Aplikasi Teori Bilangan pada Bitcoin Menggunakan Kriptografi

Muhammad Alfian Rasyidin, 13516104
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13516104@std.stei.itb.ac.id

***Abstrak* — Kriptografi merupakan salah satu ilmu matematika yang paling banyak digunakan, khususnya dalam dunia komputer. Semakin bermunculan *financial technology* dalam era globalisasi ini mendorong pelaku bisnis untuk dapat memastikan data pribadi penggunanya disimpan secara aman dengan meningkatkan fitur keamanan sistem yang dimilikinya. Bitcoin merupakan salah satu inovasi *financial technology* yang berbasis *cryptocurrecy*. Tak ada bank sentral yang mencatat pembukuan transaksi-transaksi yang dilakukan, seperti bank pada umumnya. Hal ini membuat Bitcoin harus bekerja lebih untuk menjamin data pribadi penggunanya. Lalu, apa saja yang digunakan Bitcoin untuk itu? Bagaimana penerapan prinsip kriptografi pada sistem pembayaran ini?**

***Kata Kunci* — bitcoin, fungsi hash, kriptografi, teori bilangan.**

I. PENDAHULUAN

Financial technology, atau yang sering disingkat dengan *fintech* merupakan salah satu sektor bisnis yang paling banyak berkembang saat ini. Dengan semakin banyaknya penjualan dan pembelian yang dilakukan secara daring *(online)* membuat permintaan akan transaksi elektronik semakin besar. Hal ini yang membuat banyak perusahaan-perusahaan pemula *(startup)* bergerak dalam sektor ini. Tujuan mereka tak lain ialah memciptakan inovasi agar transaksi elektronik menjadi semakin mudah, cepat, murah, dan menjangkau hingga ke seluruh wilayah.

Bitcoin merupakan salah satu dari sekian banyak inovasi *financial technology* yang populer saat ini. Inovasi ini tergolong unik dari yang lain, bahkan masih menjadi sorotan mengenai legalitasnya saat ini [1]. Tidak seperti kebanyakan *financial technology* lainnya yang masih menggunakan bank sentral sebagai pusat pertukaran dan perekaman transaksi, Bitcoin tidak menggunakan bank sentral untuk melakukan transaksi elektroniknya. Bitcoin merekam transaksinya secara *peer to peer connection* antar pengguna layanan itu sendiri. Hal ini yang membuat setiap orang seolah-olah dapat melihat seluruh transaksi yang dilakukan di dunia, walaupun kita tidak menjadi subjek yang melakukan transaksi tersebut. Oleh karena itu, fitur keamanaan menjadi hal paling penting dalam melakukan segala aktivitas transaksi di Bitcoin, bukan hanya Bitcoin, namun *financial technology* lainnya juga.

Fitur keamaan digunakan Bitcoin dalam melakukan enkripsi terhadap transaksi yang dilakukan, memastikan bahwa transaksi yang dilakukan merupakan transaksi yang sahih dan lain sebagainya. Teori bilangan merupakan ilmu yang menjadi dasar berkembangnya sistem persandian saat ini. Ilmu yang mempelajari tentang persandian disebut juga dengan kriptografi. Seiring bertambahnya waktu, semakin banyak algoritma yang telah ditemukan dan digunakan untuk membuat persandian saat ini.

II. LANDASAN TEORI

A. Aritmatika Modulo

Aritmatika modulo adalah perhitungan bilangan bulat yang dilakukan secara aljabar dan mementingkan sisa pembagian disebut dengan modulo (notasi mod). Aritmatika modulo merupakan salah satu bahasan matematika yang paling banyak digunakan di bidang komputer. Secara teori, definisi aritmatika modulo ialah sebagai berikut:

"Jika a, q, r, dan m merupakan bilangan bulat , dengan $m>0$, operasi a mod m (dibaca: a modulo m) memberikan sisa r. Sehingga $a = mq + r$, dengan $0 \leq r < m$." [3]

Sering kali banyak bilangan bulat mempunyai sisa pembagian yang sama jika dibagi dengan suatu nilai yang sama. Hal ini yang disebut juga dengan kekongruenan di dalam aritmatika modulo. Kekongruen ini biasa dituliskan dengan notasi (≡). Kekongruenan menurut definisi adalah sebagai berikut:

