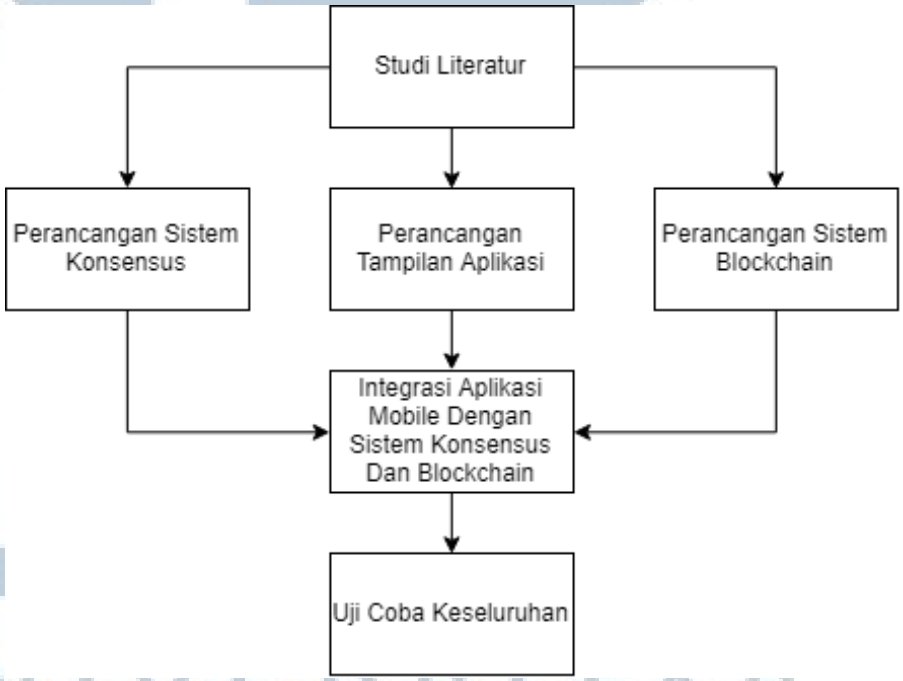
BAB III

METODE PENELITIAN

3.1. Metode Penelitian

Metode penelitian pada penelitian ini berdasarkan pada studi literatur, lalu dilanjutkan dengan perancangan dan integrasi sistem secara keseluruhan, pada akhirnya akan dilanjutkan dengan uji coba keseluruhan. Metode ini dipilih untuk menganalisa dan mengetahui kemampuan dari rancangan protokol dalam sistem yang akan dirancang oleh peneliti.

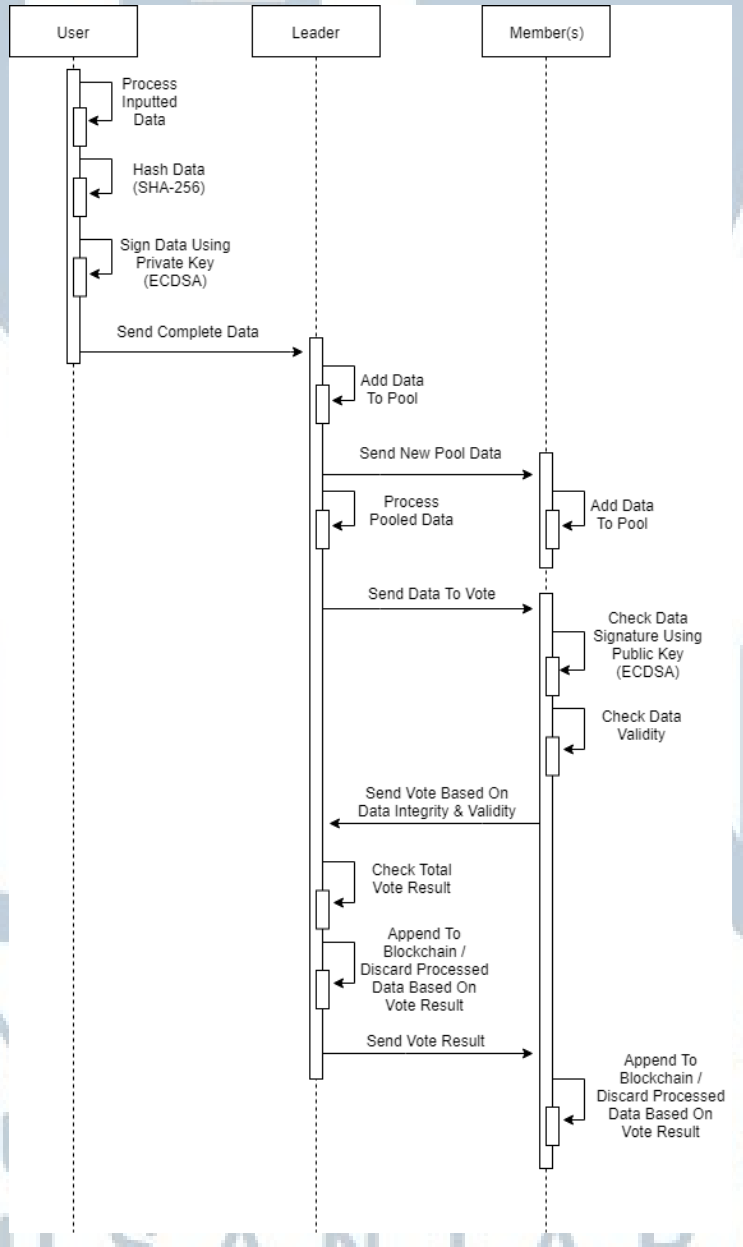
Gambar 3.1 menunjukkan alur penelitian yang dilakukan oleh peneliti secara keseluruhan.



