

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

Bayu Samudra - 13520128¹

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

¹13520128@std.stei.itb.ac.id

Abstrak—NANTI DULU

Kata Kunci—Blockchain, 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 blockchain yang saat ini berkembang cukup pesat.

Teknologi blockchain saat ini penggunaannya 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 blockchain, yaitu *Non-Fungible Token* (NFT) yang berjalan diatas blockchain untuk menjaga kepemilikan dari suatu barang.

Seperti namanya, blockchain terdiri atas beberapa blok yang saling berkaitan satu sama lain. Setiap blok pada blockchain 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 blok tersebut. Tanda tangan digital pada dasarnya merupakan kumpulan bit yang dapat memrepresentasikan keabsahan kepemilikan data berdasarkan kuncin 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. Perubahan 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 blockchain.

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 [4]. 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, diperlukan 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. Berdasarkan sumber dari [1], Berikut ini adalah formula yang dapat digunakan untuk mendapatkan nilai acak menggunakan LCG:

$$x_{i+1} = (ax_i + b) \mod m \quad (1)$$

Untuk memulai pembangkitan bilangan acak, diperlukan nilai x_0 yang merupakan umpan dari bilangan acak ini.

Periode bilangan acak dari LCG ini pastilah tidak akan melebihi nilai m . Hal ini dikarenakan adanya modulo yang diberikan pada persamaan 1. Menurut [3], Algoritma ini memiliki periode sebagai berikut:

Teorema II.1 (Teorema Hull–Dobell). Sebuah LCG yang didefinisikan pada definisi 1 dapat memiliki periode penuh, yaitu berperiode $m - 1$ jika memenuhi syarat berikut:

- 1) b relatif prima terhadap m ,
- 2) $a \equiv 1 \pmod{p}$ jika p merupakan faktor prima dari m ,
- 3) $a \equiv 1 \pmod{4}$ jika m adalah bilangan yang habis dibagi oleh 4.

Pembangkit bilangan acak berbasis LCG biasanya sudah tersedia dalam berbagai bahasa pemrograman. Selain mudah diimplementasikan, algoritma ini juga sangat mangkus dikarenakan hanya diperlukan kompleksitas $O(1)$ dalam membuat bilangan acak. Sayangnya, algoritma ini cukup mudah ditebak nilai acaknya sehingga tidak cocok untuk penggunaan kriptografi. [1]

2) *Blum-Blum-Shub:* Algoritma *Blum-Blum-Shub* (BBS) merupakan salah satu algoritma pembangkit bilangan acak yang lebih aman untuk kebutuhan kriptografi. Menurut [1], algoritma ini merupakan algoritma yang paling mangkus dan paling seerhana dari semua algoritma pembangkitan bilangan acak yang termasuk dalam kategori *cryptographically-secure pseudorandom number generator* (CSPRNG). Menurut [1], Berikut ini adalah algoritma yang digunakan untuk membuat bilangan acak menggunakan BBS:

- 1) Menentukan bilangan prima rahasia p dan q yang memenuhi kongruensi berikut

$$p \equiv q \equiv -1 \pmod{4} \quad (2)$$

- 2) Hitunglah nilai $n = pq$. Nilai n ini disebut dengan bilangan bulat blum.
- 3) Diperlukan menentukan nilai umpan x_0 . Untuk mendapatkan nilai ini, tentukan bilangan bulat acak lain, misalkan s yang memenuhi:

$$1 < s < n$$

s dan n relatif prima.

Nilai x_0 dengan formula sebagai berikut

$$x_0 = s^2 \mod n \quad (3)$$

- 4) Nilai x_i bisa diperoleh dengan formula berikut

$$x_i = x_{i-1}^2 \mod n \quad (4)$$

- 5) Diambil nilai LSB dari x_i sebut saja z_i . Nilai $z_i = x_i \mod 2$. Nilai z_i menyusun bit-bit dari bilangan baru yang dibentuk.

D. SHA-3 (Keccak)

SHA-3 merupakan algoritma fungsi hash satu arah yang dibuat oleh Guido Breton, Joan Daemen, dan Michaël Peeters. Algoritma ini menggantikan algoritma MD5 dan SHA-1 yang telah ditemukan kolisinya sehingga sudah tidak aman lagi.