"Jika a, b, dan m adalah bilangan bulat, dengan $m>0$. a dikatakan kongruen dengan b $(a \equiv b \pmod{m})$, jika dan hanya jika m habis membagi $a-b$ $(m|a-b)$" [3]

Selanjutnya, sifat lain yang perlu dipahami ialah bilangan prima dan relatif prima. Kedua prinsip ini biasa digunakan untuk membuat *(generate)* kunci publik dan kunci pribadi dalam suatu sistem keamanan. Bilangan prima itu sendiri didedifinisikan sebagai berikut:

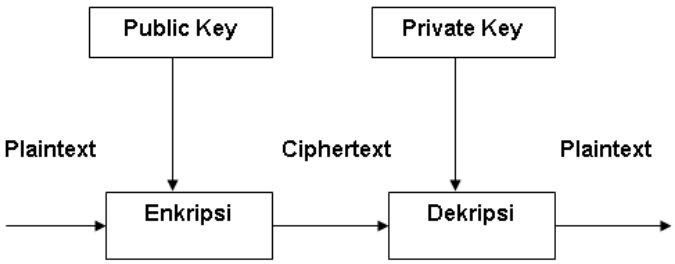
" Jika p merupakan bilangan bilangan posif lebih besar dari 1, dan jika pembaginya hanya 1 dan p, maka p merupakan bilangan prima" [3]

Sedangkan, dua bilangan dapat dikatakan relatif prima yaitu jika *a* dan *b* merupakan bilangan bulat dan jika PBB *(a,b)* = 1 [3].

B. Kriptografi

Ilmu mengamankan pesan disebut juga dengan kriptografi. Dalam perkembangannya, semakin banyak algoritma yang membuat pesan semakin sulit untuk dibocorkan tanpa autentikasi. Sistem pengamanan inilah yang menjadi cikal bakal *financial technology* berkembang hingga saat ini. Kebutuhan akan elektronik yang mudah dan aman menjadikan ilmu ini terus berkembang dan menjadi salah satu hal yang dipromosikan ke pengguna agar menggunakan jasanya.

Fasilitas yang digunakan untuk menkonversikan *plain-text ke chipertext* dan sebaliknya disebut juga dengan *Cryptosystem.* Terdapat beberapa aturan yang dibuat baik secara statis maupun dinamis dalam menentukan transformasi menjadi suatu kunci baru tertentu. Banyak metode-metode yang telah ditemukan untuk membangkitkan kata-kata bersandi ini.



Gambar 1. Skema Enkripsi dan Dekripsi
sumber : kaaeka.files.wordpress.com/2011/07/kriptografi4.png

Salah satunya yaitu Julius Caesar yang berasal dari Romawi sekitar tahun 60 S.M. Teknik yang digunakan ialah mensubtitusikan alfabet secara berurutan, ini berarti sama saja membaginya dengan 26 (jumlah alfabet). Semisal yaitu kata berikut yang menggeser sebanyak 5 huruf setelahnya.

plain text *:* SEJARAH KRIPTOGRAFI
chipertext *:* XJOFWFM PWNUYTLWFJN

Tentunya kata yang telah menjadi *chipertext* lebih sulit untuk dipahami kembali maknanya. Untuk mengembalikan *chipertext* menjadi *plaintext* disebut dengan proses dekripsi *(decryption)*. Dalam metode ini, proses tersebut dapat dilakukan dengan menguranginya dengan 5 dan membaginya secara modulo dengan 26.

Pada dasarnya terdapat beberapa teknik dasar dalam kriptografi yaitu:

a. Subtitusi

Penerapannya seperti pada contoh algoritma yang digunakan Julius Caesar yaitu mencocokkan *plaintext* dan *chypertext* yang merupakan pasangannya. Berikut contoh tabel subtitusi pada contoh soal sebelumnya:

A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T
F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y

U-V-W-X-Y-Z
Z-A-B-C-D E

b. *Blocking*

Metode ini menggunakan pemilihan jumlah baris dan kolom pada sebuah matriks (tabel) untuk melakukan konversi pesan. *Plaintext* biasanya dienkripsikan dengan cara menuliskannya di matriks secara vertikal beruturan dari kolom paling kiri. Jika kolom terkiri sudah terisi penuh, maka penulisan dilanjutkan ke kolom yang berada di kanannya, begitu seterusnya. *Chipertext* yang dibaca ialah kebalikannya, yaitu membacanya secara baris per baris, mulai dengan baris pertama yang berada paling atas. Berikut contoh penerapannya:

S	A	I	R
E	H	P	A
J		T	F
A	K	O	I
R	R	G	

Tabel 1. Penerapan Metode *Blocking*

Sehingga, *chipertext* yang dihasilkan yaitu SAIREHPAJ TFAKOIRRG . Selain dengan memasukkan *plaintext* secara vertikal, enkripsi juga bisa dilakukan dengan memasukkan *plaintext* secara baris per baris, kemudian membaca *chipertext* dengan kolom per kolom.

c. Permutasi

Permutasi merupakan salah satu ilmu dalam matematika yang memanfaatkan teknik kombinasi yang memperhatikan urutan. Prinsip dari teknik permutasi ini sebenarnya hampir mirip dengan teknik subtitusi. Namun, teknik subtitusi ialah mengganti nilai dari kode itu sendiri dengan cara melakukan operasi aritmatika dan membaginya dengan modulo dari 26. Sedangkan, teknik permutasi tidak mengubah nilai kode tersebut, tetapi melakukan pengacakan urutan. Hal ini sering disebut juga dengan transposisi. Berikut contohnya:

plaintext *:* SEJARAH KRIPTOGRAFI
chipertext *: EKSJAARHIFARGOTPI*

Chipertext yang dihasilkan dengan teknik ini lebih dilakukan secara acak dan hanya dengan mengetahui kunci dekripsinya, kita dapat menerjemahkannya kembali ke *plaintext.*

d. Pemampatan

Teknik dasar berikutnya yaitu pemampatan atau *compression.* Sesuai dengan namanya teknik ini akan menghasilkan jumlah karakter *chipertext* lebih sedikit dibandingkan dengan jumlah karakter *plaintext*-nya. Oleh karena itu, terjadi penghapusan beberapa elemen yang telah ditentukan. Namun, elemen-elemen yang terhapus tersebut sebenarnya masih diikutkan dengan *chipertext*, tetapi digunakan sebagai lampiran sehingga dapat menjadi pengecoh. Berikut contoh penerapannya:

plaintext *:* SEJARAH KRIPTOGRAFI
elemen yang dihapus : JARTRI

chipertext *:* SEARHKIPOGAF
lampiran chipertext : OFWYWN
(dengan melakukan subtitusi)

Teknik-teknik tersebut biasa digunakan pada masa kuno, sebelum berkembangnya komputer. Tekniknya cukup sederhana, namun sebenarnya *chipertext* yang dihasilkan cukup kompleks dan sulit untuk dipecahkan. Setelah ditemukannya komputer, kriptografi semakin berkembang dan menghasilkan banyak tipe enkripsi yang beredar saat ini yang banyak digunakan untuk keperluan privasi seperti pada *financial technology*. Berikut beberapa yang sering digunakan [6]:

a. *Advanced Encryption Standard* (AES)
Enkripsi ini mulai muncul pada tahun 2001 dan menggunakan panjang kunci bervariasi yaitu 128, 192, atau 256 bit. Penerapan enkripsi ini biasanya pada *smart card.*

b. RSA *Encryption*
RSA merupakan singkatan dari nama-nama perancang algoritma ini yairu Rivest, Shamir, Adleman pada tahun 1977. Algoritma ini dapat digunakan oleh berbagai platform *(multi-platform)* dan mendukung proses otentikasi *(authentication).*

c. *Secure Socket Layer* (SSL)
Enkripsi ini banyak digunakan di portal-portal dalam jaringan *(website)* dalam melakukan tukar-menukar data antara pengguna *(client)* dan penyedia *(server)*. Metode yang digunakan ialah menggunakan kunci publik dan kunci pribadi dan dapat juga melakukan autentikasi.

d. *Secure Hash Algorithm* (SHA)
Algoritma ini dirnacang oleh *National Institute of Standard and Technology* (NIST) di Amerika Serikat. Algoritma ini mendukung *digital signature.* Beberapa versi yang ada saat ini yaitu SHA-256, SHA-384, SHA-512 yang juga terintegrasi dengan *Advanced Encryption Standard* (AES). Bitcoin menggunakan SHA-256 sebagai enkripsinya untuk melakukan validasi transaksi dan otentikasi dalam bentuk *digital signature.*