Gambar 3.1 Block diagram alur penelitian

3.2. Perancangan Sistem *Blockchain*

Sistem *blockchain* dirancang menggunakan bahasa pemrograman Java*Script*, sehingga dapat diintegrasikan dengan aplikasi mobile yang akan dirancang. Sistem tersebut akan dirancang dalam bentuk library yang dapat dipanggil dalam sistem. Secara garis besar, cara kerja sistem *blockchain* yang dirancang memiliki diagram sekuensial pada Gambar 3.2.



Gambar 3.2 Diagram sekuensial cara kerja sistem blockchain yang dirancang

Blockchain yang digunakan menggunakan satu block untuk satu transaksi. Keunggulan dari menggunakan satu block untuk satu transaksi dibanding satu block untuk banyak transaksi adalah agar transaksi tersebut lebih cepat di proses, sehingga akan mempercepat waktu agar transaksi tersebut di masukkan ke dalam *blockchain* atau ditolak. Namun kerugian dengan menggunakan satu block untuk satu transaksi adalah penggunaan penyimpanan data untuk *blockchain* akan relatif lebih besar, dikarenakan satu transaksi memiliki header sendiri, sedangkan ukuran penyimpanan data akan lebih kecil ketika beberapa transaksi memiliki satu header yang sama.

Penelitian ini menggunakan dua buah *blockchain* yaitu kontrak untuk menyimpan data format voting dan transaksi yang digunakan untuk menyimpan data pilihan.

Blockchain akan menggunakan format JSON (Java*Script* Object Notation) dan akan disimpan dalam tempat penyimpanan pada aplikasi mobile. Rancangan JSON dari *blockchain* adalah sebagai berikut:

Tabel 3.1 Format JSON dalam *blockchain*

Name	Value	Description
contracts	Object	Object yang menyimpan *blockchain* kontrak
transactions	Object	Object yang menyimpan *blockchain* transaksi
chain	Array	Array yang menyimpan block

data	Object	Object yang menyimpan data kontrak dan transaksi
hash	Hexadecimal	Hasil *hash* dari block tersebut
index	Integer	Posisi block
prev*Hash*	Hexadecimal	*Hash* dari block terdahulu
sender	*Public key*	*Public key* dari pemilih
sign	Signature	Hasil *hash* yang di sign menggunakan *Private key*
timestamp	Integer	Timestamp saat block tersebut dibuat

3.3. Perancangan Algoritma Konsensus

Secara garis besar, perancangan algoritma konsensus pada penelitian ini terbagi menjadi dua bagian yaitu perancangan protokol *peer-to-peer* dan perancangan algoritma Raft.

