Implementasi Blockchain dalam Pengembangan *Whistleblowing System*

Alifia Rahmah - 13520122
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: 13520122@std.stei.itb.ac.id

Tindakan-tindakan nirintegritas dan nirmoral seperti korupsi dan pungutan liar adalah permasalahan yang kerap terjadi di instansi Indonesia. Oleh karena itu, perlu adanya sistem pengaduan yang juga menjaga anonimitas pelapor agar tidak mudah dilacak pelaku, atau biasa dikenal dengan istilah *whistleblowing*. Teknologi *blockchain* yang menjaga aspek *integrity* dan *non-repudiation* dari setiap transaksi di dalamnya menjadi salah satu solusi dari permasalahan ini. Oleh karena itu, dikembangkan sebuah sistem *whistleblowing* berupa aplikasi web yang menggunakan implementasi *blockchain* sederhana sebagai basis data dari daftar laporan pengaduan yang ditulis oleh pelapor. Pengujian menunjukkan aplikasi dapat menjalankan fungsi membuat laporan dan menampilkan daftar laporan sesuai yang diharapkan.

Kata kunci—whistleblowing, blockchain, web application

I. PENDAHULUAN

Integritas petugas pemerintah merupakan masalah yang kerap kali terjadi di berbagai negara, termasuk Indonesia. Tindakan-tindakan nirintegritas seperti korupsi, pungutan liar, suap, dan gratifikasi sering terjadi, baik pada instansi pemerintah ataupun swasta. Menurut Indonesian Corruption Watch (ICW), terdapat 798 kasus korupsi di Indonesia pada tahun 2023, yang menyebabkan potensi kerugian negara hingga mencapai Rp28,4 triliun.

Pencegahan dan tindak lanjut dari perilaku korupsi perlu dilakukan dan diimplementasikan di Indonesia. Salah satu solusi dari permasalahan ini adalah dengan mengembangkan sistem pengaduan tindakan. Untuk menjaga keamanan pelapor, sistem harus dapat melindungi identitas pelapor, sehingga sistem dapat dikembangkan secara anonim.

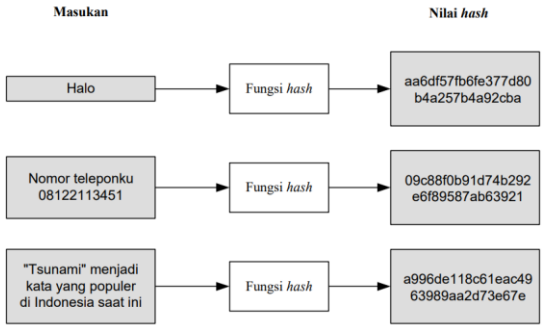
Sistem *whistleblowing* yang ada pada saat ini memiliki kelemahan sebagaimana kelemahan *website* pada umumnya, yaitu permasalahan menjaga aspek *integrity* pada basis data. Padahal, untuk membangun sistem whistleblower, diperlukan penjagaan integritas dari daftar laporan agar laporan tidak mudah dimodifikasi bahkan dihapus.

Teknologi *blockchain*, yang menggunakan untuk menjaga *integrity* dan *non-repudiation*, seringkali menjadi solusi untuk bidang yang membutuhkan integritas data dan kejujuran yang tinggi. Oleh karena itu, dikembangkan sistem *whistleblowing* berupa aplikasi web yang menggunakan teknologi *blockchain* sebagai basis data dari laporan yang masuk.

II. DASAR TEORI

A. *Fungsi Hash*

Fungsi *hash* adalah sebuah fungsi yang mengkompresi pesan berukuran sembarang menjadi string dengan ukuran tetap tanpa menggunakan kunci. Keluaran dari fungsi *hash* biasa disebut pesan ringkas (*message digest*) atau nilai *hash* (*hash value*). Fungsi *hash* bersifat *satu* arah, sehingga keluaran dari fungsi *hash* tidak dapat dikembalikan menjadi masukan semula.



