<<JUDUL SKRIPSI / TUGAS AKHIR>>

**[SKRIPSI | TUGAS AKHIR]**

**Oleh**

**<<Nama Penulis>> <<NIM >>**

**[<<Nama Penulis>> <<NIM >>]**

**[<<Kelas/Kelompok>> :<<Kelas>>/<<Kelompok>>] \***



**<<Program>>**

**<<Program Studi>**

**<<Nama Fakultas/School>>**

**Universitas Bina Nusantara**

**Jakarta**

**<<Tahun lulus>>**

# <<JUDUL SKRIPSI/ TUGAS AKHIR>>

**[SKRIPSI | TUGAS AKHIR]**

**diajukan sebagai salah satu syarat**

**untuk gelar kesarjanaan pada**

**Program Studi <<Nama Program Studi>>**

**Jenjang Pendidikan Strata-1**

**Oleh**

**<<Nama Penulis>> <<NIM >>**

**[<<Nama Penulis>> <<NIM >>]**

**[<<Nama Penulis>> <<NIM >>]**

**[<<Kelas/Kelompok>> : <<Kelas>>/<<Kelompok>>] \***



**<<Program>>**

**<<Program Studi>**

**<<Nama Fakultas/School>>**

**Universitas Bina Nusantara**

**Jakarta**

**<<Tahun lulus>>**

<<JUDUL SKRIPSI / TUGAS AKHIR>>

**[SKRIPSI | TUGAS AKHIR]**

**Disusun Oleh**

**<<tanda tangan>> [<<tanda tangan>>]**

**<<Nama Penulis>> [<<Nama Penulis>>]**

**<<NIM>> [<<NIM>>]**

**Disetujui oleh:**

**Pembimbing dan Head of Study Program**

**<<tanda tangan>> <<tanda tangan>>**

**<<Nama Pembimbing 1>> [<<Nama Pembimbing 2>>]**

**<<Kode Dosen>> [<<Kode Dosen>>]**

**<<tanda tangan>>**

**<<Nama Head of Study Program >>**

**Head of<<Nama Program>> Study Program**

**Universitas Bina Nusantara**

**Jakarta**

**<<Tahun lulus>>**

**PERNYATAAN**

Dengan ini saya,

Nama : <<Nama Mahasiswa>>

NIM : <<NIM Mahasiswa>>

Judul Skripsi : <<Judul Skripsi>>

Memberikan kepada Universitas Bina Nusantara ***hak non-eksklusif***untuk menyimpan Skripsi karya saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja, dalam bentuk format tercetak dan atau elektronik.

Menyatakan bahwa saya, tidak akan menggunakan seluruh atau sebagian isi Skripsi saya, dalam bentuk apapun juga termasuk dalam penelitian karya ilmiah saya selanjutnya.

Jakarta, <<tanggal ……>>

Hormat saya, Diketahui oleh,

<<Tanda Tangan>> <<Tanda Tangan>>

## <<Nama Mahasiswa>> <<Nama Dosen>>

<<NIM Mahasiswa*>>* <<Kode Dosen*>>*

**UNIVERSITAS BINA NUSANTARA**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<<Nama Fakultas/School>>

Program <<Nama Program>>

[Skripsi| Tugas Akhir] <<Nama Sarjana>>

Semester [Ganjil/Genap] Tahun <<Tahun Semester /Tahun Semester>>

**<<JUDUL SKRIPSI / TUGAS AKHIR>>**

**<<Nama Penulis>><<NIM>>**

**[<<Nama Penulis>><<NIM>>]**

**[<<Nama Penulis>><<NIM>>]**

**[Kelas/Kelompok : <<Kelas>>/<<Kelompok>>]**

***ABSTRACT***

*Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english Abstract in english*

***Keywords*** *:<<keyword 1>>, <<keyword 2>>, ....*

# ABSTRAK

Abstrak dalam bahasa indonesia Abstrak dalam bahasa indonesia Abstrak dalam bahasa indonesia Abstrak dalam bahasa IndonesiaAbstrak dalam bahasa Indonesia Abstrak dalam bahasa Indonesia Abstrak dalam bahasa indonesia Abstrak dalam bahasa indonesia Abstrak dalam bahasa indonesia Abstrak dalam bahasa indonesia Abstrak dalam bahasa IndonesiaAbstrak dalam bahasa Indonesia Abstrak dalam bahasa Indonesia Abstrak dalam bahasa indonesia Abstrak dalam bahasa indonesia Abstrak dalam bahasa indonesia Abstrak dalam bahasa indonesia Abstrak dalam bahasa IndonesiaAbstrak dalam bahasa Indonesia Abstrak dalam bahasa Indonesia Abstrak dalam bahasa indonesia

**Kata kunci** :<<keyword 1>>, <<keyword 2>>, ....

# KATA PENGANTAR

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborumLorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum

# DAFTAR ISI

HALAMAN SAMPUL [romawi]

HALAMAN JUDUL [romawi]

HALAMAN PERSETUJUAN DOSEN PEMBIMBING [romawi]

HALAMAN PERNYATAAN DOSEN PENGUJI [romawi]

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI [SKRIPSI | TUGAS AKHIR] [romawi]

ABSTRAK [romawi]

KATA PENGANTAR [romawi]

DAFTAR ISI [romawi]

DAFTAR TABEL [romawi]

DAFTAR GAMBAR [romawi]

DAFTAR LAMPIRAN [romawi]

BAB 1 PENDAHULUAN 11

1.1. Latar belakang 11

1.2. Rumusan masalah 12

1.3. Ruang lingkup 12

1.4. Tujuan dan Manfaat 12

1.5. Metode Penelitian 13

1.5.1 Metode Perancangan 14

1.6 Sistematika Penulisan 15

BAB 2 TINJAUAN PUSTAKA 17

2.1. Blockchain 17

2.2. Etherum 17

2.3. Web3.js Library 17

2.4. **Smart Contract** 17

2.5. **Miner** 18

REFERENSI [angka]

LAMPIRAN-LAMPIRAN (Termasuk Foto Kopi Surat Survei) [angka]

RIWAYAT HIDUP

# DAFTAR TABEL

Table x.x Nama Tabel [0-9]

Table x.x Nama Tabel [0-9]

Table x.x Nama Tabel [0-9]

Table x.x Nama Tabel [0-9]

Table x.x Nama Tabel [0-9]

Table x.x Nama Tabel [0-9]

***Catatan****:*

*Untuk memudahkan pembuatan daftar tabel, untuk setiap penamaan tabel dapat menggunakan insert caption (klik kanan table -> insert caption). Caption pada setiap tabel kemudian dapat digunakan untuk membuat daftar tabel (references -> insert table of figures)*

# DAFTAR GAMBAR

Gambar x.x Nama Gambar [0-9]