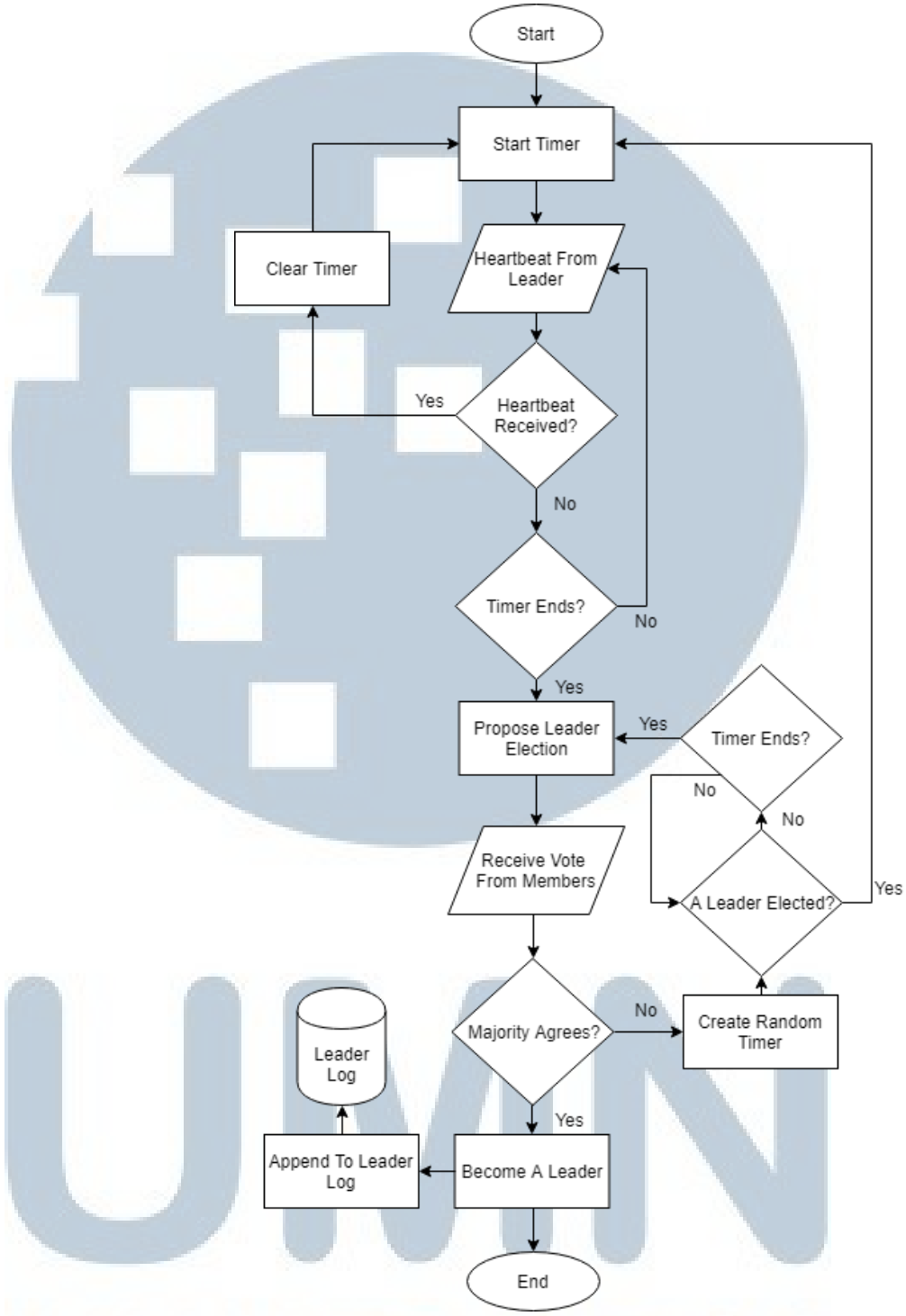
3.3.1. Perancangan Algoritma Raft

Sistem konsensus yang digunakan akan dirancang menggunakan bahasa pemrograman Java*Script* dan akan diimplementasikan dalam bentuk library. Sistem konsensus yang dirancang akan mengimplementasikan komunikasi *peer-to-peer* dan *blockchain* yang juga akan dirancang oleh peneliti.

Sistem yang dirancang akan menggunakan sistem kepemimpinan milik Raft seperti *heartbeat* untuk menyatakan bahwa pemimpinnya masih terhubung. Ketika ada anggota yang tidak menerima *heartbeat* dari pemimpin dalam kurun waktu tertentu, maka ia akan mencalonkan diri menjadi pemimpin, jika

mayoritas setuju maka ia akan menjadi pemimpin, jika tidak maka ia akan menunggu selama waktu acak yang ditentukan sebelum memulai pemilihan pemimpin lagi untuk menghilangkan adanya deadlock antar beberapa calon pemimpin, namun hal ini dapat disela ketika ada pemimpin baru yang terpilih, sehingga seluruh calon pemimpin akan menjadi anggota seperti biasa dan memulai alur sistemnya dari awal.