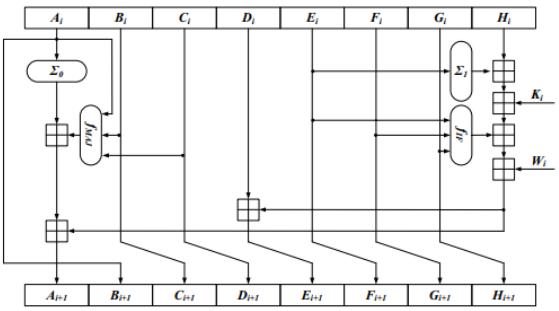
Gambar II.1. Ilustrasi fungsi *hash*
(sumber: Bahan Kuliah IF4020 Kriptografi)

Fungsi *hash* memiliki beberapa sifat, di antaranya:

- *Collision resistance*
  Sifat ini memiliki arti sangat sukar untuk menemukan dua masukan a dan b sehingga hasil fungsi H(a) memiliki nilai yang sama dengan hasil fungsi H(b).
- *Preimage resistance*
  Sifat ini memiliki arti untuk sembarang nilai, sangat sukar untuk menemukan masukan dari fungsi *hash* dengan keluaran nilai tersebut.
- *Second preimage resistance*
  Sifat ini memiliki arti untuk input a dan output y = H(a), sangat sukar menemukan input b sedemikian rupa sehingga nilai H(b) = y.

B. Secure Hash Algorithm 256-bit (SHA-256)

Algoritma Secure Hash Algorithm 256-bit (SHA-256) merupakan jenis spesifik dari keluarga SHA-2 dengan panjang nilai *hash* 256 bit. Algoritma ini melakukan



Gambar II.2. Garis besar cara kerja algoritma SHA-2

C. Blockchain

Blockchain adalah sebuah basis data berupa buku besar (*legder*) yang terdesentralisasi dan dikelola secara kolektif oleh peserta dari *blockchain* tersebut. Karena terdesentralisasi, *blockchain* tidak memiliki satu *server* khusus yang memiliki akses penuh terhadap keseluruhan data.

Pada *blockchain*, setiap transaksi dicatat dalam *ledger* menggunakan arsitektur *peer-to-peer*, sehingga Setiap *peer* memiliki catatan blok yang sama. Setiap data *transaski direpresentasikan* sebagai sebuah blok yang terhubung satu sama lain dalam suatu rantai struktur data *linked list*. Dalam setiap blok, terdapat pointer nilai *hash* yang merujuk ke blok sebelumnya. Karena diperlukan nilai *hash* dari blok sebelumnya, jika ada yang memaksa melakukan perubahan pada suatu blok, maka nilai *hash* dari blok tersebut akan berubah dan hubungan antar blok menjadi terputus. Selain itu, karena masing-masing *peer* memiliki catatan yang sama, perubahan pada satu catatan menjadi mudah dilacak dan ditolak. Hal ini yang menjadikan sistem *blockchain* dapat menjamin aspek *integrity* dan *non-repudiation*.

Untuk memutuskan apakah sebuah blok dapat ditambahkan di dalam jaringan *blockchain*, diperlukan metode persetujuan untuk menyepakati *peer* mana yang dapat menambahkan blok, yang biasa disebut konsensus. Terdapat beberapa metode konsensus di dalam *blockchain*, salah satunya proof of work, yang menggunakan sejenis *puzzle*.

-

D. Integrity dan Non-Repudiation

Integritas (*integrity*) dan antipenyangkalan (*non-repudiation*) adalah dua dari tujuh aspek keamanan informasi. Konsep integritas memiliki arti keutuhan isi dari keseluruhan data. Data tidak boleh dapat diubah atau dihapus, baik saat dilakukan transmisi maupun dalam penyimpanan.

Konsep antipenyangkalan memiliki arti pengirim data tidak dapat mengelak bahwa data tersebut memang dikirim oleh dia. Dalam kata lain, antipenyangkalan menjamin bahwa terdapat bukti yang cukup kuat, sehingga seseorang yang ingin mengirim data tidak dapat mengelak bahwa memang dia yang mengirim data tersebut.

E. Tindakan Korupsi

Menurut Kamus Besar Bahasa Indonesia (KBBI), korupsi adalah tindakan penyelewengan atau penyalahgunaan uang negara (*perusahaan*, organisasi, yayasan, dan sebagainya) untuk keuntungan pribadi atau orang lain.