Fungsi hash merupakan fungsi yang menerima masukan string dengan panjang sembarang dan menghasilkan hash yang memiliki panjang tetap. Fungsi hash satu arah berarti pesan yang telah melakukan kompresi menjadi nilai hash tidak bisa dipulihkan kembali menjadi nilai aslinya. [1]

Dalam algoritma SHA-3 dikenal sebuah istilah spon. Spon merupakan state yang diinisialisasi dengan nilai 0. Pada algoritma ini dikenal beberapa fase, yaitu sebagai berikut: [1]

- 1) Fase Persiapan
Pada fase ini, pesan yang akan dihash akan diberikan padding terlebih dahulu dan dipecah menjadi beberapa blok dengan ukuran r .
- 2) Fase Penyerapan
Pada fase ini, blok-blok yang telah dipecah tadi diserap dengan cara melakukan operasi xor terhadap spon dengan panjang r . Hasil operasi tersebut lalu dimasukkan ke dalam fungsi permutasi. Hal ini dilakukan hingga semua blok sudah terisi.

3) Fase Pemerasan

Dilakukan inisialisasi pada string kosong Z . Selagi panjang Z belum sama dengan panjang string keluaran yang diinginkan, ambil r digit pertama disambungkan dengan Z lalu masukan spons ke dalam fungsi permutasi.

Berikut ini adalah ilustrasi pembentukan spons dari algoritma SHA-3.

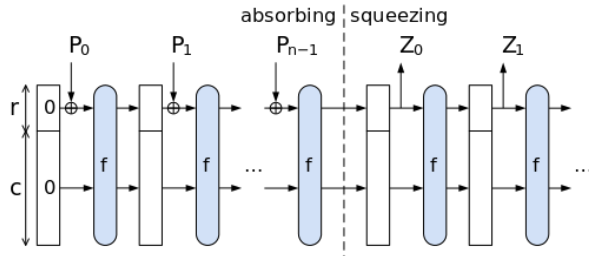


Fig. 1. Ilustrasi pembentukan spons (Sumber: Wikipedia)

E. Digital Signature Algorithm (DSA)

Salah satu aspek penting yang harus ada dalam blockchain adalah tanda tangan digital. Terdapat cukup banyak algoritma tanda tangan digital yang tersedia. Untuk bahasan kali ini, penulis hanya membatasi membahas mengenai tanda tangan digital DSA (*Digital Signature Algorithm*).

Dikutip dari [1], Sebelum melakukan proses diperlukan melakukan perhitungan beberapa nilai sebagai berikut:

- Nilai p merupakan bilangan prima yang bersifat publik dengan panjang L . Nilai L haruslah kelipatan 64 dan berada pada rentang $64 \leq L \leq 1024$.
- Nilai q merupakan bilangan prima 160 bit yang merupakan faktor dari $p - 1$ dan bersifat publik.
- Nilai $g = h^{(p-1)/q}$ dengan nilai $h < p - 1$ sehingga membuat nilai $g \bmod p > 1$. Nilai ini bersifat publik.
- x merupakan bilangan bulat kurang dari q . Nilai ini bersifat privat.
- Nilai $y = g^x \bmod p$ yang merupakan kunci publik.
- Pesan M yang akan ditandatangani.
- Nilai $H(M)$ yang merupakan hash dari pesan M .

Untuk membuat tanda tangan, seorang pengirim perlu mendapatkan sebuah angka acak k yang kurang dari q . Tanda tangan r dan s dapat didapatkan dengan rumus sebagai berikut: [1]

$$r = (g^k \bmod p) \bmod q \quad (5)$$

$$s = k^{-1}(H(M) + xr) \bmod q \quad (6)$$

Untuk melakukan verifikasi pesan, seorang penerima perlu mendapatkan nilai (p, q, g, y) dan hasil tandatangan (r, s) . Perhitungan yang dilakukan adalah sebagai berikut: [1]

$$w = s^{-1} \bmod q \quad (7)$$

$$u_1 = (H(M) \cdot w) \bmod q \quad (8)$$

$$u_2 = rw \bmod q \quad (9)$$

$$v = ((g^{u_1} \cdot y^{u_2}) \bmod p) \bmod q \quad (10)$$

Apabila nilai $v = r$, dapat dikatakan tandatangan sah.

