Bitcoin: Cara Kerja dan Perbandingannya dengan Mata Uang Konvensional

Damiann Muhammad Mangan - 13510071
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510071@std.stei.itb.ac.id

***Abstract*—Makalah ini akan membahas mengenai Bitcoin; mata uang digital pertama yang menggunakan sistem *peer-to-peer*. Penulis akan mengelaborasikan baik apa itu Bitcoin, bagaimana cara kerjanya, dan apa acuan pengembangannya. Penulis juga akan memaparkan opini penulis pada beberapa sudut pandang terhadap Bitcoin, serta kelebihan dan kekurangannya dibandingkan mata uang nasional.**

***Index Terms*—kriptografi asimetri, hash function, hashcash, proof-of-work, digital currency, peer-to-peer, cryptocurrency**

I. Pendahuluan

Sejak sebelum tahun masehi mulai dijadikan sebagai patokan perhitungan waktu, manusia sudah menggunakan sistem jual beli; sistem yang jauh lebih efisien dibanding sistem barter. Berbeda dengan sistem barter, sistem yang menuntut pertukaran terjadi apabila pihak pertama memiliki barang yang diinginkan oleh pihak kedua dan sebaliknya (contoh: Alice memiliki kucing dan ingin menukarnya dengan anjing, sedangkan Bob yang memiliki anjing menginginkan burung; karena *supply* dan *demand* tidak cocok, barter tidak terjadi), sistem mata uang memberi keleluasaan pemilik barang untuk menukarnya dengan sebuah media antara, yang merupakan uang, untuk nantinya bisa ditukar dengan barang yang diinginkan (contoh: Alice memiliki kucing dan ingin menukarnya dengan anjing, maka ia menukar kucingnya dengan uang; Bob yang memiliki anjing tidak menolak untuk menukar anjingnya dengan uang, karena nantinya uang dapat digunakan untuk bertukar dengan hal yang ia inginkan).

Masing-masing negara menggunakan suatu mata uang sesuai dengan kesepakatan negara dan masyarakatnya, seperti Indonesia menggunakan mata uang Rupiah, Australia menggunakan mata uang Dolar Australia, ataupun mata uang Euro yang digunakan oleh Uni Eropa yang terdiri dari 17 negara di Benua Eropa.

Uang sendiri adalah medium pertukaran yang memiliki nilai. Dalam penggunaannya, dapat digunakan koin, kertas, maupun nota dari bank untuk merepresentasikan uang. Sejak adanya era digital, uang dapat direpresentasi dalam bentuk saldo di bank ataupun virtual, mata uang yang memiliki lingkungan virtual dan beregulasi dan terikat oleh suatu jasa, seperti *game*.

Mata uang digital atau *digital currency*, berbeda dengan uang dalam bentuk saldo ataupun uang virtual, merupakan mata uang yang memiliki bentuk digital dan dapat digunakan untuk bertransaksi dengan barang di dunia nyata. Jenis mata uang ini mulai bermunculan sejak tahun 1996 hingga sekarang.

II. Cryptocurrency

Cryptocurrency adalah mata uang digital yang menggantungkan keamanannya dengan kriptografi. Dalam makalah ini, penulis hanya akan berfokus kepada Bitcoin, *cryptocurrency* terbesar. Dibawah ini merupakan contoh-contoh *cryptocurrency* dan keunikan masing-masing.

A. Bitcoin

Mata uang digital yang merupakan pokok pembahasan di makalah ini menggunakan *hashcash proof-of-work* untuk keamanannya dalam bertransaksi. Baik *hashcash* maupun *proof-of-work* akan dibahas di bagian selanjutnya.

B. Litecoin

Litecoin merupakan *cryptocurrency* yang memiliki mekanisme serupa dan berdasarkan Bitcoin. Pengembang membentuk mata uang ini bermaksud untuk memperbaiki kekurangan Bitcoin dengan menggunakan *scrypt,* algoritma buatan Colin Percival, yang diklaim mampu mengurangi keuntungan penggunaan GPU, FPGA, dan ASIC dalam menambang dibandingkan CPU, dalam berjalannya *proof-of-work*.