Secara garis besar sistem leader election dirancang sesuai dengan diagram alur pada Gambar 3.3.

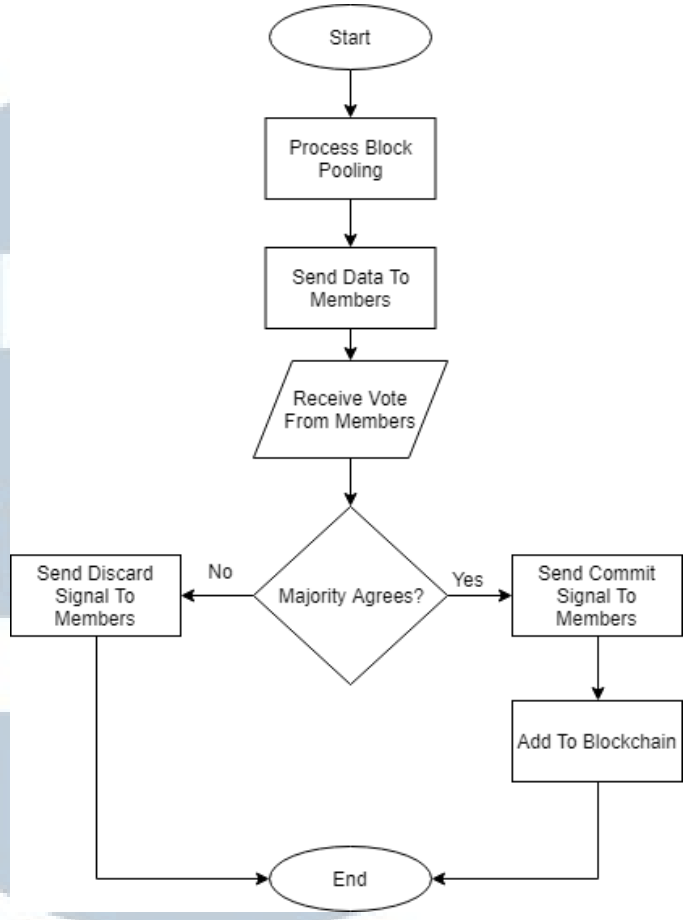


Gambar 3.3 Flowchart leader election

Log replication milik Raft tidak akan diimplementasikan dalam sistem yang akan dirancang dan sebagai gantinya akan digunakan *blockchain* sebagai log replication dalam sistem. Log

append akan diimplementasi dalam sistem dan akan digunakan ketika ada data baru yang ingin dimasukkan kedalam blockchain. Ketika ada data baru, pemimpin akan memproses data tersebut sesuai dengan gilirannya. Saat gilirannya untuk diproses, maka pemimpin akan mengirimkan data tersebut ke seluruh anggota yang ada dan juga menerima hasil voting dari seluruh anggota yang ada, jika mayoritas setuju maka pemimpin akan mengirimkan sinyal untuk commit kepada seluruh anggota lalu menambahkan data dalam blockchain dan jika ada anggota yang sebelumnya tidak setuju, maka ia harus melakukan sinkronisasi ulang, jika mayoritas tidak setuju, maka pemimpin akan mengirimkan sinyal discard kepada seluruh anggota dan membuang data tersebut.

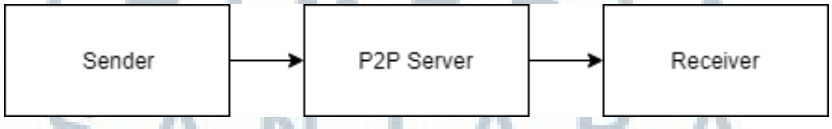
Secara garis besar sistem log append dirancang sesuai dengan diagram alur sebagai berikut:



Gambar 3.4 Flowchart log append

3.3.2. Perancangan Protokol *Peer-to-peer*

Protokol *peer-to-peer* akan dirancang dalam bahasa Java*Script* menggunakan library yang bernama Socket.IO. Dalam penelitian ini, peneliti akan menggunakan server *peer-to-peer* sebagai broker untuk komunikasi antara pengirim dan penerima. Alur dari komunikasi *peer-to-peer* yang dirancang oleh peneliti adalah sebagai berikut.



