada Maret 2015 di React.js Con, Facebook mengumumkan bahwa React Native adalah proyek open source dan tersedia di GitHub. Sejak itu React Native telah menjadi salah satu *framework* yang sangat populer. [9]

React Native memungkinkan developer untuk membuat aplikasi mobile hanya dengan menggunakan Java*Script*. React native menggunakan desain yang sama seperti React, memungkinkan developer untuk membuat user interface mobile apps dari beberapa komponen yang ada. [9]

Dengan React Native, developer tidak membangun mobile web app, HTML 5 app, atau hybrid app. Namun developer membuat mobile app sungguhan yang sama dengan aplikasi yang dirancang menggunakan Objective-C atau Java. React Native menggunakan dasar rancangan user

interface seperti aplikasi iOS dan Android pada umumnya. Developer hanya merancang komponen menggunakan Java*Script* dan React. [9]

2.3. Komunikasi

2.3.1. *Peer-to-peer*

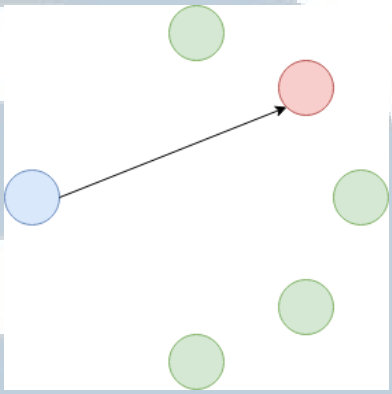
Peer-to-peer (P2P) adalah sistem komunikasi yang terdesentralisasi, dimana seluruh pengguna yang terkoneksi dapat berkomunikasi satu sama lain. *Peer-to-peer* berbeda dengan sistem *client/server* dimana *client* melakukan request dan server membalas dengan response, jaringan P2P menggunakan sistem dimana setiap pengguna dapat bekerja sebagai client dan server. [10]

Peer-to-peer saat ini belum memungkinkan untuk beberapa pengguna untuk saling berkomunikasi satu sama lain tanpa adanya pihak ke tiga seperti broker yang berguna untuk melanjutkan pesan dari pengirim ke penerima, atau dengan menggunakan tracker untuk menyimpan daftar IP dari seluruh pengguna yang terhubung.

2.3.2. Unicast

Unicast merupakan metode transmisi data yang merupakan point-to-point yang artinya dari suatu titik dan memiliki tujuan hanya satu titik yang lain. Paket pengiriman dari unicast sendiri memiliki satu identitas pengirim dan satu identitas penerima. Browsing internet pun termasuk unicast, dikarenakan pengguna meminta request dari server, hal tersebut masuk ke dalam kategori

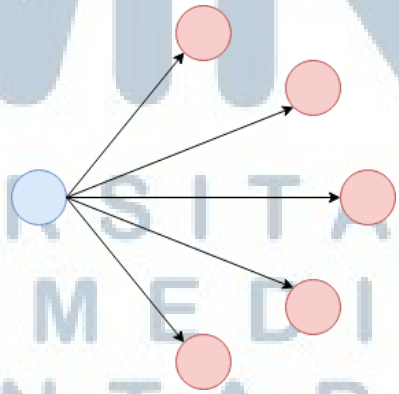
point-to-point [11]. Gambar 2.2 menunjukkan alur komunikasi dari unicast.



Gambar 2.2 Alur komunikasi unicast

2.3.3. Broadcast

Broadcast merupakan metode transmisi data yang berasal dari satu titik dan memiliki tujuan ke semua titik lain yang terhubung. Biasanya broadcast digunakan untuk *heartbeat* atau pencarian titik pada jaringan [11]. Broadcast merupakan komunikasi yang tergolong berat, dikarenakan bandwidth yang dibutuhkan adalah data_size*(N-1). Gambar 2.3 menunjukkan alur komunikasi dari broadcast.



