BAB 1

PENDAHULUAN

1.1. Latar Belakang

Belakangan ini, teknologi blockchain sangatlah populer. Ini dikarenakan banyak sekali berita-berita tentang Bitcoin yang beredar saat ini. Bitcoin utamanya digunakan dalam transaksi di internet tanpa menggunakan perantara alias tidak menggunakan jasa bank [24]. Tetapi penggunaan blockchain bukan pada Bitcoin saja, salah satu blockchain paling populer lainnya adalah Ethereum. Blockchain adalah sebuah tipe data struktur yang bersifat append only, dimana data yang sudah ditulis tidak dapat diubah. Oleh karena itu, data hanya dapat ditambahkan ke blockchain. Karena blockchain mempunyai karakteristik data struktur tersebut, maka terdapat banyak kegunaan yang bisa diperoleh, salah satunya adalah membuat data menjadi tidak dapat diubah seperti data Bitcoin ataupun data dari *smart contract* Ethereum. Data struktur tersebut mempunyai keunggulan dibandingkan data struktur lainnya, yaitu karena immutability dari data struktur tersebut. Banyak sekali keuntungan dari transaksi yang tidak dapat diubah ini, dan oleh karena itu para pengusaha, perusahaan startup, investor, organisasi global dan pemerintah semuanya telah mengidentifikasi blockchain sebagai teknologi revolusioner [34].

Blockchain dalam dunia perusahaan atau industri melakukan perkembangan yang cukup pesat mulai dari tahun 2014. Forbes mengeluarkan daftar Forbes Blockchain 50 yang dimana perusahaan-perusahaan raksasa di dunia sudah mulai melirik Blockchain bahkan mengimplementasikan teknologi blockchain mulai dari Amazon, Google, Microsoft, dll. Blockchain service sendiri sudah termasuk dalam layanan Cloud sehingga penggunaan teknologi tersebut bagi perusahaan membuat penghematan biaya. Association Research Follow Blockchain Daekin University, Dimaz Wijaya, menungkapkan bahwa blockchain membuat perubahan besar yaitu internet of value. Dahulu internet dikenal sebagai tempat untuk bertukar informasi, sementara saat ini blockchain dikenal sebagai tempat untuk bertukar nilai atau transaksi. Manfaat blockchain yang ditawarkan sehingga menjadikan internet of value adalah transaksi yang permanen sehingga apabila sudah melakukan transaksi

tidak bisa di-cancel, semua informasi yang terdapat di blockchain dapat dipastikan kebenarannya, terdapat banyak produk blockchain yang ada di seluruh dunia, kepemilikannya dipastikan menggunakan digital signature, dapat memindahtangankan kepemilikan token tersebut ke orang lain dengan mudah, memiliki uang yang tidak hanya memiliki angka, namun memiliki fungsi dalam mengelola uang tersebut [6].

Ethereum adalah sebuah blockchain yang mampu menjalankan kode yang ditulis oleh programmer, yang biasa disebut dengan *smart contract*. Bahasa pemrograman yang digunakan untuk membuatnya adalah Solidity. Untuk menjalankan program yang dibuat, dibutuhkan sebuah satuan unit dari Ethereum untuk membayar para *miner*, dan disebut “gas". Setiap baris kode yang digunakan dalam program memiliki satuan gasnya masing-masing. Keseluruhan dari seluruh barisan kode tersebut akan dijumlahkan dan menjadi harga untuk menjalankan sebuah fungsi pada Ethereum. Miner adalah orang orang yang menjalankan suatu program yang memastikan blockchain Ethereum bisa bertransaksi. Cara program tersebut membuat blockchain tetap hidup adalah dengan para miner tersebut mine sebuah block. Sebuah block akan di mine sehingga valid, dan apabila block tersebut valid, maka akan di broadcast ke seluruh network. Program tersebut melakukan mine dengan mengambil sebuah block, lalu di hash, dan di cari hasil hashing tersebut yang sesuai dengan difficulty yang ada sekarang. Semakin berat sebuah komputasi yang dijalankan oleh Ethereum, semakin banyak gas yang diperlukan untuk membayar para miner, karena semakin berat sebuah komputasi, maka semakin banyak resource yang diperlukan oleh Ethereum network.