F. Decrease and Conquer (DnC)

Decrease and conquer (DnC) merupakan metode perancangan algoritma penyelesaian dengan mereduksi persoalan menjadi dua bagian yang selanjutnya akan dipilih sebuah sub persoalan untuk dievaluasi selanjutnya. [2]

Terdapat beberapa variasi dari metode *Decrease and conquer*, yaitu sebagai berikut

• *Decrease by constant*

Pada variasi ini, ukuran persoalan dikurangi berdasarkan besar yang konstan setiap iterasi algoritma berlangsung. Salah satu contoh algoritma yang termasuk dalam kategori ini adalah *selection sort* dengan konstanta 1.

• *Decrease by constant factor*

Pada variasi ini, ukuran persoalan direduksi berdasarkan nilai faktor yang konstan selama iterasi berlangsung. Salah satu contoh algoritma yang termasuk dalam kategori ini adalah pencarian biner dengan faktor konstanta 2.

• *Decrease by variable size*

Pada variasi ini, ukuran persoalan direduksi dengan jumlah bervariasi setiap kali dilakukannya iterasi. Salah satu contoh algoritma yang termasuk dalam bentuk ini adalah pencarian interpolasi.

Algoritma ini juga terdiri atas dua tahapan penting yaitu sebagai berikut:

1) *Decrease*

Pada tahap ini, persoalan akan dibagi menjadi beberapa upa-persoalan yang lebih kecil.

2) *Conquer*

Pada tahap ini, akan dipilih sebuah upa-persoalan yang akan diselesaikan. Upa-persoalan terpilih akan diselesaikan kembali menggunakan DnC secara rekursif.

III. PERANCANGAN ALGORITMA

Pada bab ini, akan dibahas rancangan algoritma yang digunakan untuk menyelesaikan permasalahan.

A. Deskripsi Permasalahan

Akan dibandingkan kesamaan antara dua buah blockchain yang sama panjang. Bila kedua blockchain berbeda, akan dicari blok pertama yang menyebabkan kedua blockchain berbeda.

B. Asumsi dan Batasan

Dalam perancangan ini, diberikan beberapa asumsi sebagai berikut:

- Blockchain bisa saja memiliki lebih dari 1 buah blok yang berbeda.
- Nilai hash dari blok sebelumnya valid. Hal ini berarti tidak ada blok yang memiliki nilai blok yang berbeda dengan yang dicatatkan pada blok tersebut.
- Dalam pengujian, struktur blockchain hanya terdiri atas nilai hash sebelumnya dan konten dari blok. Hal ini dimaksudkan untuk menyederhanakan dan mempercepat proses pengujian.

C. Desain Algoritma

Algoritma yang digunakan menggunakan metode *decrease and conquer* berbasis *decrease by constant factor*. Faktor yang digunakan untuk mereduksi adalah 2. Berikut ini adalah algoritma lengkap mengenai proses yang dilakukan saat pencarian blok yang berbeda:

- 1) Set nilai awal l sebagai indeks batas bawah (inklusif) dari pencarian dan nilai r sebagai indeks batas atas (eksklusif) dari pencarian.
- 2) Cek apakah nilai $l < r$. Bila tidak hentikan iterasi. Kedua blockchain merupakan blok yang sama.
- 3) Hitung hash blok tengah dengan indeks ke- $\lfloor \frac{l+r}{2} \rfloor$ dari kedua blok.
- 4) Bila nilai hash dari keduanya sama, maka set nilai l menjadi $\lfloor \frac{l+r}{2} \rfloor$. Lanjutkan iterasi ke langkah ke-2.
- 5) Bila nilai hash dari keduanya tidak sama, perlu diperiksa letak dari blok tengah. Bila blok tengah merupakan blok awal (berindeks 0), maka kedua blockchain berbeda pada blok pertama. Hentikan iterasi.
- 6) Bila nilai hash dari keduanya tidak sama dan blok tengah tidak berada pada indeks 0, perlu diperiksa hash blok sebelumnya. Apabila hash blok sebelumnya dari kedua blockchain memiliki nilai yang sama, blok pertama yang berbeda adalah blok tengah. Hentikan iterasi.
- 7) Bila nilai hash dari keduanya tidak sama, blok tengah tidak berada pada indeks 0, dan indeks sebelumnya berbeda, ubah nilai r menjadi $\lfloor \frac{l+r}{2} \rfloor$. Lanjutkan iterasi ke langkah 2.