C. Fungsi Hash

Fungsi *hash (hash function)* ialah sebuah fungsi yang mengkonversikan masukkan menjadi kelauran yang umumnya berukuran jauh lebih kecil daripada ukuran awalnya. Fungsi ini dapat menerima masukan apapun dan berukuran bebas, sehingga dapat dinyatakan:

$$\boldsymbol{h = H(M)}$$

h merupakan nilai *hash* atau *hash value* yaitu keluaran pesan yang telah melewati fungsi *hash*. *H* merupakan fungsi *hash*, dan *M* merupakan masukan pesan atau sering disebut *(plaintext).*

Nama lain yang sama dengan fungsi *hash* ialah fungsi kompresi/kontraksi *(compression function), fingerprint, cryptographic checksum, message integrity check* (MIC), *manipulation detection code* (MDC). Aplikasi dari fungsi *hash* ialah menguji kesamaan dari arsip yang dikirim oleh pengirim dengan arsip yang diterima oleh penerima. Biasanya, pengujian ini dilakukan dengan mencocokkan suatu *string* yang dihasilkan oleh kunci pribadi *(private key)* yang hanya dimiliki dan diketahui oleh pengirim dan *string* yang dihasilkan dengan kunci publik *(public key)* yang diketahui oleh publik untuk keperluan pengujian.

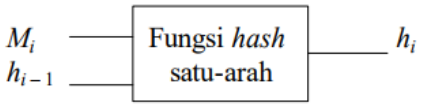
Bitcoin sendiri menggunakan fitur keamanan *Secure Hash Algorithm* (SHA-256) yang berarti menggunakan fungsi *hash* yang berbasis (panjang karakter) yaitu 256 bit. Selain itu juga, fungsi *hash* yang digunakan ialah fungsi *hash* satu arah *(one-way hash)*. Ini berarti pesan yang telah dienkripsi tidak dapat dikembalikan menjadi pesan semula, tidak memiliki balikan *(non-invertible).*

Berikut merupakan sifat-sifat dari fungsi *hash* satu-arah[4]:

1. Fungsi *H* tidak memiliki batasan blok.
2. *Hash value (h)* yang dihasilkan oleh fungsi *H* memiliki panjang yang tetap *(fixed-length output).*
3. Setiap nilai *x* yang diberikan, *H(x)* selalu dapat dan mudah untuk dihitung.
4. Jika $h = H(x)$ dan $a = H(h)$, maka *h* tidak mungkin sama dengan *a* bagaimana pun caranya.
5. Untuk setiap *x*, tidak mungkin dapat mencari $y^{-1} = x$ sedemikian sehingga $H(y) = H(x)$.
6. Tidak mungkin mencari pasangan *x* dan *y* sedemikian sehingga $H(x) = H(y)$.

Berikut definisi matematis dan ilustrasi dari definisi fungsi *hash* satu arah:

$$\boldsymbol{h_i = H(M_i, h_{i-1})}$$



Gambar 2. Skema Fungsi Hash
sumber : Diktat IF5054 Kriptografi [4]

D. Bitcoin

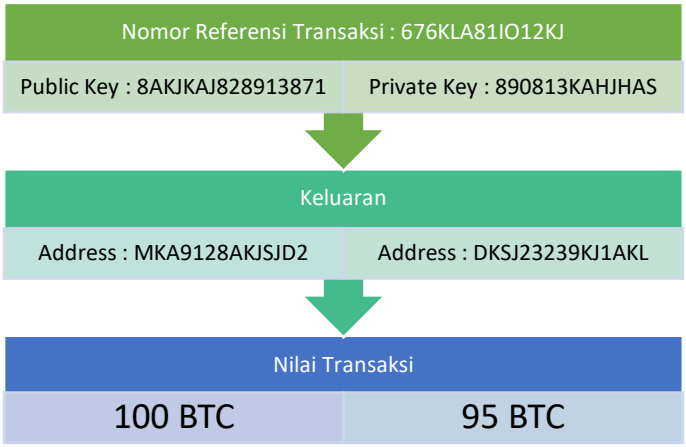
Satoshi Nakamoto merupakan nama samaran dari pendiri Bitcoin ini di awal terciptanya pada tahun 2009. Bitcoin tidak berafiliasi dengan bank sentral untuk mengurus sistem pembukuan yang dimilikinya [8]. Hal yang membuatnya menjadi pilihan ialah tidak adanya biaya transaksi dan tidak diperlukan nama untuk melakukan transaksinya (anonim).