Dikarenakan harga tiap transaksi sangatlah penting, maka sudah ada beberapa penelitian mengenai optimasi pada *smart contract*. Salah satunya adalah berasal dari peneliti bernama Chen Yi-Cyuan. Pada penelitian tersebut, penulis lebih menjurus kepada penempatan deklarasi lokasi variable. Hal tersebut didasari oleh sistem penyimpanan dari Ethereum sendiri, yaitu setiap bytes32 , ia akan menyimpan sebuah nilai. Walaupun nilai tersebut memiliki besar yang lebih kecil dibandingkan dengan bytes32, Ethereum akan tetap memesan memori sebesar bytes32 ”Memori membutuhkan biaya 3 gas untuk setiap 32 byte yang diperpanjang. Harga gas saat ini sekitar 50 gwei yang artinya 1 GB harganya 4,7 eth. Namun, sebagian besar byte

tersebut adalah nol, dan tidak akan memakan ruang di penambang karena tersembunyi di balik hash. Jadi jika Anda menyetel setiap 32 byte ke nilai bukan nol, itu akan menelan biaya 20.000 gas per 32 byte, atau 31k eth / GB" [29]. Penelitian kedua berasal dari Lucas Aschenbach, yaitu menggabungkan sebuah node atau beberapa variabel untuk memenuhi besar bytes32 yang telah dipesan oleh Ethereum [5].

Pada saat ini fungsi keccak256 banyak digunakan untuk berbagai macam kebutuhan. Salah satu contohnya adalah dalam Merkle Tree yang digunakan pada teknologi blockchain yang diterapkan oleh Bitcoin. Dikarenakan keccak256 sebuah fitur avalanche effect dimana jika terjadi sekecil apapun perubahan didalam sebuah data, file maupun text akan menimbulkan bentuk hash yang sangat berbeda. Hal ini penyerupai seperti gunung es yang longsor jika para pendaki tidak hati-hati dan mengubah struktur dari gunung es. Dari fitur avalanche effect tersebut keccak256 memiliki peran yang penting dalam sistem blockchain di Bitcoin, yaitu sebagai penjamin bahwa seluruh data yang tersimpan didalam blockchain bersifat immutable, permanen, dan saling mengunci satu blok dengan blok lainnya.

Berdasarkan pemaparan diatas, penulis menggagaskan ide baru untuk mengurangi penggunaan gas dengan mengurangi berat komputasi yang menggunakan multiple parameter mapping dengan menggunakan algoritma keccak256. Dengan mengurangi dimensi dari map yang digunakan, komputasi *smart contract* di network Ethereum menjadi lebih ringan dan gas yang digunakan pun berkurang.

1.2. Identifikasi Masalah

Berdasarkan latar belakang diatas, yang menjadi permasalahan yang akan dibahas adalah sebagai berikut:

1. Bagaimana cara mengatasi transaksi yang cukup mahal ini di Jaringan Ethereum?
2. Bagaimana cara mengatasi kesulitan metode penggabungan dimensi map dengan algoritma hashing keccak256 dapat meningkatkan efisiensi dari gas yang digunakan pada *smart contract*?
3. Bagaimana implementasi yang tepat untuk memaksimalkan potensi dari harga value pada teknologi blockhain ini?

1.3. Maksud dan Tujuan

Maksud dari penelitan ini adalah untuk menerapkan teknologi blockhain pada aplikasi Dapp web yang bertujuan sebagai berikut:

1. Membantu dengan memanfaatkan api keccak256 yang dapat membawa perubahan pada teknologi blockhain ini sebagai jalan penghematan terbaru pada sebuah transaksi blockchain di jaringan Ethereum.
2. Dapat meringankan user dalam bertransaksi dalam skala jumlah yang lumayan banyak agar terhindar dari biaya gas yang cukup mahal dengan menggunakan api keccak256 yang memanfaatkan metode dari system pembulatan dari bytes32 yang terdiri dari multiple dimensi mapping yang berpengaruh pada besarnya biaya transaksi dan juga dapat mengurangi biaya transaksi pada *smart contract*.
3. Untuk membantu potensi dalam memaksimalkan sebuah transaksi ini penulis akan membuat aplikasi Desentral Aplikasi Web (DApp Web) yang nantinya akan menjumlahkan data parameter yang ada dan diproses secara langsung dapat terlihat hasil optimasi gas fee yang dapat diakses oleh user

1.4. Batasan Masalah

Adapun batasan masalah dalam pembangunan sistem ini agar dapat terarah dan dapat mencapai tujuan yang telah ditentukan adalah sebagai berikut :

1. Bahasa pemrograman yang digunakan yaitu Solidity yang jika dijalankan akan terintegrasi dengan web simple dari JavaScript web3.js
2. Aplikasi program terdiri dari aplikasi DApp web sebagai tampilan utama dan servernya yaitu Metamask sebagai penghubung ke jaringan Ethereum.
3. Pengujian dan pemaparan sistem yang dibangun menggunakan jaringan blockchain ethereum local atau private yaitu dengan ektensi browser Metamask dibawah Ethereum Virtual Machine.
4. Aplikasi Dapp web ini hanya dapat digunakan untuk membuktikan optimasi algoritma hashing keccak256.
5. Framework yang digunakan yaitu ReactJS sebagai client-side dan NodeJS sebagai server-side.
6. Text Editor dalam membangun aplikasi menggunakan Sublime Text 3.
7. Aplikasi Dapp web ini juga tidak mengandung unsur smart contract.
8. Pembangunan aplikasi Dapp web ini pun berbasis objek dengan tools pemodelan UML (Unified Modelling Language).

