Analisis dan Perbandingan *Cryptocurrency* Bitcoin dan Litecoin

Rubiano Adityas - 13510041
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510041@std.stei.itb.ac.id

***Abstract*—Makalah ini membahas tentang analisis dan perbandingan mata uang digital Bitcoin dan Litecoin. Selain pembahasan mengenai analisis dan perbandingan tersebut tersebut, juga dipaparkan mengenai mata uang digital sebagai hasil implementasi dari tanda tangan digital, dan berbagai macam teori yang melandasinya.**

***Index Terms* — Cryptocurrency, Bitcoin, digital signature, kriptografi, Litecoin.**

I. PENDAHULUAN

Kriptografi merupakan cabang ilmu yang esensial dalam bidang keamanan informasi, di zaman dimana penggunaan teknologi informasi sangat tinggi, dan jumlah transmisi data tentu sangat banyak. Suatu pesan yang dikirim bisa diserang oleh pihak ketiga (*adversaries*), sehingga pihak ketiga dapat mengetahui isi pesan, atau mengubah isi pesan tersebut. Apabila data yang ditransmisikan memiliki nilai kerahasiaan yang tinggi (misal: rencana bisnis perusahaan dagang), maka tentu penyerangan terhadap pesan akan sangat merugikan. Oleh karena itu, dikembangkanlah berbagai macam metode kriptografi untuk mengamankan pesan/informasi yang ditransmisikan. Kriptografi secara umum bisa dibagi menjadi dua, klasik dan modern. Usia ilmu kriptografi modern relatif muda, namun kriptografi klasik sudah ada sejak zaman yunani kuno.

Dewasa ini, banyak sekali teknologi terapan yang menggunakan kriptografi, misalnya adalah kriptografi kunci publik dan digital signature. Kriptografi kunci publik kerap digunakan apabila dibutuhkan proses pengiriman data yang lebih aman ketimbang kriptografi kunci simetri. Hal ini dikarenakan kunci privat hanya diketahui oleh satu pihak, dan proses pembentukan kunci dilakukan dengan metode matematika yang sulit untuk dibalikkan (kurang *reversible*), seperti operasi modulo, perpangkatan, dan logaritmik. Namun dikarenakan ongkos operasi enkripsi dan dekripsi kriptografi kunci publik yang relatif berat, maka dari itu, kriptografi kunci publik biasa digunakan hanya untuk proses pengiriman kunci simetri dengan aman. Setelah kunci simetri didapat, barulah kedua belah pihak bertransaksi data dengan kriptografi kunci simetri.

Digital signature merupakan salah satu hasil implementasi kriptografi, lebih spesifiknya gabungan antara kriptografi kunci publik dan fungsi hash. Digital signature biasa digunakan untuk proses otentikasi suatu berkas digital, sehingga semua pihak bisa memastikan bahwa berkas digital yang didapat adalah kredibel, berasal dari sumber yang asli, tidak dimodifikasi. Dengan kombinasi fungsi hash dan kunci privat, sumber dapat menyisipkan digital signature-nya pada berkas digital, yang kemudian dikirim ke tujuan. Pihak yang dituju dapat menguji otentitas berkas tersebut dengan kombinasi fungsi hash dan kunci publik.

Kriptografi kunci publik dan digital signature bisa dibilang merupakan implementasi kriptografi yang umum dan kerap dijumpai penggunaannya pada teknologi-teknologi penunjang kebutuhan masyarakat, seperti kartu kredit, email, dan lain sebagainya. Namun para matematikawan dan ilmuwan komputer telah menemukan penggunaan lain dari kriptografi yang berpotensi untuk menunjang, atau bahkan mengubah cara hidup masyarakat, terutama dalam metode jual-beli, yakni mata uang digital, atau dalam konteks kriptografi, kerap disebut sebagai cryptocurrency. Cryptocurrency adalah mata uang digital yang tidak diregulasi oleh pemerintahan yang diakui dunia, dan maka dari itu tidak termasuk dari 182 mata uang resmi yang diakui. Tidak seperti mata uang konvensional, yang dicetak dan diisu oleh pemerintah, cryptocurrency didapat dengan proses mining, dengan mengikuti aturan yang ditetapkan oleh Financial Crimes Enforement Network (FinCen), sebua biro cabang dari Departemen Keuangan AS.