Gambar 2.3 Alur komunikasi broadcast

2.4. Penelitian Terkait

Penelitian tentang *blockchain* belum terlalu banyak, namun ada beberapa penelitian terkait dengan penelitian ini. Penelitian tersebut telah mengkaji beberapa metode yang digunakan untuk mengintegrasikan sistem voting pada umumnya dengan sistem *blockchain*. [14]

2.4.1. A Smart Contract for Boardroom Voting with Maximum Voter Privacy

Penelitian "A Smart Contract for Boardroom Voting with Maximum Voter Privacy" dibuat oleh Patrick McCorry, Siamak F. Shahandashti, dan Feng Hao di Newcastle University. Penelitian tersebut tidak bergantung pada otoritas yang terpercaya untuk menghitung hasil voting untuk melindungi privasi pemilih, melainkan menggunakan sistem perhitungan yang otomatis. Penelitian tersebut menggunakan jaringan *blockchain* milik Ethereum dan memerlukan biaya untuk melakukan voting. [12]

Berikut merupakan fitur-fitur yang disebutkan dalam penelitian "A Smart Contract for Boardroom Voting with Maximum Voter Privacy":

2.4.1.1 Self-Tallying Voting Protocol

Self-Tallying Voting Protocol memungkinkan semua pemilih dan pihak ketiga lainnya untuk melakukan perhitungan hasil voting setelah semua vote telah

dilakukan. Protokol tersebut dinyatakan dapat memberikan privasi yang sangat maksimal, dikarenakan memerlukan semua pemilih untuk menyelesaikan pemilihan terlebih dahulu untuk dilakukan perhitungan. [12]

Adapun beberapa kelemahan dari protokol tersebut yaitu:

1. Pemilih terakhir dapat menghitung suara lebih dahulu dibandingkan yang lain
2. Adanya pemilih yang tidak melakukan pemilihan, sehingga pemilihan dinyatakan belum selesai

2.4.1.2 The Open Vote Network Protocol

The Open Vote Network Protocol menggunakan 2 babak untuk voting yaitu registrasi dan voting. Pada babak pertama yaitu registrasi, para pemilih meregistrasikan voting key mereka ke dalam sistem. Pada babak kedua yaitu voting, para pemilih akan memilih pemimpin yang mereka inginkan. [12]

Protokol tersebut dibagi menjadi dua bagian yaitu voter dan *observer*. Voter dimaksudkan untuk melakukan voting dan *observer* untuk melihat proses pemilihan yang sedang terjadi. [12]

2.4.1.3 Ethereum Network

Penelitian tersebut menggunakan jaringan Ethereum sebagai sistem *blockchain*. Jaringan Ethereum sendiri sudah terdiri dari dasar-dasar yang dibutuhkan untuk menjalankan sistem *blockchain*, namun dengan menggunakan jaringan Ethereum, maka pengguna diharapkan dapat melakukan mining untuk mendapatkan *cryptocurrency* yang nantinya akan digunakan untuk voting. [12]

Berikut merupakan spesifikasi dari jaringan Ethereum yang digunakan pada penelitian tersebut:

1. Menggunakan konsensus Proof of Stake (PoS)
2. Menggunakan sistem ekonomi Ethereum untuk menyimpan dan mengolah data
3. Menggunakan smart contract bernama solidity untuk melakukan transaksi

2.4.2. Digital Voting with the use of *Blockchain* Technology

Penelitian "Digital Voting with the use of *Blockchain* Technology" dibuat oleh Andrew Barnes, Christopher Brake, dan Thomas Perry di Plymouth University. Penelitian tersebut bertujuan untuk mengintegrasikan sistem *blockchain* dalam voting tanpa mengubah sistem voting yang ada sebelumnya. Penelitian tersebut

menggunakan *miner* milik pemerintah sebagai *leader* yang menentukan transaksi yang ada sah atau tidak. Penelitian tersebut juga menggunakan dua buah *blockchain* untuk memisahkan user dengan voting yang mereka lakukan untuk memastikan kerahasiaan identitas pemilihnya. [2]