1.5. Metodologi Penelitian

Untuk melakukan penelitian ini, salah satu hal yang paling penting untuk dikerjakan adalah pengumpulan data. Pengumpulan data berguna untuk mengetahui apa saja yang diperlukan dalam melakukan eksperimen ini dan apa saja hasil dari eksperimen ini.

Untuk pengumpulan data, penulis memiliki 2 cara, yaitu dengan metode observasi dan studi literature dengan riset melalui internet dan eksperimentasi dengan kode penulis tersebut. Observasi melalui internet dapat dilakukan dengan membaca jurnal dan artikel yang ada dalam internet.

Data penting lainnya yang kita harus ambil pada pelaksanaan skripsi ini adalah data konsumsi gas, dan penulis dapat memperoleh data tersebut dengan mendeploy *smart contract* tersebut ke blockchain Ethereum. Dengan mendeploy *smart contract* yang sebelum dan sesudah digunakan algoritma keccak256 pada parameter, kita dapat mengetahui seberapa banyak masingmasing *smart contract* menggunakan gas, dan penulis dapat membandingkan hasil kedua data tersebut.

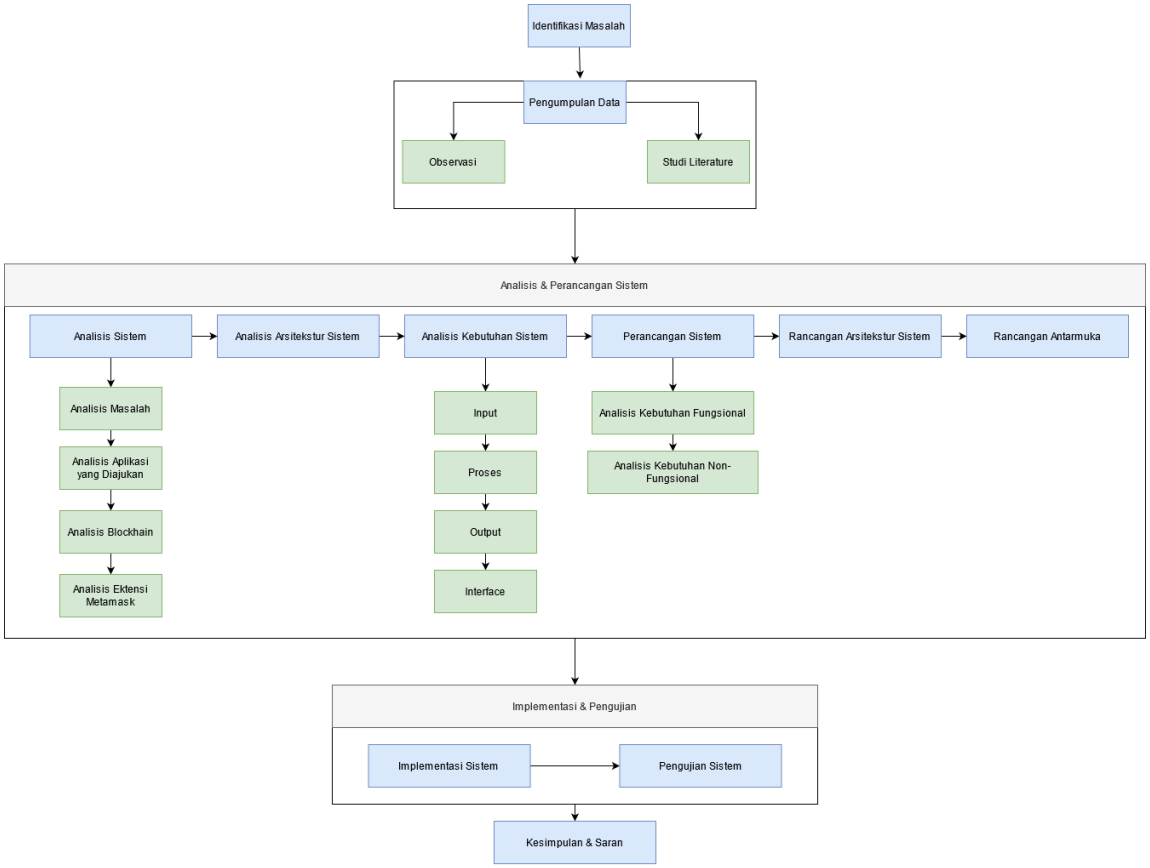
Untuk melakukan hal tersebut, *smart contract* pertama yang kita buat adalah kode yang masih belum diproses mapnya dengan algoritma keccak. Ini artinya key dari map tersebut masih berupa multidimensional parameter. *Smart contract* kedua yang kita harus buat adalah kode yang sudah kita optimisasi key mapnya dengan algoritma keccak256. Kedua *smart contract* ini akan di deploy ke Ethereum network. Sesudah itu penulis dapat memperoleh data seberapa banyak gas yang digunakan oleh masing-masing *smart contract*. Dengan menggunakan *smart contract* yang sudah dioptimisasi, gas yang diperlukan untuk melakukan kalkulasi yang sama akan berkurang.