C. PPcoin

PPcoin dibuat oleh pengembang yang bermaksud untuk memperbaiki Bitcoin dengan mengaplikasikan *proof-of-stake* bersamaan dengan *proof-of-work*. *Proof-of-stake* menggunakan presentasi jumlah BTC (satuan uang bitcoin) yang ia punya sebagai berat presentasi untuk *vote* apakah suatu transaksi sah atau tidak.

Berikut ini adalah tabel perbandingan besarnya pasar *cryptocurrency* yang memiliki sistem *peer-to-peer*.

Mata uang	Besarnya pasar	Website
Bitcoin	~1 Milyar USD	bitcoin.org
Litecoin	~38 Juta USD	litecoin.org
PPcoin	~4 Juta USD	ppcoin.org

Tabel 1. Perbandingan besar pasar *cryptocurrency* terbesar

III. KRIPTOGRAFI ASIMETRI

Kriptografi asimetri merupakan teknik yang pengubahan pesan bermakna dengan kunci privat, sehingga terbentuk *ciphertext* yang hanya bisa didekripsikan dengan kunci publik; nilai kunci publik berubah sesuai dengan nilai kunci privat. Hal ini dapat dicapai dengan memanfaatkan berbagai kenyataan-kenyataan matematis pada bilangan bulat; seperti fungsi logaritmik diskrit dengan modulo, ataupun penggunaan teorema Fermat. Berikut ini adalah nama-nama kriptografi asimetri yang marak dijumpai saat ini, algoritma RSA, algoritma ElGamal, ataupun algoritma *Elliptical Curve*.

III. FUNGSI HASH

Fungsi *hash* merupakan fungsi yang menerima masukan *string* sepanjang apapun dan akan mengembalikan *message digest* dengan panjang yang tetap. Fungsi *hash* memiliki sifat satu arah, karena *message digest* memiliki panjang yang tetap dan masukan dapat memiliki panjang yang bervariasi. Fungsi *hash* tidak tepat untuk disebut sebuah proses enkripsi, karena tidak memiliki kunci, walaupun *message digest* sudah tidak memiliki makna. Sebagai gantinya, fungsi *hash* memiliki fungsi sendiri, yaitu:

- Mampu menjaga integritas data;
  karena fungsi *hash* sangat peka dengan perubahan 1 bit pada pesan. Apabila ada pihak yang mengubah pesan, dapat secara dini dideteksi.

- Menghemat waktu pengiriman;
  untuk memeriksa sebuah salinan arsip, cukup dikirim *message digest* dari arsip utama untuk nantinya digunakan sebagai verifikasi dengan dibandingkan dengan *message digest* arsip salinan.

- Menormalkan panjang data yang beragam;
  basis data tempat penyimpanan *password* cukup menyimpan hasil *hash* dari *password*-nya. Selain memberi keamanan tambahan karena *message digest* tidak bisa dibaca ataupun dikembalikan ke nilai aslinya, panjang data yang disimpan pun menjadi seragam dan menghemat memori.

Berikut ini merupakan contoh perbandingan keluaran fungsi *hash* MD5 untuk memperlihatkan kepekaannya.

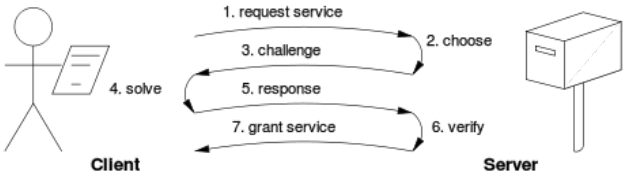
```
string:
123456789
hasil:
25f9e794323b453885f5181f1b624d0b

string:
123456788
hasil:
f5f091a697cd91c4170cda38e81f4b1a
```

III. PROOF-OF-WORK

Proof-of-work adalah sebuah fungsi atau protokol yang diharapkan mampu mengagalkan *denial of service* ataupun berbagai penggunaan jasa berlebihan seperti *spam* dengan menuntut sebuah pekerjaan dilakukan oleh pengguna/pengaju jasa sebelum menggunakan jasa tersebut, biasanya mengakibatkan waktu proses saat dilakukan komputer. Kunci dari fungsi ini adalah asimetri; pekerjaan tersebut haruslah sulit (tetapi dapat dilakukan) dari pihak pengaju tetapi mudah diperiksa oleh pihak pemberi jasa. *Proof-of-work* berbeda dengan CAPTCHA, yang dimaksudkan untuk diselesaikan oleh manusia.

