Analisis Keamanan Bitcoin

Reinhard Denis Najogie | 13509097
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509097@stei.itb.ac.id

Abstrak — Bitcoin adalah salah satu implementasi pertama dari *cyptocurrency* atau mata uang *digital*. Penggunaannya semakin meningkat dalam beberapa tahun terakhir seiring dengan meningkatnya volume transaksi online yang memerlukan mata uang *digital*. Diciptakan pada tahun 2009, Bitcoin merupakan mata uang yang unik dimana tidak ada suatu badan pusat yang mengatur transaksi maupun penerbitannya. Bitcoin bersifat open source dan peer-to-peer. Open source artinya sistem mata uang ini dikembangkan secara bersama-sama oleh siapapun yang mau berkontribusi. Peer-to-peer artinya setiap transaksi dicatat oleh jaringan komputer yang terhubung secara langsung layaknya sistem *torrent,* tidak melalui suatu pihak penengah seperti bank atau merchant seperti yang terjadi pada kebanyakan sistem pembayaran online yang ada sekarang (paypal, kartu kredit, dsb.). Untuk "menerbitkan" bitcoin baru, perlu dilakukan proses yang dinamakan bitcoin mining, yaitu dimana komputer dengan hardware yang kuat digunakan untuk "menambang" bitcoin baru. Proses penambangan yang dimaksud adalah komputer harus menyelesaikan permasalahan matematika yang memerlukan komputasi yang intensif. Jumlah bitcoin yang bisa beredar pun terbatas untuk menghindari penurunan nilai mata uang bitcoin ini. Dalam makalah ini akan dibahas aspek-aspek keamanan yang mendasari operasi dari bitcoin. Mulai dari keamanan dan privasi akun, bagaimana sistem *digital signature* pada bitcoin, bagaimana bitcoin mengatasi masalah *double spending*, bagaimana bitcoin *mining* bekerja, serta bagaimana bitcoin mengatasi *fraud* dari pengguna yang ingin berbuat curang.

Kata Kunci—bitcoin, cryptocurrency, bitcoin mining, *double* spending

I. PENDAHULUAN

Penggunaan internet sebagai sarana transaksi bisnis sudah terjadi sejak awal perkembangan teknologi internet itu sendiri. Internet yang pada awalnya dibuat untuk sarana peneliti untuk *sharing* hasil penelitiannya, ternyata berkembang penggunaannya sampai menjadi media hiburan bahkan transaksi jual-beli seperti yang terjadi sekarang ini.

Untuk melakukan transaksi jual-beli pada internet, diperlukan cara untuk bertukar mata uang seperti yang ada pada transaksi jual-beli pada dunia nyata. Pada awal perkembangannya, cara yang banyak diadopsi adalah dengan menggunakan kartu kredit sebagai alat pembayaran transaksi melalui internet. Seorang pembeli harus memberikan detail informasi kartu kredit nya kepada penjual. Penjual lalu mengkonfirmasi informasi tersebut kepada penyedia jasa kartu kredit untuk kemudia memproses transaksi atau memberitahu konfirmasi gagal. Tahap berikutnya dari perkembangan teknologi pembayaran *digital* adalah adanya pihak yang memfasilitasi penyimpanan uang secara *digital*. Contoh teknologi yang paling terkenal dan banyak digunakan adalah Paypal[1]. Paypal berperan sebagai "dompet *digital*". Paypal bukanlah bank dimana pemilik akun akan mendapatkan bunga atas simpanan uangnya. Paypal sebenarnya adalah cara lebih aman untuk menggunakan kartu kredit. Dengan Paypal, orang tidak perlu memberitahu informasi kartu kredit nya kepada penjual, tetapi hanya alamat Paypal nya saja. Untuk mengisi uang pada Paypal, orang tetap harus menggunakan media lain seperti kartu kredit. Penggunaan pihak ketiga pada transaksi jual-beli melalui internet (kartu kredit, Paypal) menyebabkan adanya biaya tambahan sebagai jasa untuk pihak ketiga tersebut. *Cryptocurrency* seperti bitcoin adalah salah satu solusi masalah biaya transaksi ini, dimana biaya transaksi pada bitcoin sangat kecil atau bisa dianggap tidak ada. Hal ini menggambarkan transaksi pada dunia nyata dimana pembeli memberikan uang langsung kepada penjual dan tidak ada biaya transaksi untuk perantara.