III. MEKANISME BITCOIN

A. Ide Awal Bitcoin

Bitcoin tidak memiliki sentral yang mencatat daftar rekaman transaksi yang telah dilakukan, seperti *financial technology* lainnya. Tak hanya daftar rekaman transaksi, namun jumlah deposit yang dimiliki oleh pengguna pun tidak disimpan. Oleh karena itu, pembukuan *(legder)* dilakukan secara publik dengan memanfaatkan *peer-to-peer connection* yang dilakukan oleh seluruh pengguna yang terdaftar. Jumlah deposit tidak perlu dicatat di sistem, karena prinsipnya ialah menyocokkan semua transaksi masuk/keluar yang telah divalidasi (sudah berada di pembukuan) dengan transaksi baru yang akan dimasukkan ke pembukuan.

Sistem pembukuan ini dilakukan secara terus menerus dan selalu dikelola oleh komunitas pengguna secara terdistribusi. Hal ini juga seolah membuat setiap orang dapat melihat transaksi milik semua orang. Oleh karena setiap orang seolah dapat melihat akun pengguna lainnya, Bitcoin menggunakan kunci publik *(public names)* disamping menggunakan nama asli. Hal ini digunakan agar rekaman transaksi tetap bersifat anonim. Selain itu, kunci publik juga digunakan untuk melakukan validasi akan transaksi yang telah dilakukan *(signatures)*.

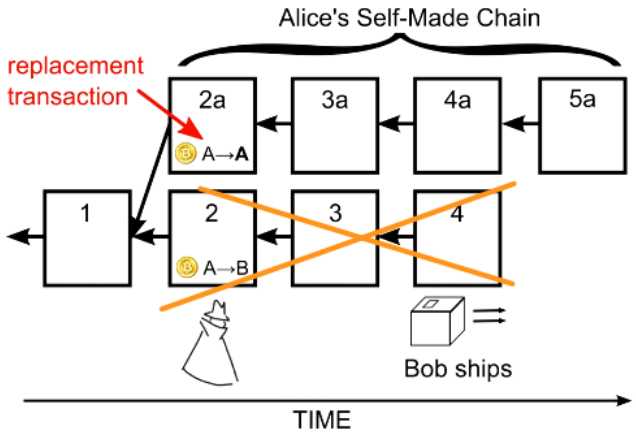


Gambar 3. Pemodelan Transaksi di Bitcoin

Pembukuan tidak mungkin dilakukan dengan mencatat per transaksi, hal itu akan membuat semakin panjang rangkain data yang harus disimpan, yang tentunya tidak efisien. Oleh karena itu, proses pembukuan dilakukan dengan cara blok yang sering disebut dengan rantai blok *(block chain)*. Rantai ini berisikan daftar transaksi-transaksi yang dilakukan di dalam blok itu. Blok mempunyai alamat unik masing-masing yang akan menjadi *identifier* dalam mencari transaksi. Suatu blok juga mempunyai komponen yaitu *header* yang menyimpan alamat dari blok sebelumnya dan komponen lainnya yaitu daftar transaksi-transaksi yang ada di blok tersebut. Jika dilakukan proses pencarian secara mundur *(backtrack)*, maka akan ditemukan hingga transaksi yang pertama kali dibuat. Hal ini karena rantai blok selalu disimpan dan hanya diperpanjang, namun tidak ada proses pemotongan.

Rantai Blok = Header + Daftar Transaksi

Rantai blok dibentuk oleh para penambang *(miners)* yang lama kelamaan menjadi rantai yang sangat panjang. Namun, terkadanh, rantai tersebut menjadi bercabang dan berbentuk seperti pohon. Hal ini bukankah akan menjadikan ambiguitas jika dilakukan proses *backtracking* untuk menelusuri daftar transaksi sebelumnya? Bitcoin tetap hanya mempunyai satu rantai yang dianggap sahih. Rantai tersebut ialah rantai terpanjang. Sehingga, jika ada percabangan yang muncul dalam membangun rantai, maka hanya satu rantai yang dianggap valid oleh komunitas.