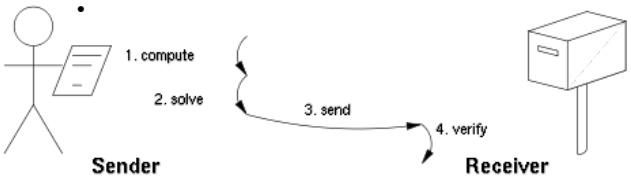
Ada dua tipe protokol *proof-of-work*,

- *Challenge-response*
  Setelah *client* dan *server* terhubung, *server* menentukan dan memberikan tantangan, contohnya suatu string yang memiliki kriteria tertentu. *Client* harus melakukan perhitungan untuk menyelesaikan tantangan tersebut sesuai kriterianya agar selanjutnya *client* dapat menggunakan jasa. *Server* akan memberikan jasa apabila jawaban yang diberikan *client* memenuhi kriteria yang telah diberikan. Berikut ini merupakan ilustrasinya.



Gambar 1. Ilustrasi *challenge-response*

- *Solution-verification*
  Tantangan yang perlu diselesaikan oleh pihak *client* sudah dapat diakses kriteria yang diperlukan oleh umum. Sehingga cukup diberikan ke *server* untuk nantinya diperiksa dan *server* akan memberikan layanan yang telah dijanjikan.



Gambar 2. Ilustrasi *solution-verification*

IV. HASHCASH

Hashcash adalah jenis *proof-of-work* yang diimplementasikan di Bitcoin; selain itu protokol ini juga diaplikasikan untuk menyaring surel yang datang ataupun pesan yang ditujukan ke alamat IP (*Internet Protocol*). Metode ini dilakukan dengan menambahkan teks pada *header* pesan yang sudah memiliki bentuk, agar saat dilakukan fungsi *hash*, dapat dihasilkan *message digest* yang sesuai dengan kriteria; Bitcoin menggunakan SHA-256 sebagai fungsi *hash*-nya. Pada paragraf selanjutnya, penulis akan memberikan contoh penggunaan protokol *hashcash*.

Header dari pesan memiliki bentuk seperti ini:

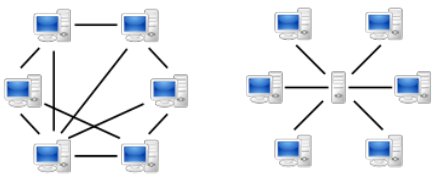
```
X-Hashcash: 1:24:040806:foo::511801694b4cd6b0:1e7297a
```

Header berisikan versi, tanggal, alamat pengirim, nilai random, dan *counter* (hexadesimal yang berada di paling kanan pada *header*). *Counter* akan terus dinaikkan hingga kriteria hasil fungsi hash yang diminta oleh penerima dicapai. Kriterianya adalah *message digest* memiliki awalan '0' berturut-turut, sebanyak yang dituntut oleh penerima.

Jumlah '0' yang digunakan terus ditambahkan sesuai dengan semakin cepatnya perhitungan yang mampu dilakukan CPU yang marak digunakan; agar serangan seperti *spam* ataupun *Denial of Service* tidak efektif dengan semakin sulitnya membentuk *header* yang valid.

V. PEER-TO-PEER

Peer-to-peer (P2P) *networking* atau *computing* merupakan aplikasi arsitektur sistem terdistribusi yang membagi-bagi pekerjaan ke setiap titik. Setiap node berfungsi baik sebagai penyedia maupun pengguna layanan. Berbeda dengan sistem *client-server*, *peer-to-peer* bersifat desentralisasi karena setiap titik memiliki hak yang serupa. Berikut ini adalah ilustrasi perbandingan *client-server* dengan *peer-to-peer*.