Gambar x.x Nama Gambar [0-9]

Gambar x.x Nama Gambar [0-9]

Gambar x.x Nama Gambar [0-9]

Gambar x.x Nama Gambar [0-9]

Gambar x.x Nama Gambar [0-9]

Gambar x.x Nama Gambar [0-9]

Gambar x.x Nama Gambar [0-9]

***Catatan****:*

*Untuk memudahkan pembuatan daftar gambar, untuk setiap penamaan gambar dapat menggunakan insert caption (klik kanan gambar -> insert caption). Caption pada setiap gambar kemudian dapat digunakan untuk membuat daftar gambar (references -> insert table of figures)*

# DAFTAR LAMPIRAN

Lampiran x Nama Lampiran L[0-9]

Lampiran x Nama Lampiran L[0-9]

Lampiran x Nama Lampiran L[0-9]

Lampiran x Nama Lampiran L[0-9]

Lampiran x Nama Lampiran L[0-9]

Lampiran x Nama Lampiran L[0-9]

Lampiran x Nama Lampiran L[0-9]

Lampiran x Nama Lampiran L[0-9]

## BAB 1

## PENDAHULUAN

* 1. **Latar belakang**

Belakangan ini, teknologi blockchain sangatlah populer. Ini dikarenakan banyak sekali berita-berita tentang Bitcoin yang beredar saat ini. Konsep dalam Bitcoin adalah untuk membuat transaksi finansial tanpa melalui perantara apapun (Nakamoto, 2018). Tetapi penggunaan blockchain bukan pada Bitcoin saja, salah satu blockchain paling populer lainnya adalah Ethereum.

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 kode oleh programmer ini, 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 sehinggah 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 hash 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. Yang pertama adalah berasal dari XXX. 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. Penelitian kedua berasal dari Y, yaitu menggabungkan sebuah atau beberapa variabel untuk memenuhi besar bytes32 yang telah dipesan oleh Ethereum. Adapula penelitian dari ZZZ yang mengatakan bahwa sebelum menulis kode pada Ethereum, diperlukan pemikiran yang sangat matang mengenai data apa yang akan disimpan pada jaringan Ethereum. Hal ini akan berpengaruh terhadap berapa banyak harga yang disebabkan jika menulis memori yang telah dipesan. Dapat dikatakan sebaiknya memilih tipe data apa yang akan digunakan oleh sebuah variabel, misalkan hanya membutuhkan tipe data angka yang kecil, maka hanya perlu memakai uint8 saja dibandingkan dengan uint256.

Dari penelitian-penelitian sebelumnya, 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. **Rumusan masalah**

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

1. Apakah banyaknya dimensi pada map di smart contract dapat menambah biaya transaksi pada Ethereum network?
2. Apakah dengan metode menggabungkan dimensi map dengan algoritma enkripsi keccak256 dapat meningkatkan efisiensi dari gas yang digunakan pada smart contract?
   1. **Ruang lingkup**

Agar pembahasan dan analisis dilakukan lebih terfokus dan terarah sesuai dengan tujuan, berikut ruang lingkup dalam penulisan ini adalah sebagai berikut:

1. Metode ini dapat digunakan untuk mengurangi biaya untuk berinteraksi dengan smart contract pada ethereum network
2. Untuk meningkatkan efisiensi dari memori dan gas pada smart contract.
3. Sistem yang di optimisasi bernama attestation system.
   1. **Tujuan dan Manfaat**

Tujuan

Adapun tujuan penelitian ini adalah sebagai berikut:

1. Untuk mengetahui apakah banyaknya dimensi mapping berpengaruh pada besarnya biaya transaksi pada smart contract.
2. Untuk mengetahui apakah dengan menggunakan keccak256 pada multiple dimensi mapping dapat mengurangi biaya transaksi pada smart contract.

Manfaat

Adapun manfaat penelitian ini adalah sebagai berikut:

1. Memahami perhitungan biaya transaksi pada Ethereum network.
2. Meningkatkan efisiensi dari gas dan memori pada smart contract.
   1. **Metode 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, kami memiliki 2 cara, yaitu dengan metode observasi dan riset melalui internet dan eksperimentasi dengan kode kami 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 kami 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 masing-masing smart contract menggunakan gas, dan kami 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 kami dapat memperoleh data seberapa banyak gas yang digunakan oleh masing-masing smart contract.

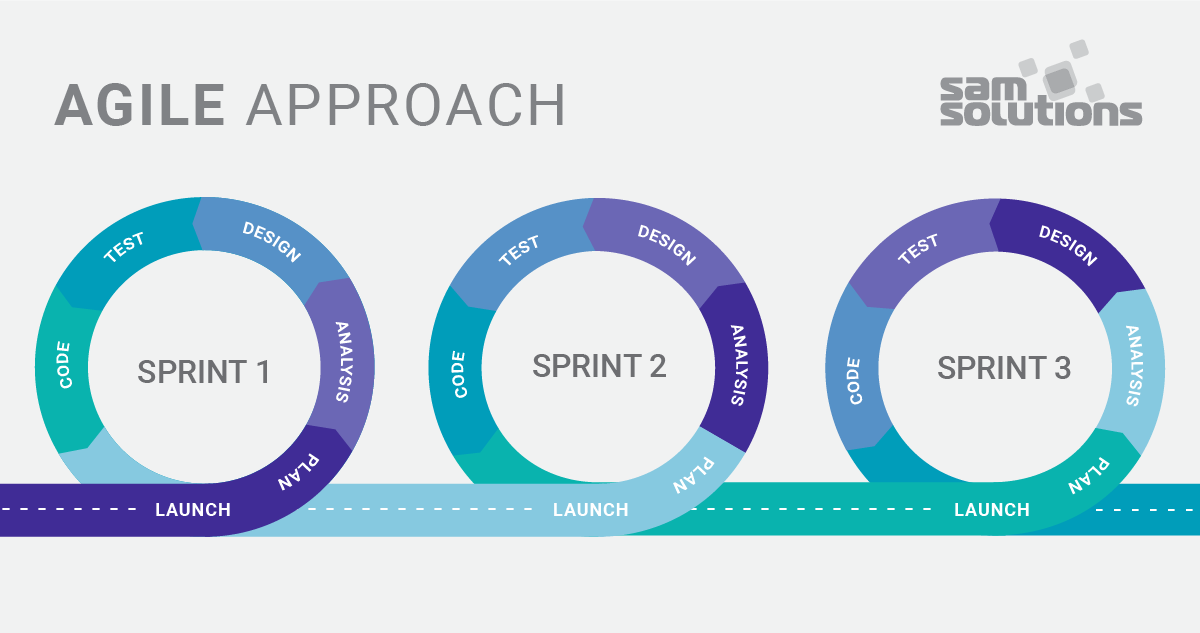
Dengan menggunakan smart contract yang sudah dioptimisasi, gas yang diperlukan untuk melakukan kalkulasi yang sama akan berkurang.

