Penerapan Algoritma *Decrease and Conquer* dalam Mencari Blok Pertama yang Berbeda pada Blockchain

Bayu Samudra - 13520128[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13520128@std.stei.itb.ac.id

***Abstrak*—NANTI DULU**
***Kata Kunci*—Blockhain, Kriptografi, SHA-32**

I. Pendahuluan

Pada saat ini, perkembangan teknologi digital sangatlah berkembang pesat. Banyak sekali teknologi digital yang baru dari tahun ke tahun. Salah satu teknologi yang muncul dan cukup terkenal saat ini adalah mata uang kripto. Mata uang kripto merupakan sebuah aset digital yang dimiliki seseorang dan dilindungi oleh kriptografi untuk menjaga kepemilikan aset tersebut. Mata uang kripto dapat dipertukarkan dari satu mata uang ke mata uang lainnya. Mata uang ini berdiri di atas teknologi blockhain yang saat ini berkembang cukup pesat.

Teknologi blockhain saat ini penggunaanya tidak hanya dipakai untuk mata uang saja. Pemanfaatan lain dari blockchain ini dapat diimplementasikan pada dunia kesehatan, engineering, bahkan hukum. Saat ini berkembang salah satu penerapan blockhain, yaitu *Non-Fungible Token* (NFT) yang berjalan diatas blockhain untuk menjaga kepemilikan dari suatu barang.

Seperti namanya, blockchain terdiri atas beberapa blok yang saling berkaitan satu sama lain. Setiap blok pada blockhain akan diikat dengan referensi hash dari rantai sebelumnya. Oleh karena itu, pengecekan dua buah blok dapat dengan mudah dilakukan dengan cara melihat saja blok terakhir yang disimpan. Selain itu, blok yang berbeda ini juga dapat dicari dengan berbagai algoritma. Pada makalah kali ini, penulis membatasi pencarian blok yang berbeda hanya pada blok pertama dari sebuah rantai acak yang dibuat.

II. Teori Dasar

A. Struktur Blok

Struktur blok terdiri atas beberapa komponen penting diantaranya adalah sebagai berikut:

1) Hash blok sebelumnya: Seperti yang telah diketahui pada bab sebelumnya, blockchain haruslah terdiri dari rangkaian blok yang saling terhubung satu sama lain. Blok ini dihubungkan dengan hash dari setiap blok sebelumnya. Nilai hash ini juga yang akan menjaga integritas dari suatu block dari perubahan. Perubahan terjadi tentu saja akan mengubah nilai hash dari blok tersebut sehingga blok tersebut akan tidak valid.

2) Konten: Konten perlu disimpan pada struktur blok. Konten ini dapat berisi data kepemilikan, data transaksi, atau data yang lainnya. Data ini harus terjaga integritasnya sehingga data ini tidak boleh berubah.

3) Tanda tangan digital: Untuk memastikan otorisasi dari sebuah blok, diperlukan sebuah bukti persetujuan dari blok tersebut. Dalam uang mata kripto, salah satu cara yang dapat dilakukan adalah menyertakan tanda tangan digital dari block tersebut. Tanda tangan digital pada dasarnya merupakan kumpulan bit yang dapat memrepresentasikan keabsahan kepemilikan data berdasarkan kucin privat dan kunci publik. Teknis tanda tangan digital ini akan dijelaskan pada bagian selanjutnya.

4) Proof of work*:* Penjagaan hanya menggunakan hash tentu saja tidaklah cukup. Pengubahan tetap saja dapat dilakukab dengan cara mengubah isi konten dari data dan juga menghitung ulang seluruh hash dari tiap-tiap blok. Proses perhitungan hash ini biasanya cukup cepat oleh karena itu diperlukan proteksi tambahan yaitu *proof of work*. Proof of work merupakan rangkaian bit yang dapat membuat hash dari sebuah block memiliki pola tertentu. Pencarian rangkaian bit ini tentu saja membutuhkan waktu yang lama sehingga menghambat proses perubahan data pada blockhain.

Pada blok yang ideal, seluruh komponen diatas perlu ada. Hal ini untuk menjaga integritas dari blok tersebut dari serangan luar yang tidak diinginkan.