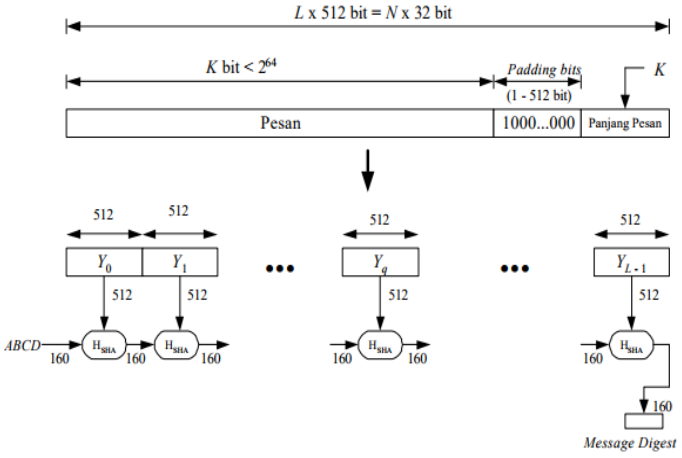


Gambar 4. Bitcoin Block Chain
sumber :
http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

B. Kriptografi dalam Bitcoin

SHA-256 berbasis 256 bit digunakan sebagai fitur keamanan dalam menguji nomor referensi transaksi yang dihasilkan oleh kunci publik *(public key)* sama dengan yang dihasilkan oleh kunci pribadi *(private key)*. Masukan fungsi *hash* pada Bitcoin berupa pesan *(string)*, biasanya berisi intruksi transaksi yang dilakukan. Sebagai contoh "A transfer Rp. 100.000 ke B". Keluaran yang dihasilkan oleh fungsi *hash* yaitu berupa rantai bilangan biner (0 dan 1) yang memanjang sebanyak 256 bit. Keluaran inilah yang menjadi nomor referensi transaksi, selain *digital signature* yang mempunyai kombinasi karakater yang berbeda yang akan dipergunakan untuk uji keaslian pesan.

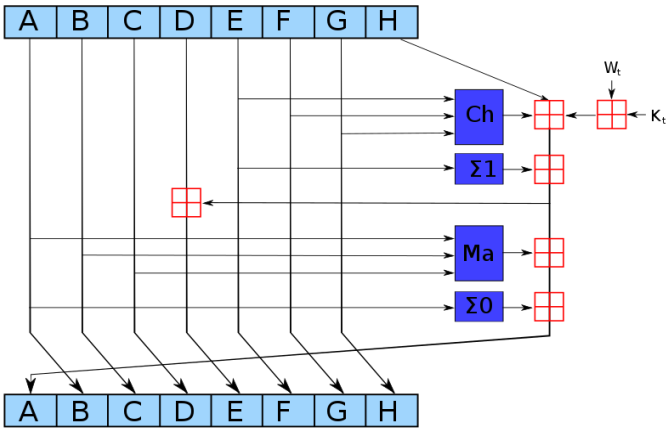
Fungsi ini bersifat publik, sehingga setiap orang memiliki akses untuk menggunakannya. Fungsi *hash* yang dibuat sedemikian sehingga berjalan cepat dan mudah, dapat menerima panjang masukan yang tidak terbatas, namun mengeluarkan keluaran yang mempunyai panjang yang selalu sama yaitu 256 bit.



Gambar 5. Skema Enkripsi SHA
sumber : Diktat IF5054 Kriptografi [4]

Secara garis besar, berikut langkah-langkah yang digunakan untuk menghasilkan nilai *hash (hash value):*

1. Penambahan *padding bits.*
2. Penambahan atau pengurangan pesan awal.
3. Inisialisasi penyangga *(buffer)* MD.
4. Pengolahan pesan dalam blok berukuran 256 bit.



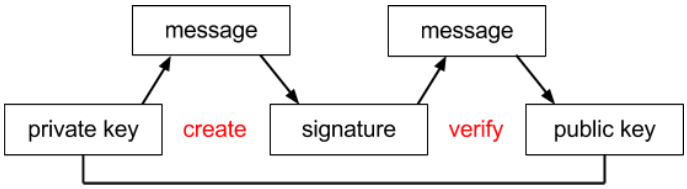
Gambar 6. Skema Pembuatan Sandi dengan SHA
sumber:
https://en.wikipedia.org/wiki/SHA-2#/media/File:SHA-2.svg

SHA-256 sendiri dirancang sedemikian rupa sehingga komputasi tidak mungkin menemukan pesan lain yang berkoresponden dengan keluaran fungsi yang diberikan. Hal ini yang membuat SHA-256 bukanlah fungsi yang bersifat acak, namun fungsi ini merupakan *deterministic function* yang berarti jika pada waktu yang berbeda dengan masukan yang sama, maka keluaran fungsi *hash* akan memberikan hasil yang sama juga.