F. Sistem Whistleblowing

Menurut Merriam-Webster, *Whistleblowing* adalah kegiatan melaporkan tindakan sebuah pihak, terutama tindakan yang dianggap ilegal, tanpa orang yang dilaporkan mengetahuinya. Istilah *whistleblowing* berasal dari istilah untuk aparat penegak hukum pada abad ke-19 yang menggunakan peluit untuk mengingatkan masyarakat. Wasit olahraga juga biasa menggunakan peluit ketika terjadi pelanggaran dalam permainan olahraga. Istilah untuk pelapor. Pelapor disebut *whistleblower*.

III. DESAIN DAN IMPLEMENTASI

A. Analisis Kebutuhan

Garis besar dari program ini adalah mengembangkan sebuah aplikasi web dengan *blockchain network*. Struktur kontrak dari *blockchain* network ini disesuaikan dengan sistem *whistleblowing* untuk menampilkan data yang diperlukan dalam proses pengaduan. Dalam laporan tindakan institusi, setidaknya diperlukan informasi sebagai berikut:

1. Nama terlapor
   Berupa nama lengkap dari terlapor.
2. Departemen/divisi terlapor
   Berupa pilihan departemen ataupun divisi dari pihak yang sedang dilaporkan
3. Kategori tindakan
   Berupa pilihan kategori dugaan tindakan yang dilakukan. Bisa berupa pungutan liar, penyuapan, maupun gratifikasi.
4. Deskripsi lengkap tindakan
   Berupa deskripsi lengkap dugaan tindakan yang dilakukan.
5. Lokasi kejadian
   Berupa lokasi dari kejadian.
6. Waktu kejadian
   Berupa waktu atau perkiraan waktu dari kejadian. Waktu dibuat sebagai atribut opsional (tidak harus ada) dan terpisah dari *timestamp* penambahan laporan karena bisa saja pelapor tidak melaporkan kejadian secara langsung.
7. Bukti
   Bukti berupa pranala gambar, rekaman, dokumen, ataupun berkas lain yang dapat bertindak sebagai bukti dari kejadian tersebut. Dalam satu laporan, bisa terdapat lebih dari satu bukti yang dilampirkan.

Enam informasi tersebut kemudian dibangun menjadi struktur data dasar dari laporan sebagai berikut.

```
export interface Report {
  index: number;
  suspect_name: string;
  dept: string;
  action_category: string;
  description: string;
  location: string;
  time_of_occurence: string;
  evidence: string[];
}
```

B. *Struktur Data*

Untuk membangun kontrak dari daftar laporan, dibentuk kelas Report. Kelas Report menyimpan atribut dan metode yang digunakan untuk operasi *blockchain*, di antaranya:

1. Atribut chain
   Implementasi sederhana dari *blockchain* berupa larik objek yang mencakup indeks, timestamp, *hash* dari blok sebelumnya, *proof of work*, dan struktur data laporan.
2. Metode create_block()
   Metode yang digunakan untuk menambahkan blok baru di dalam atribut chain.
3. Metode proof_of_work()
   Metode yang digunakan untuk melakukan validasi untuk menambah transaksi dalam *blockchain*.
4. Metode hash()
   Metode yang digunakan untuk menghitung nilai *hash* dari suatu blok. Metode ini menggunakan algoritma SHA-256 untuk melakukan perhitungan nilai *hash*.
5. Metode chain_valid()
   Metode yang digunakan untuk melakukan validasi pada atribut *chain*. Metode ini melakukan komputasi hash pada masing-masing blok di dalam *chain* dan mengembalikan nilai True jika nilai *hash* yang telah dihitung sama dengan nilai *hash* pada blok sebelumnya

C. *Rancangan Program*

Sebagai aplikasi web, *whistleblower system* ini memiliki dua bagian, yaitu back-end dan front-end.

1. Back-end
   Bagian back-end terdiri dari beberapa rute API. Rute API yang diimplementasikan di antaranya:
   - /reports
     Rute untuk menampilkan daftar report.
   - /create_report
     Rute untuk melakukan pembuatan blok baru. Rute ini memanggil metode create_block() pada Report.
   - /valid
     Rute untuk melakukan validasi *blockchain*. Rute ini memanggil metode chain_valid pada Report.
2. Front-end
   Bagian front-end terdiri dari dua halaman utama sebagai berikut:
   - Report list
     Berisi tabel daftar report, yang diintegrasikan dengan rute API /reports. Terdapat juga tombol untuk mengisi form report.
   - Create Report
     Berisi form untuk mengisi data pengaduan. Data yang telah diisi kemudian akan diintegrasikan dengan rute API /create_report untuk menambah blok baru.