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

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

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 diambil dari [https://www.sam-solutions.com/blog/waterfall-vs-agile-a-comparison-of-software-development-methodologies/](https://www.sam-solutions.com/blog/waterfall-vs-agile-a-comparison-of-software-development-methodologies/" \t "_blank)*

* 1. **Sistematika penulisan**

BAB1 : PENDAHULUAN

Bab ini berisi mengenai gambaran umum tentang skripsi ini, contohnya adalah latar belakang, rumusan masalah, ruang lingkup, tujuan dan manfaat, metodologi, dan sistematika penulisan

BAB 2: TINJAUAN PUSTAKA

Bab ini bertujuan untuk menguraikan teori yang kami gunakan untuk mengoptimisasi sistem ini karena ada beberapa konsep yang harus dimengerti sebelum dapat mengoptimisasi sistem ini

BAB 3: DESKRIPSI UMUM

Bab ini bertujuan untuk menceritakan mengenai latar belakang perusahaan, kondisi saat ini, rumusan masalah, solusi, ruang lingkup serta peran kami masing-masing sebagai mahasiswa.

BAB4: HASIL DAN PEMBAHASAN

Bab ini bertujuan untuk menjelaskan hasil analisa, rancangan, implementasi, testing, dan evaluasi terhadap optimisasi sistem yang sudah dibuat.

BAB 5: SIMPULAN DAN SARAN

Bab ini bertujuan untuk menyampaikan simpulan yang kami dapat dan saran dari pihak HARA atas optimisasi sistem ini.

## BAB 2

## TINJAUAN PUSTAKA

**2.1. Blockchain**

Seperti namanya, blockchain adalah sebuah rantai yang terdistribusi yang terdiri dari ikatan antar blok. Sebuah blok mengandung beberapa properti seperti timestamp, nonce, kumpulan transaksi, dan parent blok.  Terdistribusi maksudnya adalah blockchain tidak hanya tersimpan oleh sebuah entitas saja, tetapi dimiliki oleh banyak pihak. Hal ini akan membuat proses verifikasi dari transaksi - transaksi di dalamnya lebih dapat dipercaya karena dimonitor oleh beberapa pihak. Untuk memastikan bahwa setiap pihak memiliki data yang sama, maka harus memiliki konsep konsensus atau kesepakatan yang sama.

**2.2. Ethereum**

Ethereum adalah open-source blockchain platform yang dapat dikembangkan oleh para programmer untuk membuat aplikasi yang bersifat decentralize. Pada tahun 2015, Ethereum resmi dirilis oleh Vitalik Buterin, anak jenius dari Rusia yang saat itu masih berumur 19 tahun. Saat ini, Ethereum adalah cryptocurrency yang memiliki nilai peringkat kedua tertinggi setelah Bitcoin. Hal ini bisa terjadi karena penggunaan Ethereum dapat dirasakan dan digunakan dikehidupan sehari-hari, sebagai contohnya alat pembayaran, biaya transaksi, biaya interaksi dengan smart contract, dan lain-lain.

**2.3. Web3.js Library**

Untuk mempermudah berinteraksi dengan ethereum network, maka diperlukan web3 sebagai kumpulan library javascript yang dapat mengkoneksikan user dengan blockchain.

**2.4. Smart Contract**

Definisi pasti dari smart contract sebenarnya belum ditetapkan (Kristian Lauslahti ). Pada studi ini, smart contract dapat didefinisikan sebagai program yang berada pada blockchain network, dan harus mengikuti beberapa peraturan yang ada di dalam blockchain. Dimana ketika sebuah kesepakatan maupun aksi terjadi, maka program tersebut akan berjalan. Beberapa smart contract memiliki konteks yang mirip dengan tradisional kontrak pada umumnya, misal harus mendapat tanda tangan untuk menunjukkan persetujuan mengenai hal yang terdapat pada kontrak, pada smart contract tanda tangan tersebut disebut sebagai digital signature.

**2.5. Miner**

Sebuah transaksi akan ditambahkan ke dalam blockchain jika telah terkonfirmasi oleh beberapa nodes yang disebut miner. Tugasnya adalah mengumpulkan beberapa transaksi yang belum terkonfirmasi, lalu melakukan komputasi yang telah ditetapkan oleh network agar dapat dimasukkan kedalam blockchain. Ketika komputasi telah selesai, maka kumpulan transaksi akan terkonfirmasi dan dimasukkan ke dalam blockchain. Miner juga harus memberitahu kepada miners lainnya tentang kumpulan transaksi yang telah terkonfirmasi agar mereka juga tahu bahwa ia telah menyelesaikan tugasnya. Imbalan dari aktivitas miners adalah dengan biaya transaksi yang ada pada transaksi-transaksi yang telah dikonfirmasi.

**2.6. Keccak256**

Keccak256 adalah algoritma enkripsi yang memiliki sifat one-way. Dimana hasil enkripsi tidak dapat didekripsi kembali ke nilai awal. Tetapi hasil dari enkripsi dapat dipastikan memiliki hasil yang sama jika nilai awalnya adalah sama persis. (Itai Dinur,, 2015)

**2.7. Solidity**

Bahasa pemrograman yang berfokuskan untuk membuat smart contract pada ethereum network. Platform bahasa ini beralaskan oleh bahasa typescript dan diperkuat oleh Ethereum Virtual Machine untuk menjalankannya. Solidity melakukan kompilasi kode lalu akan memperoleh bytekode yang dapat dijalankan di Ethereum Virtual Machine (EVM).

**2.8. Gas**

Untuk membayar biaya transaksi pada Ethereum network, diperlukan tarif yang harus dibayarkan oleh pengirim transaksi. Unit itu adalah gas, yaitu salah satu satuan pada Ethereum untuk mengukur penggunaan komputasi pada transaksi. Pengeluaran biaya transaksi tentu dapat diubah-ubah, sesuai kebutuhan transaksi, tetapi jika ternyata gas yang dibutuhkan ternyata lebih banyak dibandingkan yang disediakan, maka transaksi akan gagal dan tidak dapat diterima di dalam blockchain. Nilai 1 gas adalah equivalent dengan 0,000001 ETH.(Coinvestasi,2018).