Fungsi *hash* sendiri terlihat acak karena seolah-olah memang menghasilkan nilai yang acak, seperti potongan kode berikut ini:

```
int generateRandom(char a)
{
  switch (x)
  {
     case ('a') : return 1;
     case ('b') : return 2;
     …
     //fungsi sebenarnya selalu
menghasilkan return value yang sudah unik
untuk masukan tertentu.
  }
}
```

Digital signature atau biasa disebut dengan tanda tangan digital digunakan untuk melakukan verifikasi dari transaksi yang dilakukan benar dilakukan oleh pengguna aslinya. Pada mulanya, kunci pribadi digunakan untuk membuat *digital signature* dengan kombinasi pesan yang disampaikan. Sehingga, *digital signature* tidaklah selalu sama, namun selalu berganti-ganti berdasarkan pesan yang disampaikan. Kemudian, *digital signature* tersebut digunakan untuk uji kesahihan dengan menggunakan kunci publik yang terdapat pada nomor referensi transaksi. Apabila *digital signature* tersebut dikombinasikan dengan pesan yang disampaikan menghasilkan kunci publik yang sama, maka pesan tersebut sahih dan benar dilakukan oleh pengirim, begitu juga sebaliknya. Berikut skema yang dilakukan:



Gambar 7. Skema Validasi Transaksi Bitcoin
sumber:
http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

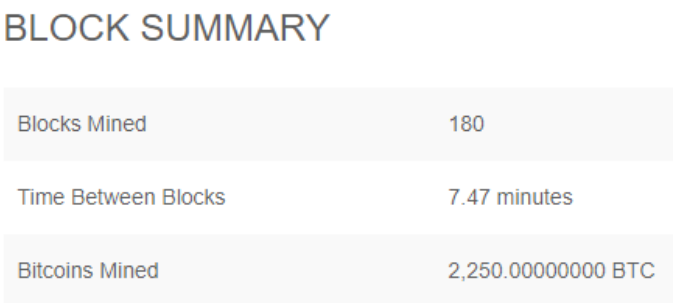
C. Penambangan Bitcoin (Bitcoin Mining)

Seperti yang telah dijelaskan sebelumnya bahwa fungsi *hash* yang dihasilkan oleh fitur keamanan Bitcoin bersifat *deterministic* atau selalu menghasilkan sandi yang sama untuk masukan yang sama. Sementara itu, di lain hal fungsi *hash* yang digunakan bersifat satu arah *(one-way hash)* yang berarti sandi keluaran yang dihasilkan fungsi *hash* tidak dapat dikembalikan menjadi pesan semula *(plaintext)* sedemikian rupa caranya. Padahal, untuk menyambungkan blok-blok transaksi ke rantai blok utama membutuhkan uji kesahihan nomor blok tersebut. Oleh karena itu, dibutuhkan sistem yang dapat melakukan uji kesahihan tersebut.

Satu-satunya cara yang hanya bisa dilakukan ialah dengan mencoba segala kemungkinan pesan yang dapat menghasilkan sandi yang dihasilkan oleh fungsi *hash* tersebut. Hal ini tentu membutuhkan waktu yang sangat lama, jika hanya dilakukan oleh satu komputer saja. SHA-256 memiliki 256 bit yang dapat memuat masing-masing dua kemungkinan yaitu 0 dan 1. Itu berarti ada sebanyak 2^{256} kombinasi yang dapat dihasilkan oleh fungsi *hash* itu sendiri.

Sebagai contoh, kita ingin mencari sandi yang diawali dengan angka 0 sebanyak 20 kali, peluang untuk mendapatkan 20 digit pertama 0 ialah $1/2^{20}$ itu berarti kita butuh sekitar 2^{19} kali percobaan untuk dapat menemukan kemungkinan pesan yang menghasilkan sandi tersebut. Hal ini yang sering disebut juga dengan *cryptographic puzzle* yang merupakan pemecahan matematika yang rumit yang harus diselesaikan oleh komputer. Hal inilah yang menjadi cikal bakal *Bitcoin miners* atau para penambang Bitcoin.