Dalam makalah ini akan dibahas dasar teori yang mendasari pembuatan mata uang bitcoin seperti teknik-teknik kriptografi yang digunakan, arsitektur sistem yang mendasari distribusi blok transaksi yang telah terjadi, resiko keamanan transaksi dengan bitcoin, serta saran untuk pengguna serta pengembangan bitcoin pada masa yang akan datang.

II. DASAR TEORI

Pada bagian ini akan dijelaskan istilah-istilah yang ada pada mata uang bitcoin serta arsitektur sistem secara

[1] www.paypal.com

umum.

A. Istilah dalam Bitcoin

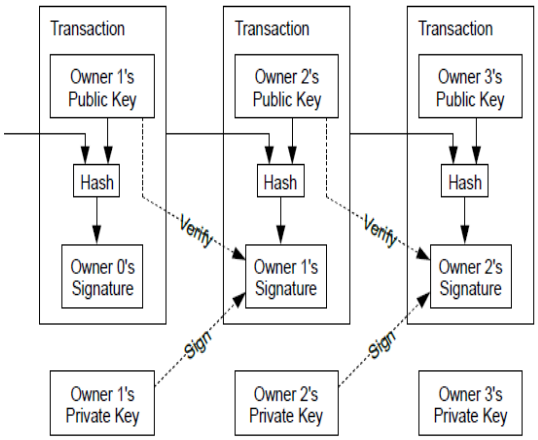
Berikut adalah penjelasan singkat tentang istilah yang kerap digunakan dalam transaksi bitcoin, seperti yang dijelaskan pada [1]:

1. *Address*
   Acuan untuk seorang pengguna bitcoin. Layaknya nomor kartu kredit atau alamat surel pada pengguna Paypal.
2. *Block Chain*
   Rekaman semua kegiatan transaksi yang ada pada bitcoin yang terbuka untuk publik sehingga bisa dilihat oleh siapapun.
3. *Block*
   Bagian dari block chain yang mencatat transaksi yang terjadi untuk periode waktu tertentu. Saat ini rata-rata satu block baru dibuat setiap kurun waktu 10 menit.
4. BTC
   Singkatan mata uang bitcoin, seperti USD untuk US dollar dan IDR untuk rupiah Indonesia.
5. *Confirmation*
   Verifikasi transaksi oleh jaringan. Pada umumnya satu verifikasi cukup, akan tetapi untuk transaksi yang melibatkan uang yang besar disarankan untuk menunggu hingga ada minimal 6 verifikasi transaksi dari jaringan.
6. *Cryptography*
   Merupakan cabang matematika dan ilmu komputer yang mendasari aspek-aspek keamanan bitcoin.
7. *Double Spend*
   Menggunakan satu uang berulang kali. Merupakan salah satu masalah utama yang diselesaikan oleh bitcoin.
8. *Hash Rate*
   Satuan kekuatan pemrosesan transaksi oleh jaringan bitcoin. Jaringan bitcoin menggunakan banyak resource untuk melakukan operasi kriptografi. 10 TH/s berarti jaringan mampu melakukan 10 triliun hitungan per detik.
9. *Mining*
   Proses yang dilakukan oleh komputer khusus pada jaringan bitcoin (bitcoin miner) untuk melakukan komputasi yang berguna untuk keberjalanan bictoin seperti konfirmasi transaksi dan menjaga keamanan bitcoin. Bitcoin miner berhak mendapatkan biaya transaksi serta bitcoin baru sebagai jasa untuk resource yang sudah digunakan untuk keberjalanan jaringan bitcoin.
10. *P2P*
    Peer-to-peer adalah sistem yang bekerja secara kolektif dimana setiap pengguna dapat langsung berinteraksi dengan pengguna lain. Tidak menggunakan pihak ketiga seperti bank seperti transaksi yang terjadi pada dunia nyata.
11. *Private Key*
    Merupakan kunci kriptografi yang digunakan untuk melakukan *signature*. Setiap bitcoin address memiliki *private key* nya sendiri.
12. *Signature*
    Salah satu istilah dalam kriptografi yang terkadang juga disebut *digital signature*. Berguna untuk membuktikan kepemilikian kita akan sejumlah bitcoin. Setiap transaksi dalam bitcoin pengguna akan memberikan *signature* nya.
13. *Wallet*
    Seperti dompet di dunia nyata. Wallet dalam bitcoin mengandung *private key* yang memungkinkan seseorang membelanjakan bitcoin yang dialokasikan pada bitcoin address pada block chain. Wallet dapat berupa software desktop yang dibangun oleh komunitas bitcoin, atau berupa web wallet yang berupa pihak ketiga yang menawarkan jasa wallet online bitcoin.