**2.9. Penyimpanan Variabel pada Ethereum**

Ketika sebuah smart contract dideploy di Ethereum Network, mereka akan memesan memori-memori yang dibutuhkan oleh seluruh variabel yang akan dipakai oleh smart contract tersebut. Besar kecilnya memori ditentukan oleh tipe data apa yang digunakan. Semakin besar tipe datanya, maka akan semakin besar memori yang harus dipesan oleh Ethereum. Tetapi Ethereum akan selalu memesan memori sebesar bytes32 seberapa kecil apapun besar variabel yang akan digunakan. Hal ini dilakukan untuk memastikan bahwa seluruh memori memiliki standarisasi tersendiri sehingga lebih mudah untuk melakukan proses pencarian data. Sebagai contoh misalkan sebuah smart contract memiliki sebuah variabel boolean yang hanya mengembalikan nilai benar atau salah. Seharusnya variabel tersebut memiliki besar uint4, tetapi Ethereum akan memesan memori sebesar bytes32 untuk variabel tersebut. Setiap besaran memori yang dipesan oleh Ethereum memiliki harga masing-masing. Didasari hal inilah maka penulis mencoba untuk mengoptimasi penggunaan memori dan harga yang digunakan pada smart contract.

**2.10. Lokasi Deklarasi Variabel**

Pada penelitian XXX, penulis lebih menjurus kepada penempatan deklarasi lokasi variable. Hal tersebut didasari oleh sistem penyimpanan dari Ethereum sendiri, yaitu setiap bytes32 memori, ia akan menyimpan sebuah nilai. Walaupun nilai tersebut memiliki besar yang lebih kecil dibandingkan dengan bytes32, Ethereum akan tetap memesan memori sebesar bytes32. Didasarkan hal tersebut, maka letak atau susunan deklarasi variabel sangatlah penting. Pada penelitian dikatakan bahwa sangat penting untuk mengetahui setiap variabel memiliki besar berapa, sehingga kita sebagai programmer dapat mengoptimisasi penggunaan memori pada smart contractnya. Misalkan dengan meletakkan variabel-variabel, yang jika ditambahkan besar memorinya tidak melebihi bytes32, dekat satu sama lain. Jika menggunakan metode tersebut, maka tidak akan ada memori yang hilang atau disia-siakan. Sehingga seluruh memori yang dipesan dapat digunakan dengan sebaik-baiknya.

**2.11. Menggabungkan Beberapa Variabel pada Mapping**

Peneliti YYY membuktikan bahwa penggabungan variabel yang ditotal masih belum mengisi memori bytes32 dapat mengurangi memori yang digunakan pada smart contract. Hal ini didasari karena sistem penyimpanan variabel pada Ethereum yang selalu memesan bytes32 memori. Sehingga jika kita menggabungkan beberapa variabel menjadi sebuah bytes32 memori, maka akan menambah efisiensi memori pada smart contract.

## BAB 3

## DESKRIPSI UMUM

**3.1. Latar belakang perusahaan**

Talk about hara/dattabot. Here’s something we can talk about

HARA adalah perusahaan startup yang berfokus di bidang agrikultur berbasis blockchain di Indonesia. Sebelumnya, HARA berada di bawah PT. Mediatrac Sistem Komunikasi atau biasa disebut Dattabot. PT. Mediatrac Sistem Komunikasi sendiri beralih nama menjadi PT. Agri Tekno Karya pada tahun ini. Dattabot sendiri merupakan perusahaan konsultan yang menggunakan Big Data Analytics untuk optimasi supply- chain, digitalisasi dokumen, analisa text dan Analisa marketing. Dengan teknologi blockchain, HARA bertujuan untuk mengedepankan transparansi pada supply-chain pangan dan pertanian, pemberi pinjaman mikro dari institusi finansial kepada mitra petani di Indonesia. Data yang telah didapatkan dari petani akan diperjualbelikan kepada orang yang memerlukan data dari segi agrikultur. Dari penjualan data, para petani sebagai penyedia data akan memperoleh insentif atas datanya.

Jasa dan produk yang ditawarkan HARA dapat dibagi menjadi dua buah kategori besar yaitu HARA Agrikultur untuk mengumpulkan dan mendistribusikan data agrikultur, serta HARA Ledger, sebuah blockchain enterprise solutions bagi perusahaan yang ingin menerapkan teknologi blockchain (Blockchain-as-a-Service). Berikut adalah rincian produk yang ditawarkan oleh HARA :

* + HARA Ledger : Sebuah private blockchain untuk mencatat berbagai aktivitas yang dibutuhkan.
  + HARA Token (HART) : Mata uang yang akan digunakan diseluruh infrastruktur HARA Ledger
  + HARA Data Exchange (HDX) : Platform jual beli data para petani kepada para pembeli data. Semua aktivitas yang berjalan di HDX tercatat didalam HARA Ledger dengan bantuan smart contract.
  + HARA Wallet : Dompet virtual untuk menyimpan asset cryptocurrency baik HART, maupun token lainnya. Dapat diunduh di dalam smartphone.
  + HARA Scan : Sebuah website untuk memonitoring seluruh aktivitas yang terjadi di HARA Ledger sehingga lebih mudah dibaca dan dipahami.

Di Indonesia, perusahaan yang bergerak pada bidang pertanian sudah mulai bermunculan, tetapi mereka lebih banyak berfokus pada penjualan hasil pertanian dari produser langsung ke konsumen tanpa ada perantara. Saat ini belum banyak perusahaan yang bergerak pada bidang penjualan data agrikultur. Adapun skema insentif untuk para penyedia data yang didukung oleh teknologi blockchain. Dapat dikatakan HARA merupakan salah satu pioneer dari sisi pelayanan menggunakan blockchain di Indonesia.

HARA juga menjadi data provider untuk sektor pertanian. Artinya HARA mengajak para petani-petani yang berada di Bojonegoro untuk memberikan data-data yang mereka miliki, seperti contohnya tanggal menanam padi, produksi hasil pertanian, lamanya menanam, berapa biaya yang dibutuhkan untuk menanam dalam satu penanaman, dan juga luas lahan yang dimiliki oleh mereka atau lahan yang mereka miliki. Untuk memudahkan pengumpulan data lahan, teknologi satelite digunakan dalam program internal. Para petani yang ingin menunjukkan lahannya harus mendownload aplikasi lalu menjelajahi keliling dari pertanian atau lahan yang mereka miliki. Dari data tersebut dapat dihitung jumlah luas lahan, keliling, lokasi dan lain sebagainya. Imbalan untuk data - data yang HARA dapatkan, para petani akan memperoleh insentif dalam bentuk stampel. Jika sudah memenuhi beberapa kriteria, stampel tersebut akan dapat ditukarkan menjadi beberapa produk jadi yang siap pakai seperti contohnya sembako. Di Bojonegoro dan Surabaya terdapat beberapa kantor yang siap melayani para petani yang ingin menukarkan stampel tersebut.