Penambang Bitcoin membantu memecahkan permasalahan matematika dari fungsi *hash* tersebut, tak lain hanya dengan cara "*trial and error"* yang dapat dilakukan. Oleh karena, fungsi *hash* ini dapat diakses oleh seluruh pengguna dimana pun berada, ini membuat siapa pun dapat menjadi penambang Bitcoin. Setiap penambang tercepat yang dapat menyelesaikan permasalahan matematika sebelumnya akan mendapat *reward* beberapa Bitcoin untuknya. Menurut data, penambang Bitcoin dapat menyelesaikan satu blok dalam waktu rata-rata yaitu 7 – 10 menit[7].



Gambar 8.Statistik Rata-Rata Waktu Penyelesaian Bitcoin per 3 Desember 2017 pukul 08.30.
sumber: https://blockchain.info/stats

Semakin lama semakin banyak penambang Bitcoin yang membantu penyelesaian masalah matematika berjalan semakin cepat. Namun, di lain hal, peluang penambang untuk menjadi yang tercepat dalam menyelesaikannya pun semakin berkurang. Oleh karena itu, saat ini banyak penambang bergabung untuk membuat komunitas yang disebut *mining pools.* Dengan menggunakan sistem ini, penambang yang berada dalam komunitas tetap mendapat *reward* yang sesuai dengan usaha yang dilakukannya untuk komunitas.

IV. SIMPULAN

Bitcoin adalah salah satu inovasi *financial technology* yang berbasis *cryptocurrency*. Pembukuan transaksi *(ledger)* dilakukan secara bersama melalui *peer-to-peer connection*, sehingga setiap pengguna menyimpan pembukuan seluruh pengguna lainnya. Sistem keamanan yang digunakan ialah SHA-256 yang bersifat tidak dapat dibalikkan *(non-invertible)* dan unik *(deterministic)*. SHA-256 digunakan sebagai sistem persandian untuk menguji kesahihan transaksi, membuat pengguna tetap anonim, dan lainnya. Pembukuan dilakukan secara blok yang disusun menjadi rantai *(block chain)*. Satu-satunya cara untuk menguji kesahihan transaksi hanyalah dengan mencoba segala kemungkinan yang dapat menghasilkan sandi yang sama. Oleh karena itu, banyak pengguna lain yang menjadi penambang Bitcoin *(Bitcoin miners)* untuk membantu menyelesaikan permasalahan matematika tersebut.

V. UCAPAN TERIMA KASIH

Penulis mengucapkan syukur kepada Allah yang Maha Esa karena berkat rahmatnya lah, sehingga penulis dapat menyelesaikan makalah ini dengan baik dan lancar. Penulis juga ingin mengucapkan terima kasih untuk Bapak Dr. Ir. Rinaldi Munir, M.T., Bapak Dr. Judhi Santoso, dan Ibu Dra. Harlili S.,M.Sc. selaku dosen mata kuliah Matematika Diskrit yang telah memberikan bimbingan dan ilmu dalam penulisan makalah ini. Penulis juga berterima kasih kepada semua pihak yang tidak dapat saya tulis seluruhnya di bagian ini, terutama untuk penulis-penulis yang tulisannya menjadi referensi di dalam penulisan makalah ini.

REFERENSI

[1] http://www.bi.go.id/id/ruang-media/siaran-pers/Pages/sp_160614.aspx diakses pada tanggal 3 Desember 2017 pukul 16.05.
[2] http://money.cnn.com/infographic/technology/what-is-bitcoin/ diakses pada tanggal 3 Desember 2017 pukul 23.40.
[3] Rinaldi Munir, Matematika Diskrit, Bandung : Penerbit Informatika, Palasari.
[4] Rinaldi Munir, Diktat IF5054 Kriptografi, 2004, Bandung : Penerbit Departemen Teknik Informatika.
[5] http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html diakses pada tanggal 3 Desember 2017 pukul 13.00.
[6] https://www.slideshare.net/RoziqBahtiar/kriptografi diakses pada tanggal 2 Desember 2017 pukul 16.07.
[7] https://blockchain.info/stats diakses pada tanggal 2 Desember 2017 pukul 22.45.
[8] https://bitcoin.org/bitcoin.pdf diakses pada tanggal 1 Desember 2017 pukul 11.35.

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, 3 Desember 2017

Muhammad Alfian Rasyidin
13516104