BAB I

PENDAHULUAN

1.1. Latar Belakang

Sistem voting sangatlah sering digunakan, meskipun pengguna mungkin tidak sadar bahwa mereka sedang menggunakan sistem voting. Banyak juga penggunaan voting dalam kehidupan sehari hari yang mungkin terlewatkan seperti survei, ujian, petisi, sampai dengan pemilu. Voting juga sangat fleksibel dan dapat untuk dikembangkan lebih lanjut, seperti voting digital yang mulai banyak digunakan. Sisi keamanan voting digital perlu diwaspadai, dikarenakan datanya sangat mudah untuk diubah. Sistem voting digital yang ada harus dapat mengamankan data yang ada dan melindungi diri dari potansi serangan peretas yang ada sehingga datanya merupakan data yang benar. Salah satu potansi untuk menyelesaikan permasalahan keamanan adalah dengan menggunakan teknologi *blockchain.* [1]

Teknologi bernama *blockchain* yang terbilang baru digunakan untuk menyimpan transaksi seperti *cryptocurrency* sebagai layaknya *history log*. Pemanfaatan *blockchain* tersebut memungkinkan data untuk disimpan secara terdesentralisasi yang berarti data tersebut didistribusikan dan disebarkan ke semua pengguna, jadi semua memiliki data yang sama. Dengan menggunakan *blockchain* kita dapat menjamin keaslian datanya, dikarenakan datanya tidak bisa diubah setelah dimasukkan ke dalam *chain* dan juga untuk memasukkan data ke dalam *chain* tersebut dibutuhkan beberapa saksi guna memastikan data yang dimasukkan sah tanpa adanya kecurangan antara satu sama lain.

Penggunaan *blockchain* sebagai sarana penyimpanan data sangatlah jauh berbeda dengan *database* pada umumnya. *Database* yang biasa digunakan seperti SQL menggunakan sistem yang terpusat, dimana semua harus mengakses database yang sama jika ingin mengolah data yang ada, sedangkan *blockchain* menggunakan sistem desentralisasi yang telah dijelaskan sebelumnya. *Database* seperti SQL dapat diubah datanya sesuai dengan kebutuhan, sedangkan *blockchain* hanya bisa menambah data ke dalam *ledger* yang ada dan tidak bisa mengubah data yang ada setelah data tersebut dimasukkan ke dalam *blockchain*. Jika untuk merusak data dari *centralized database* hanya dengan meretas ke dalam server yang ada, pada *blockchain* peretas memerlukan *computing power* yang jauh melebihi mayoritas pengguna yang ada, sehingga untuk merusak data dari *blockchain* memerlukan upaya yang lebih besar dibandingkan *centralized database*. [2]

Blockchain memerlukan adanya konsensus untuk menjamin kesahihan datanya. Pada penelitian ini peneliti menggunakan algoritma Raft untuk menyelesaikan masalah konsensus pada *blockchain* yang akan dirancang. Raft digunakan karena toleransi kesalahannya dan performanya yang setara dengan algoritma konsensus yang sangat populer yaitu Paxos. Keunggulan Raft dibandingkan Paxos adalah dapat menyelesaikan beberapa masalah yang independen dan memiliki banyak bagian besar yang dibutuhkan untuk merancang sistem yang praktis [3].

Raft juga memiliki kelebihan dibandingkan algoritma konsensus yang umum digunakan pada sistem *blockchain* seperti *PBFT* (*Practical Byzantine Fault Tolerance)*, dimana Raft memiliki keunggulan dalam kecepatan dan

penggunaan bandwith yang lebih rendah dikarenakan Raft hanya menggunakan 2 jalan pengiriman data yaitu dari leader ke member dan dari member ke leader, sehingga kompleksitasnya saat worst case adalah O(N). Sedangkan *PBFT* menggunakan konsensus yang dimana setiap nodes harus mengirimkan broadcast ke semua nodes yang ada untuk mendapatkan hasil konsensus, sehingga kompleksitasnya saat worst case adalah $O(N^2)$.

Peneliti melihat penggunaan *blockchain* pada saat ini kebanyakan hanya terbatas pada *cryptocurrency*. Maka pada penelitian ini peneliti akan merancang sistem voting berbasis *blockchain* yang memungkinkan pemilih agar dapat melakukan voting dimana saja dan kapan saja, serta memastikan keaslian data tanpa adanya pihak ketiga yang memodifikasi datanya dan juga menggunakan algoritma Raft sebagai sarana konsensus.

1.2. Rumusan Masalah

Berdasarkan masalah yang diuraikan sebelumnya, maka rumusan masalah dari penelitian ini adalah bagaimana cara merancang *blockchain* dan konsensus yang dapat dijalankan pada aplikasi berbasis mobile, apakah sistem yang dirancang tahan terhadap serangan majority attack, dan berapa lama processing time yang diperlukan pada sistem ini?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini adalah:

1. Merancang sistem *blockchain* untuk menyimpan data voting.

2. Mengimplementasikan sistem tersebut dalam aplikasi berbasis mobile.

1.4. Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut:

1. Sistem hanya akan berfokus pada sistem *blockchain* dalam aplikasi mobile.
2. Bahasa pemrograman yang digunakan adalah Java*Script*.
3. Sistem dirancang dalam sistem operasi mobile menggunakan React Native.
4. Menggunakan ECDSA sebagai *asymmetric key encryption.*
5. *Public key* dan *private key* dihasilkan dari aplikasi.
6. Menggunakan algoritma konsensus Raft.
7. Menggunakan library Socket.io untuk mendukung *peer-to-peer*.
8. Sistem berjalan dengan asumsi kondisi ideal (tidak ada *majority attack* dan *network failure*).
9. Koneksi *peer-to-peer* dijalankan dalam local network.

1.5. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini dapat memberikan kemudahan untuk melakukan voting secara digital dan memastikan data voting disebarkan secara aman dan transparan tanpa adanya kecurangan.