B. Arsitektur Bitcoin

Satoshi Nakamoto, pencipta bitcoin, dalam *white paper* nya [2] menjelaskan teori yang digunakan dalam mendesain sistem mata uang bitcoin. Pada bagian ini akan dijelaskan teori tentang transaksi, *timestamp server*, serta *proof-of-work* yang menjadi dasar keamanan sistem bitcoin.

Sebuah koin dalam bitcoin didefinisikan sebagai rantaian *digital signature*. Transaksi terjadi dengan cara melakukan *digital signature* pada hash dari transaksi terdahulu dan public *key* dari penerima koin. Penerima selanjutnya memverifikasi *digital signature* yang diterima untuk memastikan kepemilikan koin tersebut.

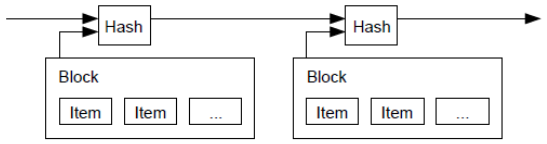


Gambar 1 – Transaksi dalam Bitcoin. Sumber: [2]

Satu permasalahan dengan sistem transaksi seperti ini adalah penerima koin tidak dapat memastikan bahwa pengirim tidak mengirim koin yang sama lebih dari satu kali (*double-spend*). Pada sistem transaksi konvensional, solusi untuk permasalahan ini adalah memberikan kepercayaan kepada pihak ketiga seperti bank untuk

mencatat transaksi dan menyelesaikan sengketa yang mungkin terjadi diantara pihak pemberi dan penerima. Pada bitcoin, hal ini tidak mungkina dilakukan karena tidak ada badan/organisasi yang meregulasi peredaran bitcoin. Oleh karena itu, solusinya adalah dengan melakukan pencatatan semua transaksi bitcoin yang pernah terjadi dan menyediakan catatan ini terbuka untuk publik. Untuk mencegah *double-spend*, diperlukan pengecekan pada catatan transaksi ini apakah transaksi pengiriman koin yang dimaksud sudah pernah terjadi berdasarkan catatan transaksi publik.

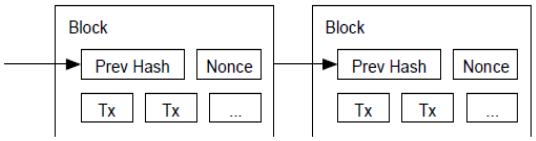
Solusi pencatatan transaksi secara publik diimplementasikan dengan *timestamp server*. Gambar 2 di bawah menggambarkan cara *timestamp server* bekerja.



Gambar 2 – *Timestamp server*. Sumber: [2]

Timestamp server bekerja dengan cara mengambil nilai hash dari block berisi item yang akan di-*timestamp* serta nilai hash dari *timestamp* sebelumnya. Nilai hash keluaran ini selanjutnya akan digunakan pada hash *timestamp* selanjutnya, dan demikian seterusnya, membentuk *timestamp* chain. Nilai hash ini dicatat dan dapat diakses oleh publik.

Implementasi *timestamp server* sendiri memerlukan *proof-of-work* sebagai logika dasar bagaimana sistem dapat bekerja dengan baik secara terdistribusi atau peer-to-peer. Ide dasar *proof-of-work* pada sistem bitcoin adalah mencari nilai yang jika di-hash dengan algoritma tertentu (seperti SHA-256), nilai hasil hashnya dimulai dengan bit 0.