Gambar 3. Perbandingan P2P dengan *client-server*

VI. DASAR USULAN PROTOKOL BITCOIN

Cryptoanarchy merupakan realisasi anarkisme dalam dunia digital. Anarkisme disini berbeda dengan konteks anarkisme oleh masyarakat luas (yang merupakan salah paham), yang menghubungkan anarkisme dengan kekerasan. Hakikatnya anarkisme diambil dari bahasa yunani, *anarchos* yang berarti "tanpa pemerintah." *Cryptoanarchy* memanfaatkan kriptografi untuk menghindari penuntutan maupun campur tangan pemerintah dalam bertukar pesan, demi keamanan privasi dan kebebasan politik.

Sebelum Bitcoin diusulkan pada tahun 2008 dan akhirnya mulai aktif (walaupun masih dalam keadaan *beta*), proposal oleh Wei Dai pada tahun 1998 mengajukan sistem *cryptocurrency* yang merupakan *cryptoanarchy*. Berikut ini adalah gambaran/intrepretasi kedua protokol yang beliau ajukan. Dapat dibaca selengkapnya di http://www.weidai.com/bmoney.txt.

"Terdapat dua protokol yang diperlukan untuk berjalannya sistem ini. Protokol pertama sulit dicapai (pada tahun 1998) karena perlu sinkronisasi untuk jaringan besar dan komunikasi *broadcast* anonim yang tidak bisa diganggu, dan protokol kedua yang lebih praktis.

Di protokol pertama, setiap partisipan memelihara basis data yang menyimpan berapa uang yang dipegang oleh setiap *pseudonym* (nama samaran).

Adapula peraturan pembuatan uang, yang besarnya berdasarkan usaha, dengan menyelesaikan persoalan komputasi (serupa dengan *proof-of-work*) dengan memberikan solusi. Peraturan pertukaran uang, melarang pertukaran yang akan membuat salah satu pihak memiliki saldo negatif. Serta tiga peraturan yang menjelaskan kontrak (perjanjian penyelesaian soal komputasi matematis).

Protokol kedua menjelaskan bahwa tidak seluruh peserta perlu menyimpan data siapa memegang berapa unit uang; cukup sebagian pihak (disebut *server*). *Server* akan terus digunakan sebagai pembantu verifikasi. Selain itu, setiap *server* perlu melakukan deposito sebagai jaminan apabila ditemukan kelakuan buruk."

VII. BITCOIN

Bitcoin merupakan *cryptocurrency* yang menggunakan sistem *peer-to-peer* pertama (sehingga sistem bersifat desentralisasi, tanpa campur tangan pemerintah sehingga *cryptoanarchy* terjadi) yang diusulkan, dengan proposalnya, dan dibuat oleh Satoshi Nakamoto, sebuah *pseudonym* yang sampai saat ini belum diketahui. Bitcoin menggunakan *hashcash* sebagai *proof-of-work* selama pertambangan unit bitcoin terjadi. Nilai terkecil bitcoin,

dinamakan *satoshis*, merupakan satuan angka dengan kelipatan 1×10^{-8}; 1×10^{-3} disebut µBTC (*microcoin*), 1×10^{-3} disebut mBTC (*millicoin*), dan 1 disebut BTC.

Ada beberapa teknik kriptografi yang membangun Bitcoin, yaitu kriptografi kunci asimetri, fungsi *hash*, serta *hashcash* sebagai *proof-of-work*. Yang pertama adalah kriptografi kunci asimetri, setiap bitcoin dihubungkan dengan kunci publik ECDSA (*Elliptical Curve Digital Signature Algorithm*). Saat bitcoin akan dikirim, dibuat pesan transaksi yang berisi kunci publik penerima, jumlah koin, serta tanda tangan pengirim (menggunakan kunci privat); untuk selanjutnya dipublikasikan/*broadcast* ke setiap pengguna protokol Bitcoin, untuk diperiksa keabsahan pemilik, berdasarkan tanda tangan pengirim dan nilai saldo pengirim. Sejarah lengkap transaksi disimpan seluruh pengguna, agar semuanya mampu memverifikasi kepemilikan bitcoin.

Catatan lengkap transaksi disimpan dalam bentuk *block chain*, yang merupakan rentetan satu catatan transaksi yang bernama *block*. Hasil *hash* dari *block chain* akan disatukan, juga ditambahkan *nonce*, dan selanjutnya diambil nilai *message digest*-nya; *message digest* yang merupakan *block chain* tersebut harus memenuhi kriteria, karena itu, diperlukan penambahan *nonce*.