IV. PENGUJIAN

Untuk memastikan aplikasi dapat berjalan dengan baik, dilakukan pengujian untuk menguji fungsionalitas blockchain dan back-end pada program. Pengujian fungsionalitas *blockchain* dilakukan menggunakan *unit testing*, sedangkan pengujian *back-end* dilakukan secara manual.

A. *Pengujian fungsionalitas blockchain*

Pengujian dilakukan menggunakan kakas unittest pada Python. Kasus yang diuji di antaranya:

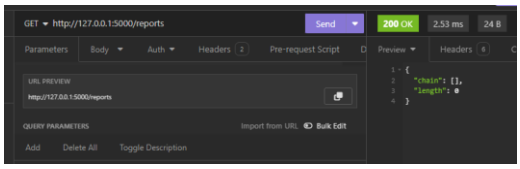
- Uji penambahan blok
- Uji validasi keseluruhan blok ketika terjadi perubahan pada nilai pada salah satu blok.

Gambar IV.1. Hasil pengujian fungsionalitas blockchain

Hasil unit testing fungsionalitas *blockchain* menunjukkan fungsi penambahan blok dan validasi ketika terjadi perubahan nilai pada salah satu blok berjalan dengan baik.

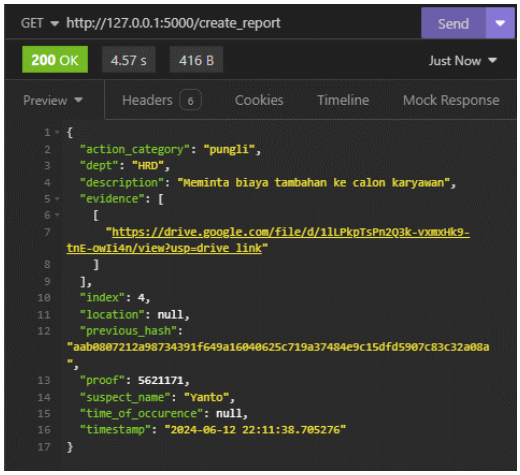
B. *Pengujian back-end*

Pengujian *back-end* dilakukan secara manual dengan menjalankan API *request* pada Insomnia API client. Pengujian pertama dilakukan dengan melakukan *request* ke rute /reports untuk memastikan kosong, melakukan *request* ke rute /create_report untuk membuat blok baru, memanggil kembali rute /reports untuk memastikan hasil laporan dapat ditampilkan, dan /valid untuk memastikan laporan yang telah masuk konsisten.



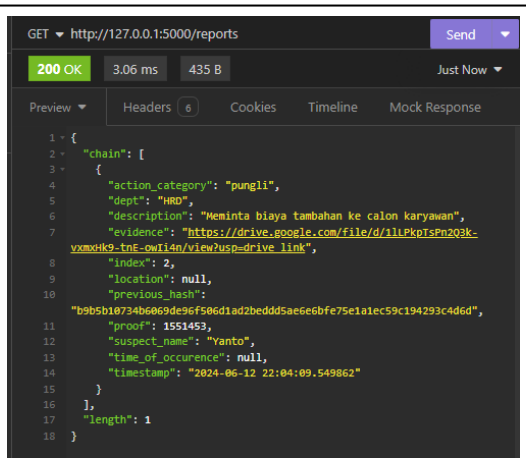
Gambar IV.2. Hasil request /reports

Hasil *request* pada /reports menunjukkan aplikasi yang belum dimasukkan laporan hanya akan mengeluarkan larik kosong, walupun sebenarnya terdapat *initialization block* di dalam *blockchain*. Hasil *request* tersebut juga mengembalikan status 200 yang berarti rute API sukses dijalankan.



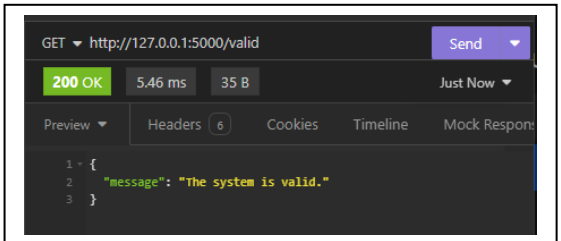
Gambar IV.3. Hasil request /create_report

Hasil *request* pada /create_report akan mengembalikan nilai dari blok yang telah dibuat. Hasil tersebut juga mengembalikan status 200 yang berarti rute API sukses dijalankan.