Gambar 3.5 Alur komunikasi *peer-to-peer*

Peneliti menggunakan dua buah metode transmisi data yaitu unicast dan broadcast. Unicast digunakan saat meminta sinkronisasi data pada pemimpin, mengirim hasil voting data dalam konsensus, mengirim hasil voting untuk pemilihan pemimpin jaringan, dan saat pengguna memilih pasangan yang mereka pilih dan melakukan konfirmasi voting. Broadcast digunakan saat pemimpin melakukan *heartbeat*, pemimpin baru menyatakan dirinya sudah terpilih, pemimpin mengirimkan data ke semua *miner* untuk diputuskan apakah data tersebut sah atau tidak, dan saat pemimpin menentukan data yang diterima dapat dimasukkan ke dalam *blockchain* atau tidak.

3.4. Perancangan Aplikasi Mobile

Dalam penelitian ini, peneliti akan menggunakan React Native sebagai *framework* perancangan aplikasi mobile. React Native digunakan untuk menyediakan aplikasi yang multi platform, agar lebih banyak pengguna yang dapat menggunakan sistem yang akan dirancang oleh peneliti.

3.4.1. Perancangan Sistem

3.4.1.1 Registrasi

Saat pengguna ingin melakukan registrasi, pengguna harus memasukkan username dan password ke dalam form yang telah diberikan pada halaman registrasi. Lalu akan dihasilkan private key berdasarkan hasil hash dari username,

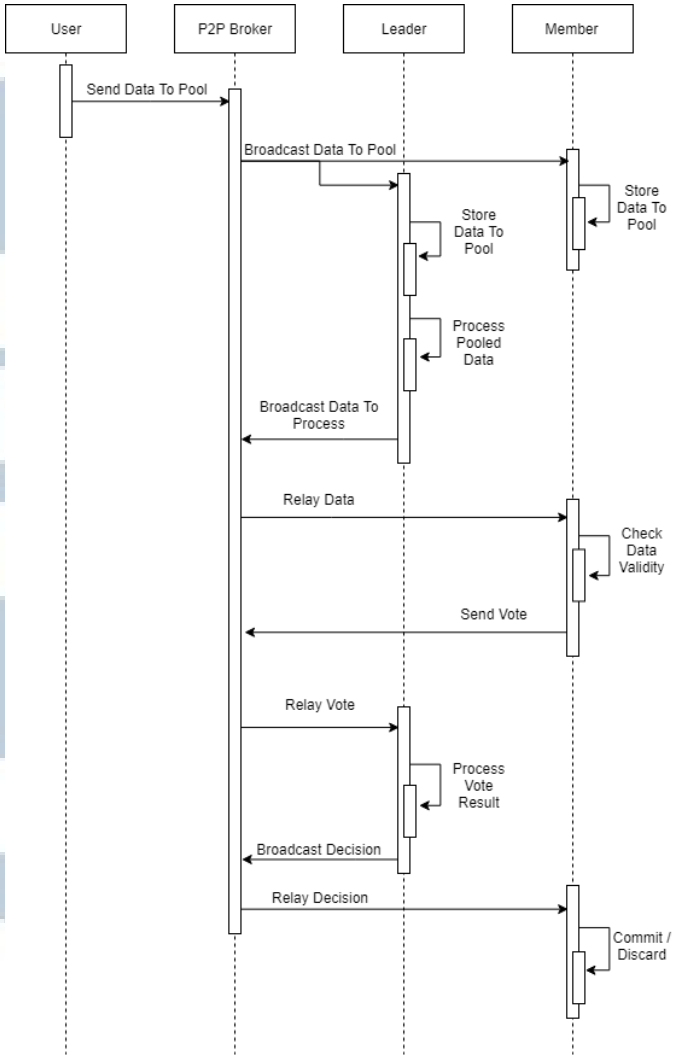
password, dan timestamp registrasi, sehingga dapat meminimalisir adanya *collision* antar private key penguna.

3.4.1.2 Input Data

Saat pengguna ingin memasukkan data ke dalam *blockchain*, maka dari perangkat pengguna akan mengirimkan data yang ingin di proses melalui broadcast kepada semua anggota konsensus termasuk pemimpin yang ada melalui *peer-to-peer* broker. Setelah itu pemimpin dan anggota akan menyimpan data tersebut kedalam block pool.