Pada kesempatan kali ini, penulis ingin membahas mengenai cryptocurrency, berberapa contoh implementasi cryptocurrency, beserta analisis dan perbandingannya.

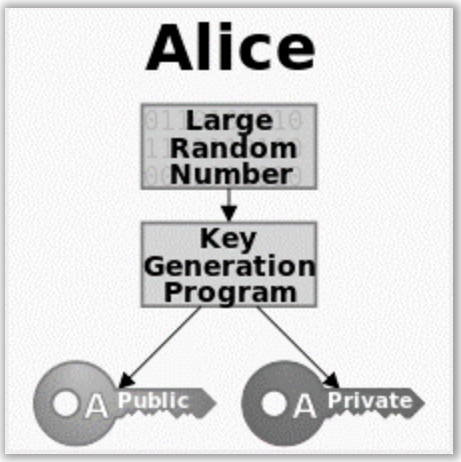
II. TEORI DASAR

A. Kriptografi Kunci Publik

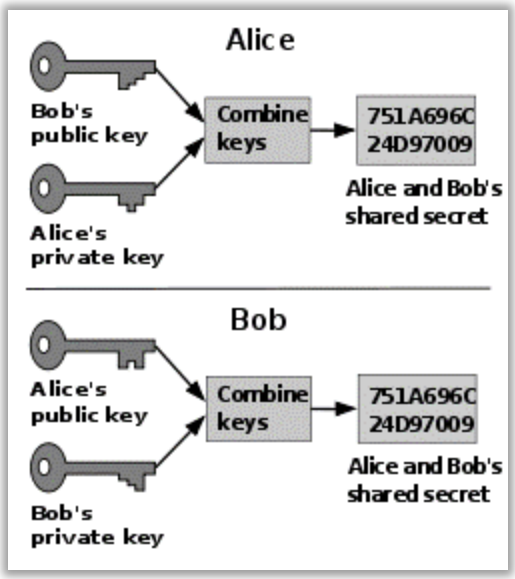
Kriptografi kunci publik adalah sebuah metode cipher yang mempergunakan dua buah kunci yang berbeda. Satu kunci dirahasiakan terhadap pihak lain (kunci privat), sementara satunya lagi diketahui oleh pihak lain (kunci publik). Walau nilai kedua kunci tersebut berbeda, mereka terhubung secara matematis. Satu kunci digunakan untuk mengenkripsi plaintext, sementara satunya lagi digunakan untuk mendekripsi ciphertext. Sebuah kunci tidak bisa sekaligus melakukan kedua fungsi tersebut, harus menggunakan dua kunci. Dari kedua kunci tersebut, kunci

publik dapat dipublikasikan ke pihak lain tanpa membahayakan keamanan enkripsi pesan, sementara kunci privat tidak boleh dipublikasikan ke pihak yang tidak memiliki otorisasi untuk membaca pesan yang terkandung dalam ciphertext.

Kriptografi kunci publik menggunakan algoritma kunci asimetrik untuk pembangunan kunci privat dan publik. Algoritma tersebut didasarkan pada relasi matematika, yang paling umum adalah faktorisasi bilangan, operasi modulo, dan logaritma diskrit. Berberapa contoh implementasi algoritma tersebut adalah Diffie-Hellman dan Elgamal. Algoritma tersebut membuat proses analisis private key dari publik key sangatlah sulit. Hal tersebutlah yang menyebabkan, tidak seperti algoritma kunci simetri, algoritma kunci publik tidak memerlukan transaksi data awal yang aman antara pengirim dan penerima, dikarenakan kunci publik tersedia untuk semua pihak, jadi tidak apa bila diketahui oleh pihak lain.