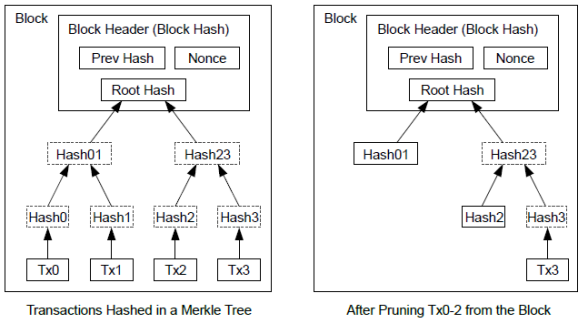


Gambar 3 – *Proof-of-work timestamp server*. Sumber: [2]

Proof-of-work juga menjadi landasan decision making dalam proses confirmation pada sistem bitcoin. *Proof-of-work* memiliki prinsip one-CPU-one-vote, yang berarti voting berdasarkan kekuatan CPU mayoritas. Jika dalam jaringan lebih banyak CPU yang bekerja secara jujur, maka rantai blok yang benar akan berkembang lebih cepat dibandingkan rantaian yang mungkin menyaingi (rantian blok dari *cracker*). *Cracker* yang ingin mengacaukan rantaian blok harus mengulangi *proof-of-work* dari awal blok hingga blok terakhir dan mengalahkan panjang rantai dari blok yang dikelola oleh CPU yang jujur. Dalam bagian analisis, akan ditunjukkan bahwa probabilitas seorang *cracker* untuk melakukan hal ini mendekati nol seiring dengan bertambahnya jumlah blok pada sistem.

Untuk menyesuaikan dengan kecepatan hardware yang ada sekarang, *proof-of-work* akan meningkatkan kesulitan pembuatan blok baru dengan membatasi jumlah blok yang dapat dibangkitkan setiap jamnya. Hal ini dilakukan untuk menghindari pembangkitan blok yang terlalu cepat dan dapat menurunkan nilai bitcoin.

Bitcoin menyimpan seluruh data transaksi yang pernah terjadi. Hal ini lantas menimbulkan pertanyaan tentang bagaimana caranya space pada komputer user cukup untuk menampung semua data transaksi bitcoin yang pernah terjadi. Bitcoin menyelesaikan masalah ini dengan menggunakan struktur data bernama Merkle Tree. Logika dasar penggunaan struktur data ini adalah data transaksi yang lebih lama dapat dihapus dan disimpan hash-nya saja. Proses ini digambarkan dengan gambar di bawah ini.



Gambar 4 – Penghapusan data transaksi. Sumber: [2]

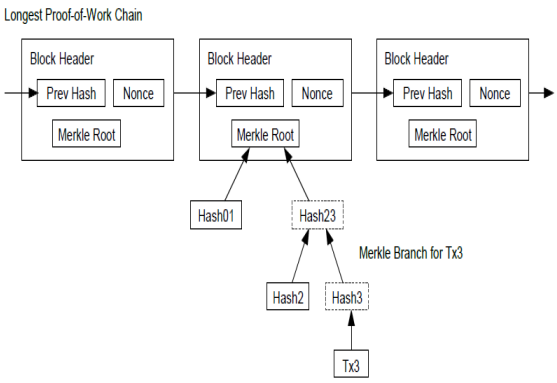
Dapat dilihat pada Gambar 4 bagaimana transaksi 0-2 dihapus dari disk dan meninggalkan nilai hashnya saja. Sebuah blok header kosong berukuran kurang lebih 80 byte. Jika blok dibuat setiap 10 menit, maka total space yang diperlukan selama setahun menjadi 80 * 6 * 24 * 365 = 4.2 MB. Ukuran ini tentunya dapat diterima dengan kapasitas storage yang ada pada kebanyakan komputer saat ini.

III. Analisis Keamanan Bitcoin

Pada bagian ini dibahas keamanan verifikasi transaksi bitcoin, aspek privasi bitcoin, serta perhitungan kemungkinan bitcoin berhasil diserang.

A. Verifikasi transaksi pada bitcoin

Verifikasi transaksi pada bitcoin, secara sederhana, dapat digambarkan seperti pada gambar di bawah ini.



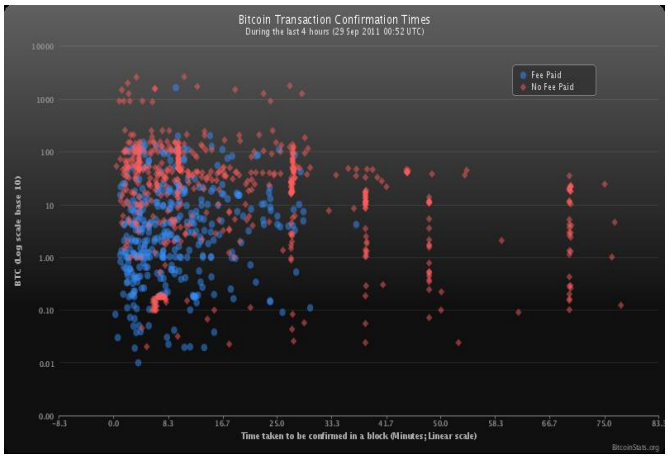
Gambar 4 – Verifikasi transaksi. Sumber: [2]