Pemimpin konsensus akan memroses data yang ada di pool secara berkala. Saat data tersebut diproses oleh pemimpin, ia akan mengirimkan data tersebut melalui broadcast ke semua anggota konsensus yang ada, lalu masing-masing anggota akan melakukan validasi data tersebut dan mengirimkan hasil validasi mereka (yes/no) melalui broker. Pemimpin yang menerima hasil tersebut akan menentukan jika data yang ada dapat dimasukkan ke dalam *blockchain* atau tidak berdasarkan suara dari para anggota. Selanjutnya pemimpin akan mengirimkan keputusan kepada seluruh anggota dan setiap anggota harus menaatinya.

Berikut adalah diagram sekuensial saat pengguna ingin memasukkan data ke dalam *blockchain*:



Gambar 3.6 Diagram sekuensial input data

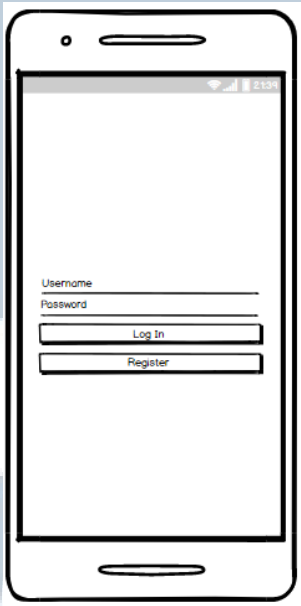
3.4.2. Perancangan User Interface

Secara garis besar, user interface untuk aplikasi mobile yang akan dirancang akan memiliki 3 buah halaman yaitu halaman login, halaman voting, dan halaman recent blocks.

3.4.2.1 Rancangan Halaman Login

Halaman ini berfungsi sebagai halaman awal pengguna untuk masuk ke dalam sistem voting. Gambar 3.7 menampilkan rancangan halaman login. Ada dua buah

<InputText> untuk melakukan input username dan password yang akan digunakan sebagai pemastian identitas saat login. Ada dua buah <Button> yang tertulis “Log In” dan “Register”. Register button digunakan untuk navigasi ke halaman register dan log in button digunakan untuk masuk ke dalam menu utama jika username dan password sesuai, jika tidak maka akan menampilkan <Alert> berisi kesalahan yang terjadi.

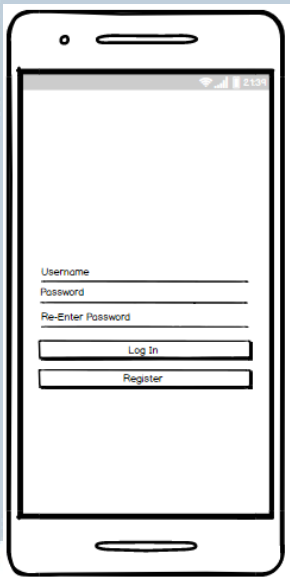


Gambar 3.7 Rancangan halaman login

3.4.2.2 Rancangan Halaman Register

Halaman register merupakan halaman yang digunakan untuk registrasi pengguna. Gambar 3.8 menunjukkan rancangan halaman register. Halaman ini memiliki tiga buah <TextInput> yaitu username yang berisikan private key pengguna yang dihasilkan secara

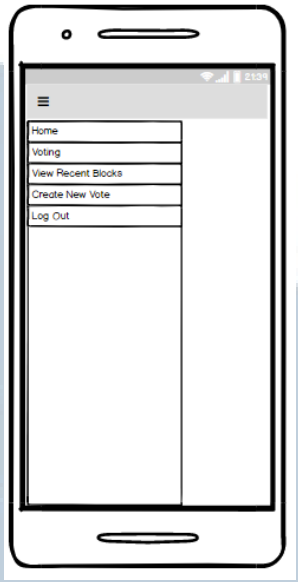
otomatis dari sistem, password, dan re-enter password yang digunakan sebagai password untuk username tersebut. Ada dua buah <Button> yaitu log in yang digunakan untuk navigasi ke halaman login dan register untuk melakukan registrasi sesuai dengan data yang dimasukkan pengguna.