Adapula bisnis HARA Loan, yaitu pelayanan pemberian pinjaman uang kepada para petani dengan bunga yang cukup rendah. Pada zaman ini, banyak petani yang sengsara karena jika mereka gagal panen dan ingin menabung lagi, mereka tidak memiliki uang yang cukup untuk mulai menanam. Sekarang solusi paling mudah adalah dengan meminjam kepada tengkulak yang memiliki kecenderungan memberikan bunga yang sangat tinggi sehingga biasanya mereka terjerat hutang yang susah untuk dilunasi. Oleh karena itu HARA menyediakan sistem peminjaman yang akan membantu para petani kecil yang ingin tetap bertani tetapi tidak ingin meminjam kepada tungkulak. Untuk proyek ini HARA bekerja sama dengan bank BNI & BTPN Syariah sebagai penyedia keuangan yang kemudian akan disalurkan kepada para petani yang ingin meminjam.

**3.2. Kondisi saat ini**

Pada perusahaan HARA, terdapat sebuah sistem attestation dimana para petani dapat memberi ulasan pada sebuah data. Apabila data tersebut berkualitas tinggi maka para petani akan memberikan ulasan yang baik. Apabila data tersebut berkualitas rendah, maka para petani akan memberikan ulasan yang tidak baik. Code dari ulasan ini ditulis di solidity untuk menggunakan ethereum smart contract. Pada smart contract, setiap operasi dan penyimpanan akan dihitung harganya. Pada smart contract attestation ini, ada beberapa data yang disimpan dan ini sangatlah tidak efisien karena biaya yang dikeluarkan menjadi beberapa kali lipat dibandingkan apa yang perlu dikeluarkan.

**3.3. Identifikasi masalah**

Pada sistem attestation di hara yang menggunakan bahasa Solidity, ada beberapa masalah yang ditemukan:

* Smart contract tersebut menggunakan penyimpanan yang banyak
* Karena penyimpanan yang banyak, maka smart contract tersebut akan menggunakan biaya yang lebih dari yang harusnya dikeluarkan.

**3.4. Solusi yang diusulkan**

Solusi yang diusulkan oleh penulis adalah optimisasi sistem yang bertujuan untuk mempercepat dan menghemat penyimpanan sehingga biaya yang dikeluarkan untuk melakukan attestation menjadi lebih murah. Penulis menggunakan teknik enkripsi keccak256 untuk mengecilkan penyimpanan di ethereum network. Ini dilakukan dengan membuat parameter dalam bentuk string dan dimasukkan kedalam fungsi enkripsi keccak yang sudah tersedia di ethereum.

**3.5. Ruang lingkup aplikasi**

Agar pembahasan dan analisis dilakukan lebih terfokus dan terarah sesuai dengan tujuan, berikut ruang lingkup dalam penulisan ini adalah sebagai berikut:

1. Metode ini dapat digunakan untuk mengurangi biaya untuk berinteraksi dengan smart contract pada ethereum network
2. Untuk meningkatkan efisiensi dari memori dan gas pada smart contract
3. Sistem yang di optimisasi bernama attestation system.

**3.6. Peran**

Peran Jonas dalam perusahaan dattabot adalah sebagai intern 3+1 dari Binus University. Jenis pekerjaan yang dilakukan oleh Jonas adalah sebagai berikut:

* Membuat optimisasi sistem pada sistem HARA.
* Membuat aplikasi blockchain pada perusahaan HARA.
* Membuat front end dalam perusahaan HARA.
* Memperlajari ethereum dan blockchain.

Vincent adalah seorang mahasiswa yang mengambil track entrepreneur pada 3+1 dari Binus university. Jenis pekerjaan yang dilakukan oleh Vincent adalah sebagai berikut:

* Mempelajari ethereum dan blockchain.
* Memahami optimisasi dan memahami berapa banyak keuntungan yang dihasilkan dari optimisasi ini
* Memvisualisasikan hasil reduced cost dari hasil optimisasi sistem ini.
* Mempelajari segi bisnis dari reduced cost pada sistem ini.

## BAB 4

## HASIL DAN PEMBAHASAN

**4.1. Analisa kebutuhan sistem**

In this part, talk about how Jonas’ supervisor/atasan needs this optimization on the system. Add something like “berdasarkan wawancara kami” or sometihng like that. Talk about the problem in the company and how this optimization is needed (basically price optimization, and who doesn’t want that?)

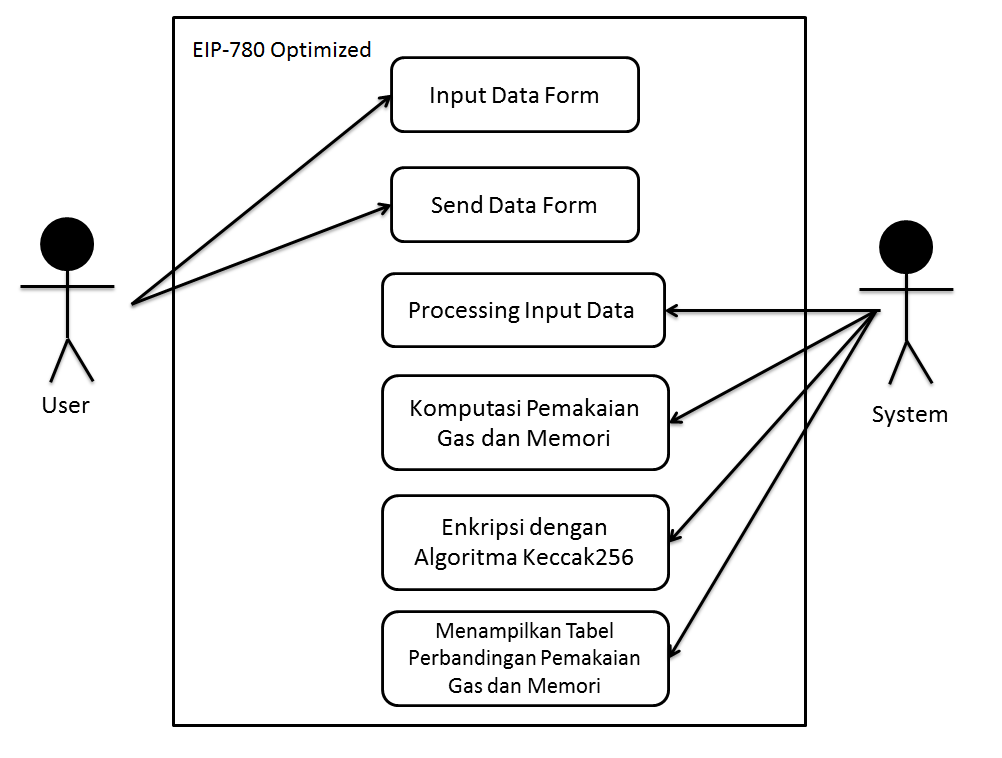
**4.2. Kerangka metodologi**

Pada proses optimisasi sistem ini, penulis menggunakan metodologi agile. Metodologi ini bertujuan untuk mempercepat pembuatan aplikasi atau sistem, tidak seperti metodologi yang sudah ada sebelumnya. Berikut adalah langkah-langkah dalam mengaplikasikan metodologi ini.