Untuk proses pengembangan aplikasi ini, penulis menggunakan solidity sebagai bahasa pemograman yang dapat digunakan pada Ethereum. Dan tidak kalah pentingnya, penulis juga menggunakan react untuk front end dari aplikasi penulis agar dapat dijalankan dengan mudah dan responsif.

Dalam membuat aplikasi ini, penulis menggunakan metodologi agile. Agile adalah sebuah metodologi pembuatan software yang mementingkan kecepatan dan efisiensi. Dengan digunakannya metodologi ini, penulis dapat membuat aplikasinya

dengan cepat. Dari semua teknik agile yang dapat dipilih, penulis menggunakan teknik extreme programming.

Berikut merupakan alur gambar metode penelitian yang digunakan .



Gambar 1.0.1 Alur Penelitian

1.5.1 Metode Pengumpulan Data

Adapun pengumpulan data yang digunakan pada penelitian ini adalah sebagai berikut:

a. Studi Literatur

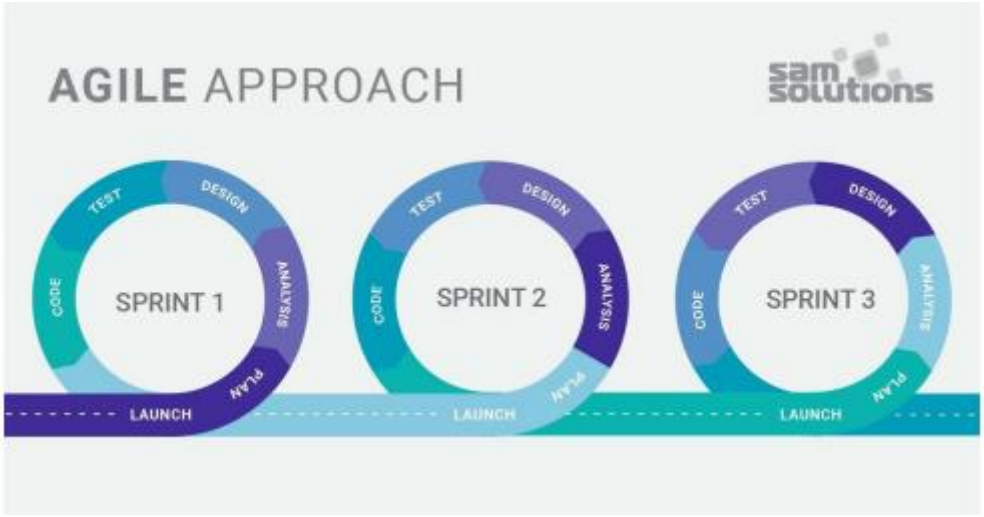
Studi literatur merupakan pengumpulan data yang meneliti berbagai macam dokumen yang berguna untuk bahan analisis dan tidak ditujukan langsung kepada subjek penelitian. Data tersebut merupakan daftar pustaka yang berupa artikel, jurnal, buku, dan laporan akhir yang ada kaitannya dengan judul penelitian.

b. Observasi

Observasi adalah teknik pengumpulan data dengan melihat situasi peneliti dalam melihat situasi penelitian. Beberapa informasi yang diperoleh dari hasil observasi adalah ruang (tempat), pelaku, kegiatan atau peristiwaan, dan waktu.