Gambar 3.8 Rancangan halaman register

3.4.2.3 Rancangan Menu Utama

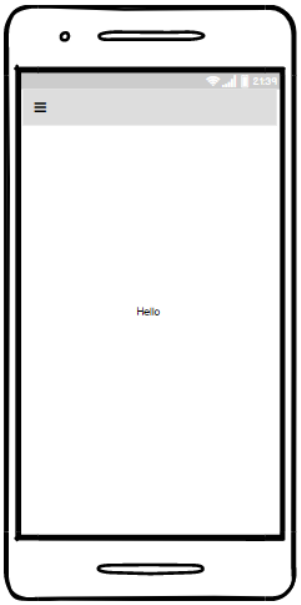
Menu utama dirancang menggunakan <DrawerNavigator> untuk navigasi pengguna setelah sukses melakukan log in. Akan dilakukan navigasi saat sesuai dengan pilihan menu yang dipilih oleh pengguna kecuali saat pengguna memilih menu log out dimana pengguna akan keluar dari sistem dan akan terjadi navigasi ke halaman log in. Gambar 3.9 menunjukkan rancangan menu utama.



Gambar 3.9 Rancangan menu utama

3.4.2.4 Rancangan Halaman Home

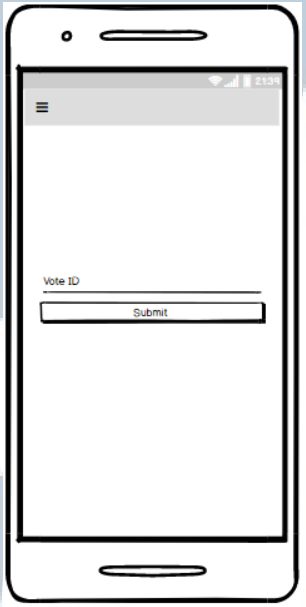
Halaman home merupakan halaman awal yang akan ditampilkan setelah pengguna berhasil log in. Gambar 3.10 menunjukkan rancangan halaman home.



Gambar 3.10 Rancangan halaman home

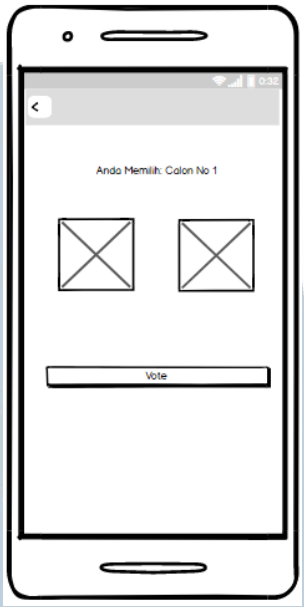
3.4.2.5 Rancangan Halaman Voting

Halaman voting merupakan halaman yang digunakan oleh pengguna untuk melakukan voting. Halaman ini berisikan satu buah <TextInput> untuk memilih voting mana yang akan dilakukan sesuai dengan voteId, satu buah <Button> untuk membuka <Modal> voting sesuai dengan voteId yang telah dimasukkan. Gambar 3.11 menampilkan rancangan halaman voting.



Gambar 3.11 Rancangan halaman voting

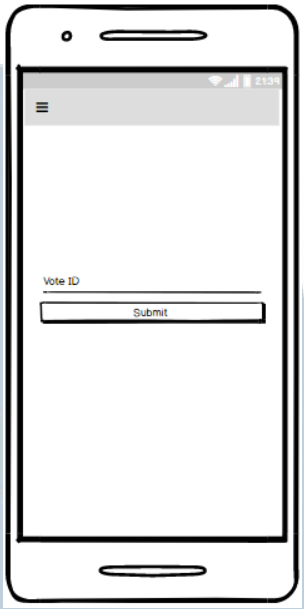
<Modal> untuk voting berisikan satu buah text untuk menunjukkan pilihan pengguna, tiga buah <Button> untuk memilih calon dan mengkonfirmasi pilihan, dan sebuah <Button> pada kiri atas layar untuk kembali ke halaman voting. Gambar 3.12 menunjukkan rancangan modal untuk melakukan voting.