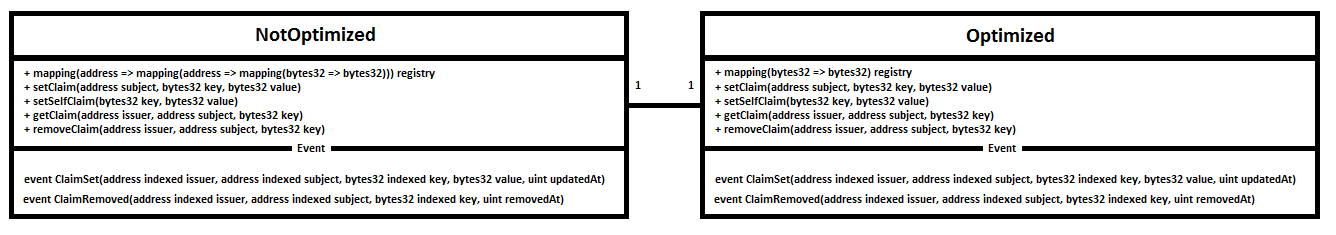
1. plan: pada tahap ini, sistem yang akan di optimisasi akan di pertimbangkan dahulu bersama tim dan akan dirancangkan bagaimana caranya untuk mengoptimisasi sistem ini.
2. analisis: pada tahap ini, dilakukan analisis agar sistem yang dirancangkan dapat di optimisasi dengan baik. Jika tahap init idak ada maka sistem yang di optimisasi akan gagal.
3. design: pada tahap ini, sistem yang akan di optimisasi akan di rancang ulang sehingga lebih efisien. Desain yang dibuat nantinya akan digunakan sebagai kerangka dari sistem tersebut.
4. test: Pada tahap ini, dibuatlah dulu testnya agar sistem yang dirancangkan tidak gagal ketika kode sudah dibuat.
5. kode: pada akhirnya, kode akan dibuat untuk mengoptimisasi sistem. Ini adalah tahap akhir dari metodologi agile.