Verifikasi pada bitcoin dapat dilakukan tanpa harus menghubungi semua komputer yang terhubung pada jaringan bitcoin. Seorang pengguna hanya perlu menyimpan salinan block header dari rantai *proof-of-work* terpanjang. Rantai ini didapatkan dari node-node yang terhubung dengan jaringan komputer bitcoin. Dari proses ini juga didapatkan cabang Merkle Tree yang terhubung dengan transaksi dengan blok tempat transaksi itu dicatat (memiliki *timestamp*).

Menurut Satoshi [2], proses verifikasi seperti ini aman selama komputer-komputer pada jaringan bitcoin secara jujur lebih banyak daripada komputer *cracker*. Apabila *cracker* berhasil mengalahkan kekuatan komputer yang ada pada jaringan bitcoin, maka *cracker* tersebut dapat membuat transaksi palsu dengan cara membuat block header palsu pada rantai blok yang tercatat.

Walaupun teknik ini terlihat rentan serangan karena bergantung pada banyaknya komputer yang jujur dan membantu keberjalanan jaringan bitcoin, akan tetapi pada implementasinya verifikasi dengan teknik ini terbukti dapat berjalan dengan baik. Belum ada kasus mengenai kesalahan verifikasi transaksi yang tercatat selama bitcoin beroperasi (hingga makalah ini dibuat, Mei 2013).

Hal yang mendasari banyaknya komputer dalam jaringan bitcoin yang bertindak jujur daripada komputer yang bersifat *cracker* adalah proses bitcoin mining. Bitcoin mining adalah proses yang meliputi pembangkitan blok yang baru untuk pencatatan transaksi bitcoin. Siapa saja bisa menjadi bitcoin miner, asalkan memiliki perangkat keras yang mampu memproses transaksi bitcoin yang begitu banyaknya setiap hari penuh selama 24 jam. Atas jasa pihak-pihak yang melakukan bitcoin mining, pihak-pihak ini menerima biaya transaksi. Transaksi dalam bitcoin memang tidak mengharuskan pembayaran biaya transaksi kepada bitcoin miner, akan tetapi pengguna yang memilih untuk membayarkan biaya transaksi akan mendapatkan prioritas untuk mendapatkan konfirmasi transaksi lebih cepat daripada pengguna yang memilih untuk tidak membayar biaya transaksi. Selain mendapatkan biaya transaksi, keuntungan lain yang didapatkan oleh bitcoin miner adalah mereka berhak mendapatkan bitcoin yang baru diterbitkan. Namun penerbitan bitcoin baru kecepatannya semakin lambat dan akan berhenti pada jumlah sekitar 21 juta BTC yang diperkirakan akan dicapai pada tahun 2140.



Gambar 5 – Grafik waktu pemrosesan transaksi terhadap nominal transaksi. Sumber: https://en.bitcoin.it/wiki/FAQ

Pada gambar di atas terlihat bahwa rata-rata waktu pemrosesan transaksi adalah 10 menit. Titik merah menandakan transaksi yang tidak membayar biaya transaksi, titik biru menandakan transaksi yang membayar biaya transaksi. Terlihat juga bahwa transaksi yang membayar biaya rata-rata lebih cepat diproses oleh jaringan komputer bitcoin.

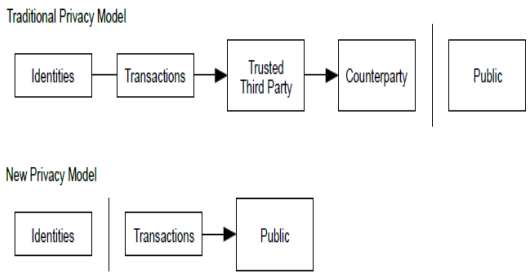
B. Privasi pada bitcoin

Privasi atau kerahasiaan data pengguna dilakukan dengan cara yang unik pada bitcoin. Berbeda dengan sistem transaksi konvensional dimana pihak ketiga seperti bank menyimpan data-data seorang pemilik akun secara detail, bitcoin sama sekali tidak menyimpan data pribadi penggunanya. Yang diperlukan untuk melakukan transaksi antara pemberi dan penerima koin adalah alamat masing-masing yang berupa nilai hash seperti:

1J8YqLewfHqm1zweGHZoagkWPfBUT6eX7Q

Secara default bitcoin juga mengganti alamat pengguna dengan nilai hash baru yang berbeda dari alamat sebelumnya. Hal ini semakin menambah anonimitas pengguna bitcoin, dimana seorang secara default dan disarankan menggunakan banyak akun. Cara seperti ini tentu tidak dapat digunakan pada dunia nyata karena akun bank biasanya terhubung dengan nama pemilik akun tersebut, seperti yang biasa ditemui (terutama di Indonesia) ketika seseorang ingin melakukan transfer dari satu akun ke akun lain.

Perbandingan sistem kerahasiaan privasi pada transaksi konvensional dengan transaksi pada sistem bitcoin dapat dilihat pada gambar di bawah ini.



Gambar 6 – Privasi pada bitcoin. Sumber: [2]

Pada gambar di atas terlihat perbedaan konsep privasi pada sistem transaksi konvensional dengan sistem bitcoin. Pada sistem transaksi konvensional, identitas, transaksi, serta pihak-pihak yang terlibat dalam transaksi disembunyikan dari publik. Seorang yang mengirimkan sejumlah uang pada orang lain tidak akan diketahui orang luar yang tidak terlibat pada transaksi tersebut, sehingga sebuah transaksi hanya diketahui oleh pengirim, penerima, dan pihak ketiga. Tentunya hal ini memiliki pengecualian pada kasus tertentu (pemeriksaan akun atas tuntutan korupsi, dsb.). Pada bitcoin, semua transaksi yang pernah terjadi dirilis ke publik, sehingga siapapun dapat mengaksesnya. Siapapun akan mengetahui bahwa A melakukan transfer sejumlah koin ke B, akan tetapi A dan B itu sendiri tidak diketahui identitas aslinya pada kehidupan nyata.

Fenomena ini kemudian menimbulkan pertanyaan, apakah dengan begini bitcoin menjadi pilihan para kriminal sebagai sarana transaksi jual-beli barang ilegal? Belum tentu, sesuai dengan laporan Federal Bureau of Investigation (FBI) pada [3], bitcoin diyakini tidak menjadi pilihan kriminal untuk melakukan pencucian uang. Pihak yang berwajib diyakini sudah menggunakan teknik lanjut untuk menganalisis rekaman transaksi bitcoin untuk menemukan transaksi kriminal [4]. Selain itu, sistem transaksi bitcoin yang bersifat anonymous secara otomatis menghindarkan pengguna dari tindakan pencurian identitas seperti yang kerap terjadi pada sistem transaksi seperti kartu kredit.

C. Perhitungan kemungkinan bitcoin berhasil diserang

Telah disebutkan sebelumnya bahwa keberhasilan bitcoin bergantung pada jumlah komputer/CPU yang bekerjasama dengan jujur untuk melakukan operasi transaksi pada bitcoin. Bitcoin bisa gagal dalam kasus jumlah komputer pada jaringan yang menyerang lebih banyak daripada jumlah komputer yang mempertahankan bitcoin.

Satoshi pada [2] menjelaskan perhitungan probabilitas sebuah serangan dapat berhasil menghancurkan sistem transaksi bitcoin.

Skenario yang dianalisis adalah seorang *cracker* ingin membangkitkan block chain secara lebih cepat daripada block chain yang dihasilkan oleh komputer yang jujur. Probabilitas dari seorang *cracker* untuk mengejar pembangkitan block dapat dimodelkan dengan permasalahan Gambler's ruin [5] dimana seorang penjudi memiliki modal tidak terbatas memulai permainan dalam kondisi rugi dan mencoba bermain hingga dapat mencapai breakeven (balik modal). Perhitungannya dirumuskan sebagai berikut [2]:

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

Dimana

p = probabilitas sebuah node yang jujur membangkitkan blok berikutnya

q = probabilitas *cracker* membangkitkan blok berikutnya

q_z = probabilitas *cracker* mengejar ketertinggalan z blok

Dengan asumsi p > q, nilai q_z turun secara eksponensial terhadap jumlah blok yang harus dikejar oleh *cracker*. Dengan semakin bertambahnya jumlah blok yang harus dikejar, kemungkinan *cracker* berhasil membuat block chain yang lebih panjang mendekati 0.