Gambar 3.12 Rancangan voting modal

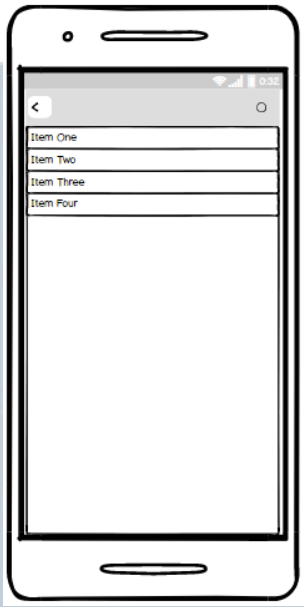
3.4.2.6 Rancangan Halaman View Recent Blocks

Halaman voting merupakan halaman yang digunakan oleh pengguna untuk melihat hasil voting. Halaman ini berisikan satu buah <TextInput> untuk memilih block untuk voting mana yang akan ditampilkan sesuai dengan voteId, satu buah <Button> untuk membuka <Modal> voting sesuai dengan voteId yang telah dimasukkan. Gambar 3.13 menampilkan rancangan halaman voting.



Gambar 3.13 Rancangan halaman view recent blocks

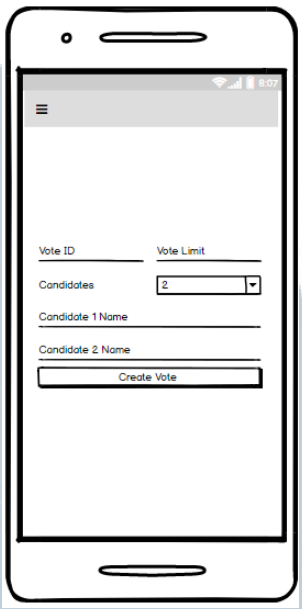
<Modal> untuk view recent blocks berisikan satu buah text untuk menunjukkan vote id pilihan pengguna dan juga jumlah vote yang telah dilakukan, satu buah <FlatList> untuk menampilkan data dari block yang sesuai dengan vote id, dan dua buah <Button> yaitu back untuk kembali ke halaman view recent blocks dan reload untuk menyegarkan <FlatList> yang ditampilkan. Gambar 3.14 menunjukkan rancangan modal untuk menampilkan block.



Gambar 3.14 Rancangan view recent blocks modal

3.4.2.7 Rancangan Halaman Create New Vote

Halaman create new vote merupakan halaman yang digunakan oleh pengguna untuk membuat vote baru. Halaman ini berisikan 4 buah <TextInput> yaitu vote id untuk memilih voting id yang akan digunakan, vote limit untuk membatasi jumlah pengguna yang melaukan voting, dan ada sebuah picker untuk mengubah jumlah kandidat yang dapat dipilih dan juga ada candidate name untuk memasukkan nama kandidat yang akan dipilih. Ada juga sebuah <Button> untuk membuat vote sesuai data yang dimasukkan pengguna. Gambar 3.16 menampilkan rancangan halaman create new vote.



Gambar 3.15 Rancangan halaman create new vote

3.4.3. Integrasi *Blockchain* dan Konsensus

Blockchain dan konsensus akan diimpor sebagai layaknya library ke dalam aplikasi mobile saat aplikasi tersebut dijalankan. Library tersebut jalan pada latar belakang aplikasi sehingga tidak dapat berinteraksi dengan pengguna secara langsung. Pada awal pengguna membuka aplikasi, pengguna tersebut akan menjadi miner tanpa disadari dan juga akan berkomunikasi menggunakan *peer-to-peer* kepada titik yang lain di latar belakang.

Hanya ada satu buah fungsi yang dapat dijalankan dengan interaksi pengguna yaitu fungsi untuk memasukkan data pilihan ke dalam pooling block. Fungsi tersebut nantinya akan mengirimkan data pilihan pengguna kepada pemimpin dari konsensus, nantinya akan dilakukan pemrosesan dalam konsensus untuk menentukan apakah data tersebut sah atau tidak.

3.5. Pengumpulan Data Penelitian

Data penelitian akan dikumpulkan dengan cara pelaksanaan uji coba secara langsung pada perangkat mobile setidaknya 2 buah yang memiliki spesifikasi seperti yang ditentukan oleh peneliti.

3.6. Instrumen Penelitian

Penelitian dilakukan menggunakan instrumen perangkat keras maupun perangkat lunak berikut:

1. Satu buah PC berspesifikasi prosesor Intel Core i7, RAM 12GB
2. Satu buah ponsel Android dengan minimum API 21 atau ponsel iOS dengan minimum OS 8
3. Text editor (Sublime Text)
4. Node.js
5. React Native