**4.3. Rancangan sistem**

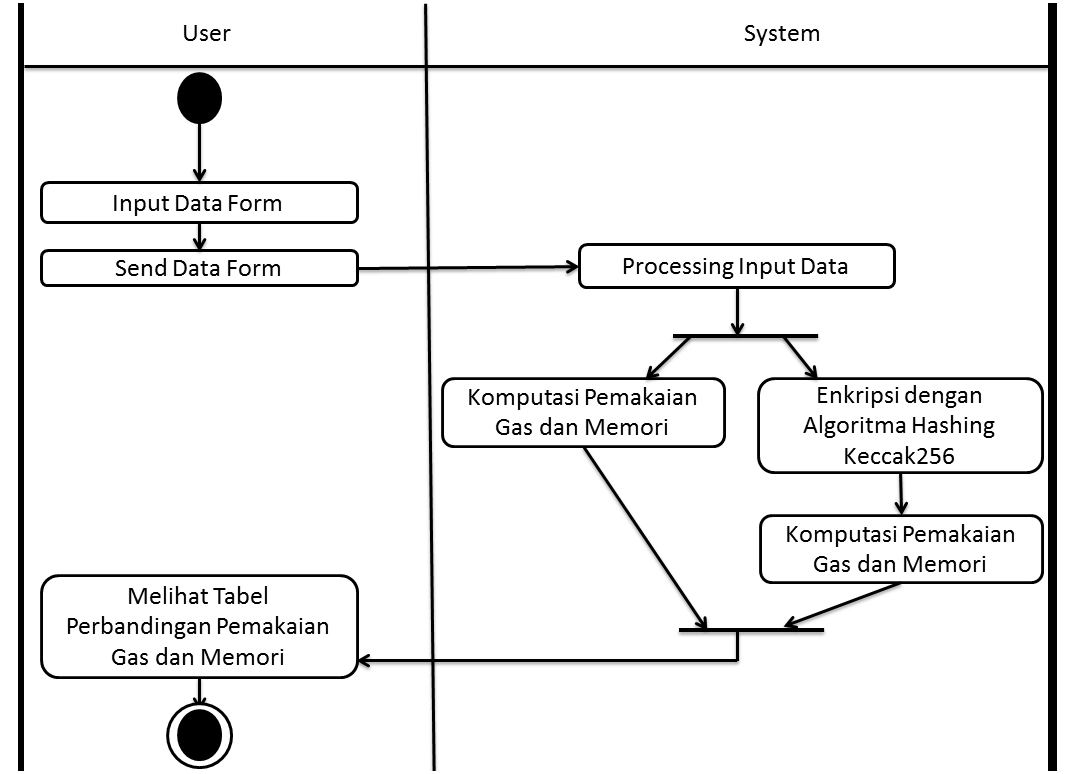
**4.3.1 Use Case Diagram**

****

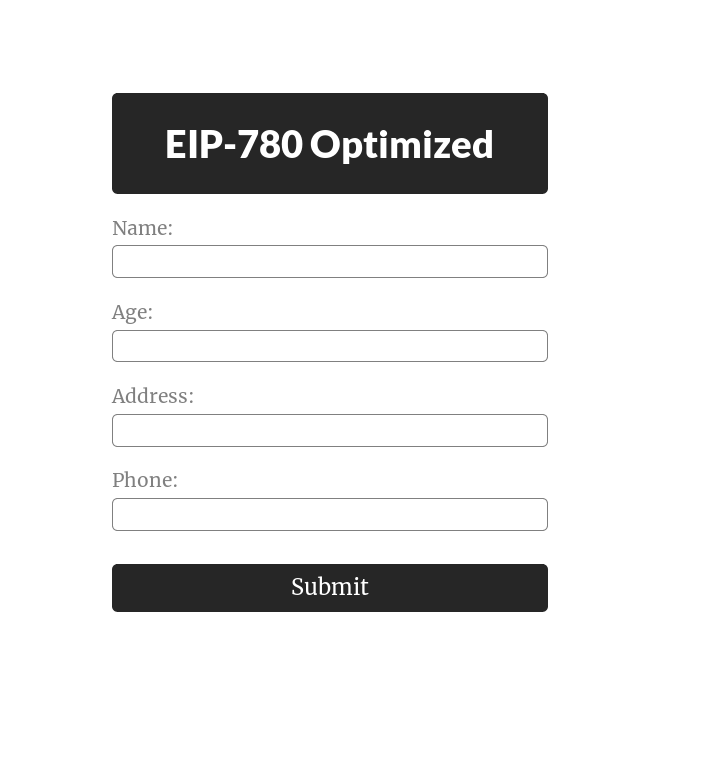
**4.3.2. Class Diagram**



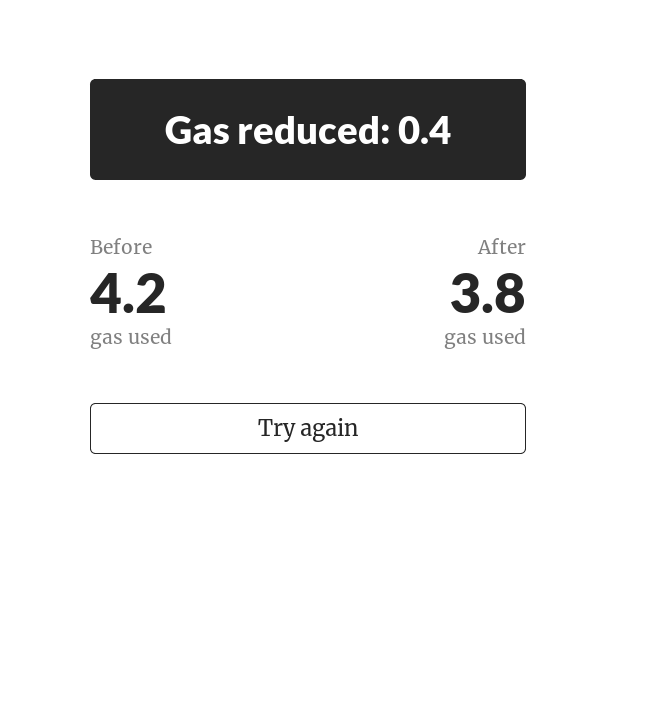
**4.3.3. Activity Diagram**



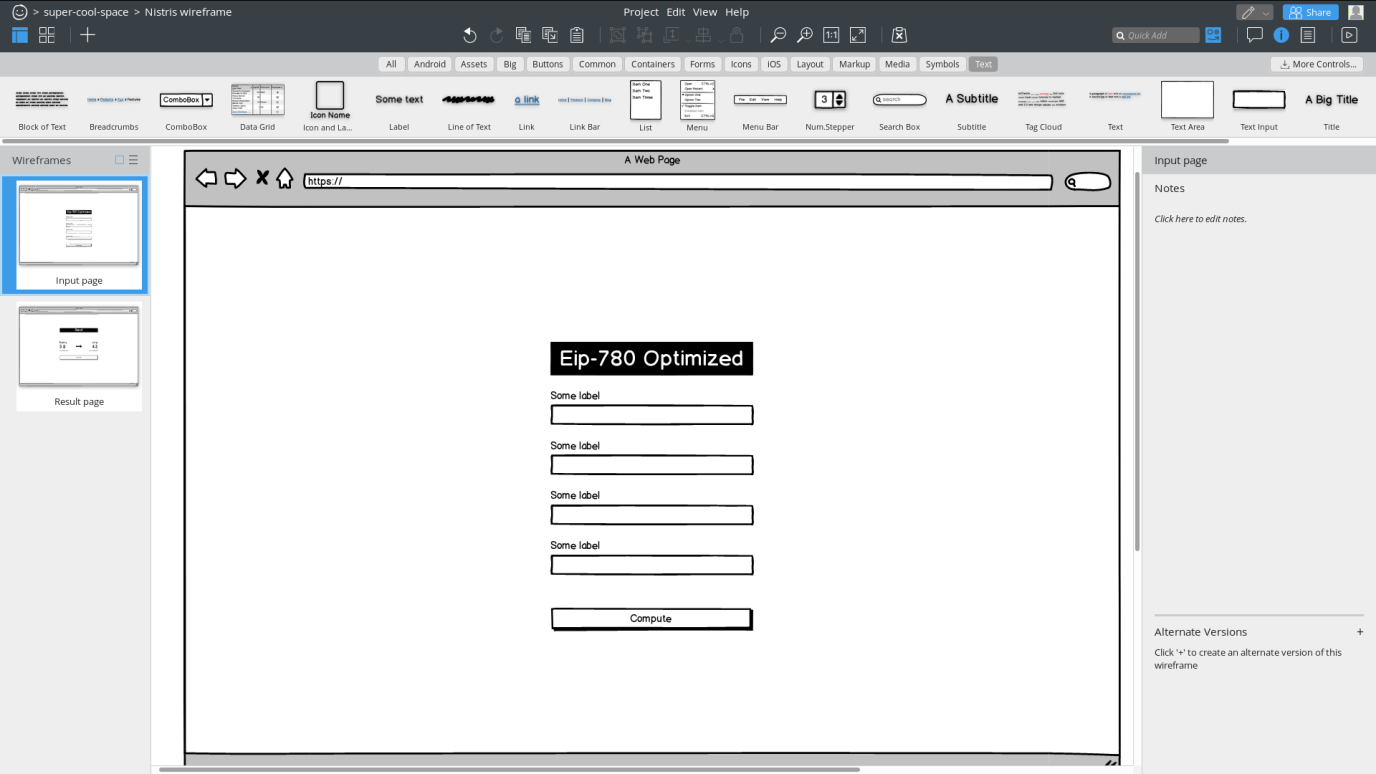
**4.4. Rancangan Layar**



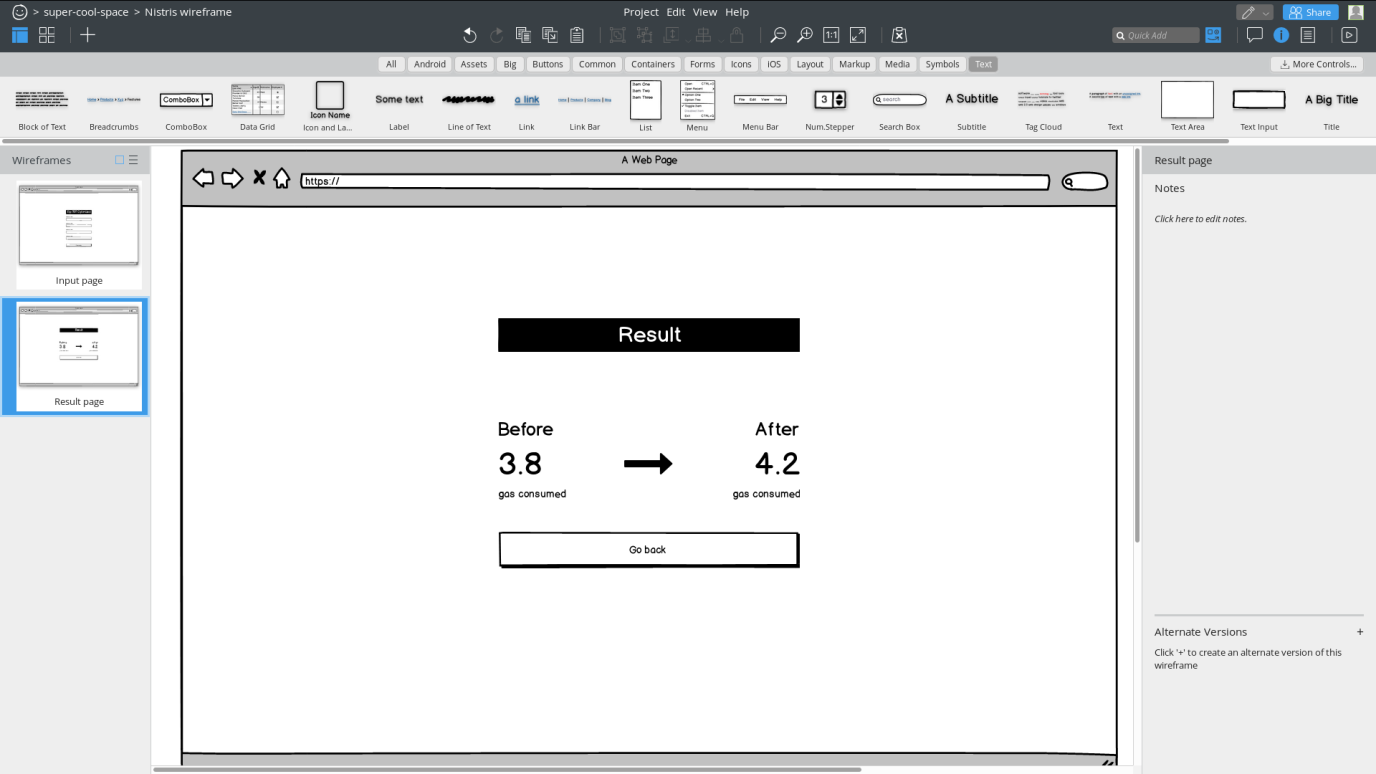
**Image Input**



**Image Result**



**Wireframe Input**



**Wireframe Result**

**4.5. Implementasi**

Pada sistem yang lama, untuk menjalankan suatu fungsi smart contract, maka ada beberapa parameter yang di passing agar smart contract itu dapat berfungsi dengan baik. Optimisasi yang dilakukan oleh penulis adalah membuat parameter tersebut menjadi satu saja, sehingga cost yang diperlukan untuk menjalankan smart contract tersebut lebih kecil. Ini dikarenakan setiap parameter dan variabel yang digunakan di ethereum akan memakan biaya dan apabila fungsi smart contract tersebut di optimisasi, maka sistem tersebut memerlukan lebih sedikit biaya untuk di jalankan. Berikut adalah perbedaan kode yang sebelum dan sesudah di optimisasi.

put some screenshot of the "app" here, put git diff for the commit that optimized the stuff. \*\*

**4.6. Testing**

Untuk memastikan apakah sebuah sistem berjalan dengan baik, maka diperlukan untuk melakukan testing. Pada sistem ini, alat testing yang digunakan adalah remix. Remix adalah sebuah kode editor ethereum yang ada di browser yang bisa digunakan untuk mentesting kode solidity. Remix sangatlah sering digunakan karena untuk mentesting menggunakan ethereum utama, maka perlu memakan biaya untuk menjalankan sebuah fungsi. Tetapi pada remix akan diberikan ether gratis untuk testing sebuah kode. Berikut adalah bukti bahwa kode yang sudah di optimisasi mempunyai cost yang lebih kecil.

@@ -192,6 +197,8 @@ Screenshot remix on ether reduction on before and after the optimization.

**4.7. Evaluasi**

How does the poeple at hara (the pros) think about the system that you made? Write sometihng like “menurut x, sistem yang sudah di optimisasi sangatlah bagus karena a, b, c.”