1.5.2 Metode Pembangunan Perangkat Lunak

Sistem ini dibuat dengan menggunakan bahasa Solidity. Bahasa pemograman ini adalah Bahasa khusus yang dimiliki oleh Ethereum. Karena sistem ini ingin berinteraksi dengan Ethereum, maka penulis harus menggunakan Solidity untuk mengoptimisasi. Pada pembuatan sistem ini, penulis menggunakan metodologi agile, dimana metodologi ini bertujuan untuk mempercepat pembuatan sebuah aplikasi atau sistem. Berikut adalah gambaran dari sistem Metodologi Agile



Gambar 1.0.2 Rancangan Penelitian

Sumber : https://www.sam-solutions.com/blog/waterfall-vs-agile-a-comparison-of-software-development-methodologies/

Akan tetapi, banyak sekali teknik agile yang dapat saya gunakan sekarang. Dari semua pilihan yang ada, penulis menggunakan teknik Extreme Programming. Extreme programming adalah teknik pembuatan software yang mementingkan kecepatan daripada dokumentasi. Berikut adalah langkah- langkah yang harus ditempuh untuk menjalankan teknik Extreme Programming.

- **Planning**

Pada tahap ini, para pembuat software akan membicarakan apa saja yang dibutuhkan dalam software ini dan bagaimana cara membuatnya dengan cepat. Pada planning ini, pembuatan software lebih dipentingkan daripada pembuatan dokumentasi.

- **Requirement Analysis**

Banyak pertemuan dengan user dan memberitahu user tentang informasi secara rinci

- **Design**

Pada tahap ini, para pembuat software akan mendesign sistem dari software tersebut agar software dapat berjalan dengan baik. Apabila software tidak di design, maka nanti kedepannya akan banyak bug yang ada dalam software tersebut, dan menggambarkan rancangan tampilan depan yang akan dibuat sehingga para peneliti yang lain dapat melihat dengan lebih jelas mengenai optimasi yang akan dilakukan pada penelitian ini. Pada tahap ini juga akan ditentukan spesifikasi dari versi, perangkat, dan alur dari program yang akan dibuat.

- **Code**

Pada tahap ini, hal yang terpenting adalah menulis code. Code yang dimaksud disini adalah code yang ditulis yang bertujuan untuk menyelesaikan masalah yang ada.

- **Testing**

Setelah menulis code selesai, maka tahap testing dimulai. Tahap ini bertujuan untuk memastikan bahwa software yang sudah dibuat berjalan dengan baik sehingga user tidak akan mendapatkan bug ketika menggunakan software tersebut.

- **Launching**

Kemudian terakhir aplikasi siap untuk dkirimkan ke pelanggan/user

1.6. Sistematika Penulisan

Sistematika penulisan skripsi tugas akhir ini disusun untuk memenuhi gambaran dari maksud dan tujuan penelitian yang dilakukan. Sistematika penulisan skripsi tugas akhir ini adalah sebagai berikut:

- **BAB I PENDAHULUAN**

Pada bab ini berisi uraian latar belakang masalah, rumusan masalah, maksud dan tujuan, , manfaat penelitian, batasan masalah, metodologi penelitian yang berisi metode pengumpulan data dan metode pembangunan perangkat lunak dan juga terakhir sistematika penulisan.

- **BAB II TINJAUAN PUSTAKA**

Pada bab ini akan membahas berbagai konsep-konsep dasar dan teori-teori pendukung yang berhubungan dengan pembangunan sistem. Seperti pembahasan mengenai landasan teori mengenai teknologi blockchain, definisi jaringan Ethereum, teori Ethereum Virtual Machine, penjelasan algoritma hashing Keccak256 pada Ethereum, Bahasa pemrograman Soldity beserta web.js nya dan tool-tool yang digunakan dalam proses pembangunan system ini. Dan terakhir hasil penelitian sebelumnya.

- **BAB III ANALISIS DAN PERANCANGAN**

Pada bab ini berisi pemaparan analisis sistem, analisis arsitekstur sistem, analisis kebutuhan sistem, dan terakhir perancangan system yang mengandung rancangan kebutuhan non-fungsional dan fungsional kemudian rancangan arsitekstur system kemudian tampilan antarmuka. Hasil dari analisis dan

perancangan tersebut dibutuhkan untuk mencapai maksud dan tujuan dari system ini.

- **BAB IV IMPLEMENTASI DAN PENGUJIAN**

  Pada bab ini berisi hasil implementasi analisis dari BAB 3 dan perancangan aplikasi yang dilakukan, serta hasil pengujian sistem untuk mengetahui apakah sistem yang dibangun sudah memenuhi kebutuhan.

- **BAB V PENUTUP**

  Pada bab ini berisi kesimpulan yang diperoleh dari hasil pengujian sistem, serta saran untuk pengembangan sistem terdesentralisasi yang telah dirancang.