Penelitian tersebut memiliki proses dan cara kerja sebagai berikut:

2.4.2.1 Registrasi

Ketika pemilih ingin melakukan registrasi untuk pertama kali, akan ada sebuah transaksi yang dilakukan berisikan data-data pemilih, lalu *miner* milik pemerintah akan membuat transaksi baru yang menentukan apakah transaksi sebelumnya yang dilakukan oleh pemilih yang mendaftar memiliki hak untuk memilih atau tidak dengan tujuan untuk memastikan identitas seseorang tidak disalahgunakan untuk tujuan penipuan. [2]

2.4.2.2 Voting

Sistem voting yang digunakan memiliki 3 buah node yaitu local, nasional, dan daerah. Node local adalah seluruh tempat pemungutan suara digital yang terkoneksi dengan node daerah. Node daerah terkoneksi dengan setiap node yang ada dengan subset dari node local yang ditentukan tergantung dengan lokasinya. Node nasional

merupakan node milik pemerintahan yang bertujuan untuk *mining transactions* dan voting untuk menambahkan block pada *blockchain*, seluruh node pemerintahan terkoneksi dengan node nasional untuk berkomunikasi dengan satu sama lain. Badan yang independen akan mengawasi dan memeriksa proses voting yang sedang terjadi. Badan tersebut harus terlebih dahulu memiliki akses ke node nasional dan dapat memeriksa kebenaran hasil enkripsi. Mereka juga dapat mencalonkan diri untuk menjadi node nasional dan akan menjadi *miner* saat proses penghitungan. [2]

Saat pemilihan, pemilih harus menunjukkan otentikasi berupa nomor identifikasi, password yang diberikan saat registrasi, dan kartu ballot yang berisikan kode QR. Setelah memilih, maka hasil tersebut akan menjadi transaksi dan akan di enkripsi menggunakan *public key* milik pemerintah. [2]

Di balik layar sistem pada tempat pemilihan akan melakukan verifikasi dengan *blockchain* untuk memastikan bahwa pemilih tersebut sudah memilih atau belum. Jika sudah, maka tempat pemilihan tidak mengijinkan pemilih tersebut untuk memilih.

Adapun beberapa fitur yang dimiliki dari penelitian tersebut yaitu:

1. Menggunakan dua buah *blockchain* untuk menjaga kerahasiaan pengguna dan pilihan mereka
2. Memiliki auditor pengaman yang memeriksa dan melacak lokasi pengguna yang terkoneksi
3. Menggunakan 3 faktor otentikasi yaitu ID, password, dan kartu polling
4. Memiliki double-check untuk memastikan pilihannya benar
5. Menggunakan enkripsi untuk menyimpan hasil voting

Ada beberapa kelemahan dari sistem yang dirancang berdasarkan penelitian tersebut yaitu:

1. Jika pemilih melupakan ID, password ataupun kartu polling saat hari voting, maka mereka tidak bisa memilih.
2. Adanya resiko terkena 51% attack, dimana mayoritas *miner* telah di compromised
3. Aplikasinya dapat dimodifikasi oleh pihak ketiga

2.4.3. Raft-based consensus for Ethereum/Quorum

Implementasi sistem "Raft-based consensus for Ethereum/Quorum" dibuat oleh seseorang yang memiliki username

jpmorganchase di GitHub. Penelitian tersebut mengimplementasikan Raft dalam sistem Ethereum, dimana seluruh sistem milik ethereum digunakan, namun konsensus yang digunakan oleh Ethereum yang bernama Proof-of-Stake diganti dengan Raft. Sistem konsensus Ethereum yang sebelumnya menggunakan banyak leader atau biasa diebut sebagai minter digantikan dengan satu leader dan tugas verifier masih seperti biasa. [14]

Implementasi sistem tersebut menghasilkan jawaban atas penggunaan clustering atau voting set pada penggunaan konsensus Raft dapat dilakukan jika cluster tersebut memiliki jumlah yang ganjil. [14]