## BAB 5

## SIMPULAN DAN SARAN

**5.1. Simpulan**

Ethereum adalah sebuah platform smart contract dimana develop dapat menulis kode dan menjalankan kode tersebut. Akan tetapi, setiap variabel, penyimpanan dan operasi akan memakan biaya. kami sadar akan pentingnya mengoptimisasi kode di solidity karena jika kode di optimisasi maka akan memakan lebih sedikit biaya dengan fungsionalitas yang sama. Dengan optimisasi kode ini, maka jumlah biaya yang dikeluarkan untuk setiap kali memanggil smart contract ini akan berkurang, dan ini artinya berkurangnya biaya yang harus dibayar oleh pihak HARA, dan ini adalah hal yang baik. Apabila sistem ini tidak di optimisasi, maka biaya tidak akan menurun dan apabila banyak orang yang menggunakan smart contract tersebut, maka biaya akan menjadi sangat besar yang harus ditanggung oleh HARA.

Pada skripsi ini, masalah yang kami selesaikan adalah "apakah banyaknya dimensi pada map di smart contract dapat menambah biaya transaksi pada Ethereum network?" dan "apakah dengan metode menggabungkan dimensi map dengan algoritma enkripsi keccak256 dapat meningkatkan efisiensi dari gas yang digunakan pada smart contract?" Jawaban untuk pertanyaan pertama adalah ya, jika semakin banyak dimensi pada map di smart contract, maka biaya transaksi akan naik. Jawaban untuk pertanyaan kedua adalah ya, dengan menggabungkan map tersebut dengan Keccak256 maka biaya transaksi akan menurun.

`Untuk kedepannya, metode keccak ini untuk mengecilkan biaya gas pada ethereum network akan banyak sekali kegunaannya. Karena smart contract ini bersifat terbuka, maka smart contract ini dapat digunakan oleh siapapun. Oleh karena itu, banyak sekali kegunaan dari smart contract ini untuk menurunkan biaya pada smart contract, terutama apabila smart contract tersebut sering dipanggil. Contoh aplikasi atau sistem yang dapat memperoleh keuntungan menurunkan cost dari smart contract ini adalah di bidang kesehatan dan sosial.

**5.2. Saran**

What do people think of this optimized system? (“dari hasil wawancara kami, x mengatakan y”)

## Lampiran

Put lampiran wawancara here (in the form of text).

## Daftar pustaka

Nakamoto, S. (2008). Bitcoin: A peer-to-per electronic cash system. Diambil dari <https://bitcoin.org/bitcoin.pdf>

Chen Ting,  et al., (2017). Under-Optimized Smart Contract Devour Your Money.

Itai D,. (2015). Security Evaluation of SHA-3.

Kristian Lauslahti et al., (2017). Smart Contracts – How will Blockchain Technology Affect Contractual Practices?

Team Coinvestasi. (2018, February 2). Apa yang Dimaksud Gas Dalam Blockchain Ethereum. Diambil dari <https://coinvestasi.com/belajar/apa-yang-dimaksud-gas-dalam-blockchain-ethereum/>