Dengan kata lain, pembentukan *block chain* merupakan aplikasi dari *hashcash*. Transaksi ini jugalah yang akan menjadi persoalan untuk diselesaikan *miner*, para penambang, untuk menemukan *nonce* yang tepat agar terbentuk *block chain* dan kepada mereka diberikan hadiah 25 BTC; setiap 210,000 BTC dikeluarkan, hadiah akan dikecilkan dua kali lipat. Agar regulasi terjamin, kesulitan (banyaknya angka '0' yang memulai *message digest*) diatur agar tepat 1 *block* yang terbentuk tiap 10 menit.

VIII. Perbandingan dengan Mata Uang Konvensional

A. Kelebihan dan Kekurangan Bitcoin

Kelebihan yang tidak bisa dipungkiri dari Bitcoin adalah sistem ini tidak berhubungan langsung dengan dunia nyata; hal ini menyebabkan keadaan politik tidak dapat merugikan lingkungan Bitcoin secara signifikan. Bitcoin juga tidak terpengaruh oleh mata uang tertentu, karena penggunanya tersebar di berbagai tempat yang memiliki akses internet; sehingga nilainya cukup stabil.

Sistem yang mendukung *cryptoanarchism* ini juga memberikan keleluasaan penggunaan bitcoin terhadap pengguna; runut balik terhadap siapa yang melakukan transaksi pun cukup sulit karena pengguna dapat membuat dan mengganti *wallet* tanpa usaha yang besar.

Di pihak lain, Bitcoin memiliki kelemahan yang sangat trivial, yakni sulit untuk melakukan transaksi dengan barang fisik secara langsung; karena pedagang yang menerima Bitcoin sebagai alat pembayaran yang sah pun cukup sedikit. Jalan keluar dari masalah ini adalah menggunakan jasa pertukaran mata uang, vendor terbesar saat ini adalah Mt.Gox, yang dapat diakses di https://mtgox.com/.

Selain itu, masih ada kelemahan dalam keamanannya. Tempat pengguna menyimpan data bitcoin-nya, *wallet*, terancam disalahgunakan apabila komputer yang memiliki akses dikuasai oleh pihak lain. Keamanan di Mt.Gox sendiri juga dapat menjadi masalah, karena pada Juni 2011 terjadi pembobolan sehingga *username*, *email*, serta *message digest* dari *password* dibocorkan.

B. Kelebihan dan Kekurangan Mata Uang Konvensional

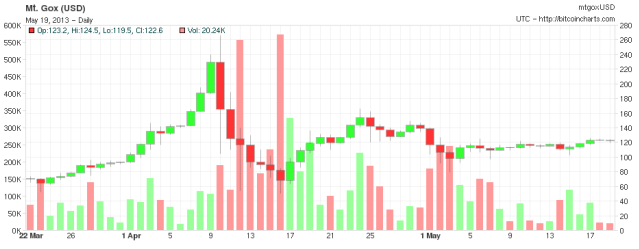
Mata uang konvensional memiliki keunggulan dalam kepraktisannya, selalu dapat digunakan dalam setiap kesempatan transaksi di negara yang menggunakan mata uang bersangkutan; mata uang konvensional juga merupakan medium pertukaran yang digunakan oleh seluruh anggota masyarakat.

Kelemahan mata uang konvensional terletak baik pada pengaruh dan ketergantungan; sebagian mata uang memiliki pengaruh yang terlalu besar, perubahan sedikit mampu menyebabkan efek berantai seperti naik/turunnya bahan pangan; begitu pula ketergantungannya yang terlalu banyak, baik dari hutang piutang negara dengan institusi lain, politik dalam negeri, ataupun hubungan politik maupun ekonomi dengan negara luar.

IX. Opini Penulis

Berdasarkan data-data dan kenyataan yang trivial, Bitcoin sangat baik untuk dijadikan tempat berinvestasi. Hal ini penulis ajukan berdasarkan kenyataan-kenyataan seperti, kokohnya nilai dari bitcoin, karena hampir tidak ada faktor dari luar yang mampu merusak lingkungan nilai ekonomi Bitcoin; juga berdasarkan fakta adanya jumlah maksimal bitcoin, sehingga dengan *supply* yang tidak bisa bertambah, *demand* akan terus naik, sehingga nilai dari bitcoin akan terus meningkat.