Selanjutnya yang perlu diperhitungkan adalah waktu yang diperlukan sebelum melakukan transaksi baru. Seorang penipu dapat berkedok sebagai pengirim uang, lalu sebelum transaksi selesai dan penerima menerima uang, si penipu membatalkan transaksi. Sistem akan memperingatkan penerima jika hal seperti ini terjadi. Si penipu tentu saja berharap peringatan ini sudah terlambat. Penerima dalam hal ini akan membangkitkan *key* baru dan memberikan public *key* nya kepada pengirim sebelum melakukan *signature*. Hal ini dilakukan untuk mencegah pengirim mempersiapkan block chain palsu sebelumnya dan berhasil mengalahkan panjang block chain yang asli (yang mana kemungkinannya sangat kecil) dan melakukan transaksi saat itu juga. Penerima menunggu hingga transaksi telah tercatat dalam sebuah blok dan z buah block telah dibuat dan terhubung setelah blok tersebut. Perhitungan matematika selengkapnya dapat dilihat, pada [2], yang mana pad akhirnya menghasilkan rumus berikut.

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Yang setelah dibuat programnya dan dijalankan, terlihat iterasi nilai probabilitas yang semakin mengecil secara eksponensial seperti dibawah ini [2]:

q=0.1
z=0 P=1.0000000

z=1 P=0.2045873
z=2 P=0.0509779
z=3 P=0.0131722
z=4 P=0.0034552
z=5 P=0.0009137
z=6 P=0.0002428
z=7 P=0.0000647
z=8 P=0.0000173
z=9 P=0.0000046
z=10 P=0.0000012

IV. KESIMPULAN DAN SARAN

Dari hasil studi literatur dan analisis yang telah dilakukan, terlihat bahwa bitcoin merupakan salah satu implementasi pertama dan tersukses dari prinsip *cryptocurrency*. Adaptasi oleh perusahaan-perusahaan besar memang masih minim, tapi penggunaan oleh individual terus meningkat dan jumlah layanan online wallet juga terus bertambah. Sorotan media internasional juga mempengaruhi popularitas bitcoin sebagai mata uang *digital* yang diharapkan bisa menggantikan peran kartu kredit atau pihak ketiga seperti paypal untuk bertransaksi melalui internet.

Dari sudut pandang kriptografi, bitcoin secara teori dan praktik terbukti kuat. Implementasi kriptografi pada sistem terdistribusi berhasil pada sistem bitcoin. Hingga makalah ini ditulis, hanya ada 1 masalah keamanan penting yang dialami bitcoin [6] yang terletak pada masalah implementasi/*coding* yaitu masalah value overflow. Kasus-kasus lain seperti pencurian bitcoin banyak diakibatkan oleh kelalaian pengguna atau online wallet yang diserang oleh *cracker*.

Salah satu alasan adaptasi bitcoin cenderung lambat adalah cara kerja bitcoin yang tidak biasa dan tidak diatur oleh lembaga keuangan manapun. Orang awam dapat melakukan kesalahan seperti tidak sengaja mempublikasikan *private key* nya, dsb. sehingga pengguna baru bisa menjadi ragu untuk menggunakan teknologi bitcoin. Oleh karena itu, adanya organisasi non-profit yang mempromosikan penggunaan bitcoin akan sangat membantu adaptasi bitcoin oleh pengguna baru dan pelaku bisnis besar.

REFERENSI

[1] http://bitcoin.org/en/vocabulary#block. Diakses 18 Mei 2013.

[2] S. (2008). Bitcoin: A peer-to-peer electronic cash system. Consulted, 1, 2012.

[3] Federal Bureau of Investigation (2012). Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity.

[4] http://bitcoin.org/en/bitcoin-for-press. Diakses 18 Mei 2013.

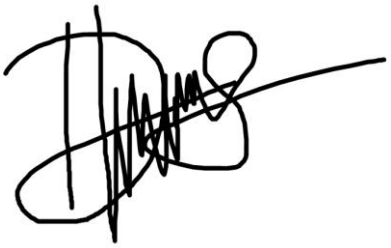
[5] http://math.ucsd.edu/~anistat/gamblers_ruin.html. Diakses 18 Mei 2013.

[6] http://bitcoin.org/en/about. Diakses 18 Mei 2013.

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, 18 Mei 2013



ttd

Reinhard Denis Najogie | 13509097