Gambar IV.4. Hasil request /reports setelah penambahan blok baru

Hasil *request* pada /reports setelah membuat blok baru menunjukkan daftar blok yang telah dibuat sebelumnya. Hasil tersebut juga mengembalikan status 200 yang berarti rute API sukses dijalankan.



Gambar IV.5. Hasil *request* /valid

Hasil *request* pada /valid mengembalikan pesan "The system is valid.", yang menunjukkan bahwa blok-blok yang telah masuk masih memiliki nilai yang konsisten.

V. KESIMPULAN

Berbagai kasus yang ditemukan dalam kehidupan sehari-hari dapat diselesaikan dengan teknologi tertentu. Salah satu kasus tersebut adalah pengembangan *whistleblowing* yang dapat dibangun dengan implementasi *blockchain* sederhana. Dengan implementasi blockchain, sistem *whistleblowing* ini dapat menjaga aspek *integrity* dan *non-repudiation* dari laporan.

VI. SARAN

Dari penyelesaian sistem *whistleblowing* menggunakan blockchain ini, didapatkan beberapa peluang untuk melakukan pengembangan program lebih lanjut. Di antaranya:

1. Integrasi dengan layanan penyimpanan cloud untuk menyimpan berkas-berkas bukti digital.
2. Penggunaan private blockchain yang terintegrasi dengan *cloud*.
3. Pengembangan sistem penjaminan akuntabilitas pelapor.
4. Penambahan fungsionalitas untuk melakukan pemrosesan pengaduan.

PRANALA KODE SUMBER

Kode program yang digunakan dalam makalah ini dapat diakses melalui pranala berikut https://github.com/alifiarahmah/blockchain-whistleblowing-plain

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa karena atas berkat rahmat dan karunia-Nya makalah berjudul "Implementasi Blockchain dalam Pengembangan *Whistleblowing System*" yang ditulis untuk menyelesaikan tugas makalah mata kuliah IF4020 Kriptografi dapat diselesaikan dengan baik. Penulis juga mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T., selaku dosen pengampu mata kuliah IF4020 Kriptografi semester II 2023/2024.

DAFTAR PUSTAKA

[1] Muhamad, Nabilah. Ada 791 Kasus Korupsi pada 2023, Potensi Kerugian Rp28 Triliun. 2024. Diakses pada 8 Juni 2024.

(https://databoks.katadata.co.id/datapublish/2024/05/20/ada-791-kasus-korupsi-pada-2023-potensi-kerugian-rp28-triliun)

[2] Hukumonline.com. KPK Luncurkan Sistem Online Pelaporan Whistleblower. 2010. Diakses pada 8 Juni 2024. (https://www.hukumonline.com/berita/a/kpk-luncurkan-sistem-online-pelaporan-iwhistlebloweri-lt4cf622c454ce0/)

[3] Munir, Rinaldi. Penggunaan Kriptografi di dalam Blockchain (Bahan Kuliah IF4020 Kriptografi). 2023. Diakses pada 8 Juni 2024. (https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/40-Penggunaan-kriptografi-di-dalam-blockchain.pdf)

[4] Munir, Rinaldi. Fungsi Hash (Bahan Kuliah IF4020 Kriptografi). 2024. Diakses pada 8 Juni 2024. (https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/24-Fungsi-hash-2024.pdf)

[5] Infinit-O. The 5 Pillars Of Information Security And How To Manage Them. 2018. Diakses pada 12 Juni 2024. (https://resourcecenter.infinit-o.com/blog/the-5-pillars-of-information-security-and-how-to-manage-them/)

[6] Wouter Penard, Tim van Werkhoven. On the Secure Hash Algorithm Family. 2016. Diakses pada 12 Juni 2024. https://web.archive.org/web/20160330153520/https://www.staff.science.uu.nl/~werkh108/docs/study/Y5_07_08/infocry/project/Cryp08.pdf

[7] Geeksforgeeks. Create simple Blockchain using Python. 2023. Diakses pada 11 Juni 2024. (https://www.geeksforgeeks.org/create-simple-blockchain-using-python/)

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Juni 2024

Alifia Rahmah 13520122