Contoh nyata hal ini terlihat pada saat Cyprus mengalami resesi ekonomi, ketakutan masyarakat negara tersebut akan turunnya nilai aset mereka yang berbentuk mata uang konvensional menyebabkan mereka beramai-ramai membeli bitcoin sehingga harganya melambung tinggi, mencapai 200 USD untuk sebuah BTC–hal ini memperlihatkan bahwa Bitcoin dapat menjadi tempat alternatif untuk menjaga aset. Berikut ini merupakan grafik kenaikan harga bitcoin pada saat terjadinya resesi di Cyprus.



Gambar 4. Grafik perubahan valuasi bitcoin

Walaupun Bitcoin merupakan tempat yang cukup aman, tidaklah bisa dilupakan bahwa kebutuhan manusia seringkali bersifat darurat dan sulit diperkirakan. Aset dalam bentuk mata uang konvensional mampu menyediakan kecepatan dan diterima oleh sebagian besar masyarakat belum dapat tergantikan dengan mata uang digital, bahkan Bitcoin yang merupakan *cryptocurrency* paling diterima di dunia.

Damiann Muhammad Mangan, 13510071

VII. PENGHARGAAN

Penulis secara pribadi berterima kasih kepada saudara kandung penulis, Dannis, atas saran dalam isi makalah. Penulis juga berterima kasih kepada Bapak Rinaldi Munir selaku dosen mata kuliah Struktur Diskrit dan referensi dari beliau. Penulis juga berterima kasih terhadap sahabat-sahabat penulis, yang tidak dapat penulis sebutkan satu per satu, yang membantu memberikan inspirasi hingga makalah ini dapat diselesaikan.

REFERENSI

[1] Munir, Rinaldi. (2004). Bahan Kuliah IF5054. Kriptografi. Departemen Teknik Informatika, Institut Teknologi. Bandung.
[2] http://bitcoincharts.com/charts/mtgoxUSD#rg60ztgSzm1g10zm2g25zv, tanggal akses: 15 Mei 2013, pukul 18.00.
[3] https://btc-e.com/exchange/ltc_usd, tanggal akses: 15 Mei 2013, pukul 18.00.
[4] https://btc-e.com/exchange/ppc_btc, tanggal akses: 15 Mei 2013, pukul 18.02.
[5] http://www.technologyreview.com/news/513661/bitcoin-isnt-the-only-cryptocurrency-in-town/, tanggal akses: 15 Mei 2013, pukul 18.06.
[6] http://www.technologyreview.com/news/424091/what-bitcoin-is-and-why-it-matters/, tanggal akses: 15 Mei 2013, pukul 18.19.
[7] http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html, tanggal akses: 15 Mei 2013, pukul 18.48.
[8] http://bitcoin.org/bitcoin.pdf, tanggal akses: 18 Mei 2013, pukul 20.04.
[9] http://dustcoin.com/mining, tanggal akses: 18 Mei 2013, pukul 20.29.
[10] http://www.tarsnap.com/scrypt/scrypt.pdf, tanggal akses: 18 Mei 2013, pukul 20.41.
[11] https://en.bitcoin.it/wiki/Proof_of_Work, tanggal akses: 19 Mei 2013, pukul 08.50.
[12] https://en.bitcoin.it/wiki/Proof_of_Stake, tanggal akses: 19 Mei 2013, pukul 08.52.
[13] http://www.hashcash.org/papers/proof-work.pdf, tanggal akses: 19 Mei 2013, pukul 12.09.
[14] http://www.activism.net/cypherpunk/crypto-anarchy.html, tanggal akses: 19 Mei 2013, pukul 17.04.
[15] http://www.weidai.com/bmoney.txt, tanggal akses: 19 Mei 2013, pukul 17.26.
[16] http://www.bitcoincharts.com/charts/mtgoxUSD#rg60ztgSzm1g10zm2g25zv, tanggal akses: 20 Mei 2013, pukul 03.44.

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