B. Protokol Pengiriman

Dalam menyebarkan struktur blockchain diperlukan aturan yang dapat menjaga integritas rantai tersebut. Beberapa protokol terinspirasi dari protokol yang diterapkan oleh bitcoin. Beberapa protokol yang penting adalah sebagai berikut:

1) Blok yang ditambahkan valid: Sebelum sebuah blok ditambahkan pada blockchain, perlu dipastikan blok tersebut harus valid. Blok yang valid dapat didefinisikan sesuai dengan kebutuhan. Salah contoh penerapan validitas pada kasus mata uang kripto adalah setiap blok yang dibuat haruslah cukup dengan jumlah saldo yang dimiliki oleh pengirim.

2) Blok baru haruslah ditransmisikan ke seluruh titik: Setiap blok baru yang dibuat haruslah ditransmisikan ke seluruh pemirsa yang berada pada jaringan. Hal ini untuk menjaga keaslian dari rantai blok yang telah dibentuk dikarenakan rangkaian yang asli tersebar di seluruh komputer yang berada pada jaringan. Untuk mengubah rantai, siperlukan mengubah semua rantai yang ada pada jaringan.

3) Blok yang akan ditambahkan haruslah berasal dari rantai yang valid: Disini rantai yang valid didefinisikan rantai yang tersusun atas blok-blok yang valid. Keabsahan dari rantai dapat dilihat dari rantai terakhir pada sebuah blok. Apabila hash terakhir tertera pada blok yang akan ditambahkan dan blok yang akan ditambahkan sah, rantai tersebut bisa jadi valid. Untuk pemeriksaan terakhir, perlu dilakukan sampling dari node lain apakah rantai yang dimiliki saat ini valid. Hal ini dapat dilakukan pemeriksaan juga menggunakan blok terakhir. Bila terjadi perbedaan, dapat dilakukan perubahan sesuai dengan rantai yang benar yang berasal dari node lain.

C. Pembangkit Bilangan Acak

Pembangkit bilangan acak merupakan salah satu alat penting dalam kriptografi. Pembangkit bilangan acak ini akan dibutuhkan dalam beberapa algoritma kriptografi. Terdapat beberapa algoritma pembangkit bilangan acak yang tersedia diantaranya adalah sebagai berikut:

1) Linear Congruential Generator (LCG): Pembangkit bilangan acak ini didasarkan pada rekursifitas terhadap nilai sebelumnya.

III. Kesimpulan

Steganografi merupakan salah satu cara untuk menyembunyikan data pada sebuah cover. Steganografi memiliki banyak cara, salah satunya adalah steganografi dengan metode LSB. Metode LSB ini sangatlah sederhana dan mudah untuk diimplementasikan pada sebuah media baik itu gambar maupun media lainnya.

Penggunaan sistem acak dan penggunaan multi kanal dapat meningkatkan kualitas dari steganografi yang dilakukan. hal ini ditunjukan dengan hasill steganalisis visual yang menunjukan sistem acak memberikan keamanan lebih dibandingkan tanpa pengacakan. Selain itu, penggunaan kanal secara merata dapat juga memberikan penyamaran lebih terhadap steganalisis visual sehingga lebih sulit dikenali.

Ucapan Terima Kasih

Alhamdulillah, segala puji Allah SWT karena atas pertolongan dan rahmatnya, saya dapat menyelesaikan makalah ini. Penulis juga turut memberikan ucapan terima kasih kepada keluarga yang selalu setia untuk memberikan motivasi dan semangat untuk dapat menyelesaikan makalah ini. Penulis juga turut mengucapkan terima kasih kepada para dosen pengampu mata kuliah Matematika Diskrit, yaitu ibu Dr. Nur Ulfa Maulidevi, S.T., M.Sc., bapak Dr. Ir. Rinaldi Munir, M.T., dan ibu Dra. Harlili S., M.Sc. atas segala ilmunya yang telah membantu penulis dalam menyelesaikan makalah ini. Semoga dengan kebaikan yang telah diberikan, Allah akan menggantinya dengan yang lebih baik lagi.

Sumber Daya

Segala sumber daya yang digunakan untuk membangun makalah ini dapat anda akses pada https://github.com/bayusamudra5502/stima-blockchain.

Daftar Pustaka

[1] Munir, Rinaldi. 2019. *Kriptografi Edisi Kedua*. Bandung: Penerbit Informatika

Pernyataan

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

Cimahi, 21 Mei 2022

Bayu Samudra - 13520128