D. Psedeocode Penyelesaian

Psedeocode dari penyelesaian permasalahan di atas ditunjukkan oleh algoritma pada figur 2.

Fungsi `CheckDifference()` memberikan nilai 0 pada saat ditemukan blok yang berada pada indeks ke-0 tapi berbeda atau blok yang tidak berada di indeks ke-0, berbeda, dan hash sebelumnya sama. Fungsi ini juga memberikan nilai 1 apabila ditemukan nilai blok yang dites pada indeks tersebut sama. Fungsi ini juga memberikan nilai -1 bila blok pada indeks yang dipilih dan pada indeks sebelumnya dari dua buah blockchain berbeda.

Nilai 0 pada fungsi `CheckDifference()` berarti blok yang membuat dua buah chain berbeda ditemukan. Nilai -1 berarti blok yang membuat berbeda berada pada indeks kurang dari

```
func FindFirstDiff(chain1, chain2 Chain)
    int64 {
    if chain1.length != chain2.length {
        panic("Ukuran chain harus sama")
    }

    l := int64(0)
    r := chain1.length

    for l < r {
        center := (l + r) / 2
        diff :=
            CheckDifference(chain1, chain2,
                center)

        if diff == 0 {
            return center
        } else if diff > 0 {
            l = center + 1
        } else {
            r = center
        }
    }

    return -1
}
```

Fig. 2. Algoritma Pencarian Blok dengan DnC

```
func CheckDifference(Chain1, Chain2 Chain,
    idx int64) int64 {
    it1 := Chain1.GetChainItem(idx)
    it2 := Chain2.GetChainItem(idx)

    if it1.GetBase64Hash()
        != it2.GetBase64Hash() {
        if idx > 0 {
            last1 := Chain1.GetChainItem(idx - 1)
            last2 := Chain2.GetChainItem(idx - 1)

            if last1.GetBase64Hash() ==
                last2.GetBase64Hash() {
                return 0
            } else {
                return -1
            }
        } else {
            return 0
        }
    } else {
        return 1
    }
}
```

Fig. 3. Algoritma Pembanding

indeks saat ini. Nilai 1 berarti blok yang membuat berbeda bisa jadi berada pada indeks yang lebih besar dari indeks saat ini. Pemberian nilai 1 pada fungsi ini tidak menjamin akan mendapatkan blok yang berbeda dikarenakan bisa jadi kedua buah blockchain sama.

E. Analisis Solusi

IV. 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 ditunjukkan dengan hasil steganalisis visual yang menunjukkan 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 Dr. Masayu Leylia Khodra. 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
- [2] Munir, Rinaldi. 2021. *Algoritma Decrease and Conquer*. Bandung: Institut Teknologi Bandung. Diakses pada 2022-05-21 melalui <https://informatika.stei.itb.ac.id/rinaldi.munir/Stmik/2020-2021/Algoritma-Decrease-and-Conquer-2021-Bagian1.pdf>
- [3] Hull, T. E. & Dobell, A. R. 1962. Random Number Generators. *SIAM Review*, 4(3), 233. Diakses pada 2022-05-21 melalui http://chagall.med.cornell.edu/BioinfoCourse/PDFs/Lecture4/random_number_generator.pdf.
- [4] Nakamoto, Satoshi. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Diakses pada 2022-05-21 melalui <https://bitcoin.org/bitcoin.pdf>.

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