Gambar 1 Proses Algoritma Umum Pembangkitan Kunci Asimetri



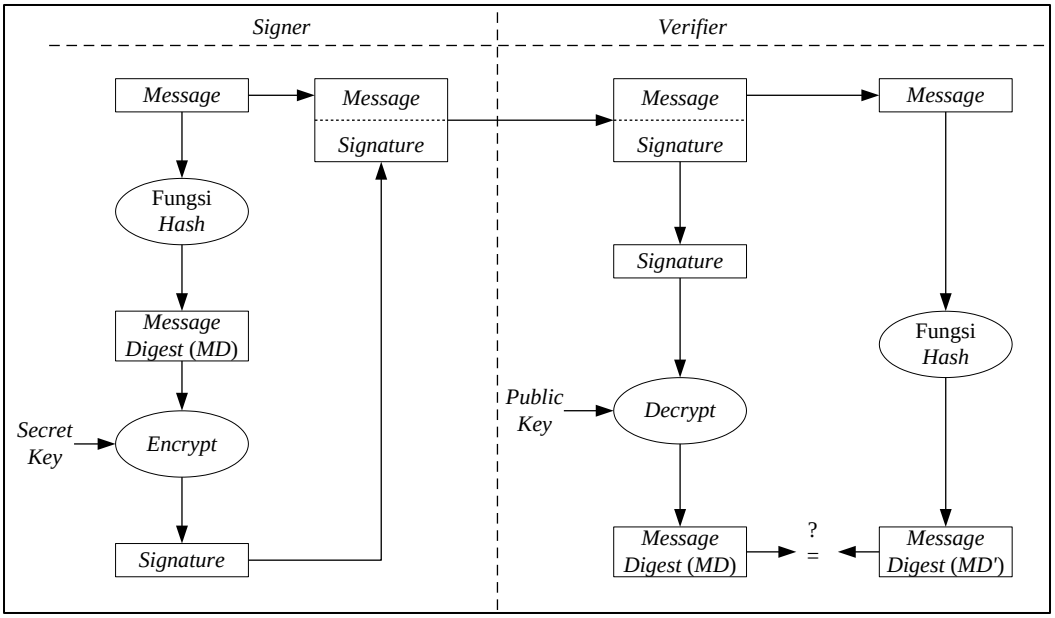
Gambar 2 Penggunaan Kedua Kunci untuk Mengenkripsi dan Mendekripsi Pesan

Penggunaan kunci sesungguhnya bersifat reversibel, dalam artian, kunci publik atau privat bisa digunakan untuk mengenkripsi data, sementara itu, kunci yang tidak dipakan untuk proses enkripsi, digunakan untuk proses dekripsi. Penentuan key mana yang digunakan untuk enkripsi dan dekripsi bergantung dari tujuan transaksi data. Untuk kasus transaksi data rahasia, pesan dienkripsi dengan kunci publik dari pihak penerima. Hal ini menyebankan pesan tersebut tidak bisa didekripsi oleh pihak yang tidak memiliki kunci privat yang sesuai, yang asumsinya hanya dimiliki oleh pihak penerima. Proses transaksi data rahasia tersebut digunakan untuk menjamin kerahasiaan pesan. Dalam kasus lainnya, yakni digital signature, dibahas pada upabab berikutnya.

B. Digital Signature

Digital signature, atau tanda tangan digital, adalah suatu metode untuk menjamin otentitas sebuah berkas/pesan digital. Sebuah digital signature yang valid akan memberikan konfirmasi kepada penerima pesan, bahwa pesan yang terkirim berasal dari sumber yang diacu pesan tersebut. Dengan begitu, digital signature mampu mencegah penyangkalan pengiriman pesan oleh sang pengirim (aspek otentikasi dan nonrepudasi), serta melihat apakah pesan termodifikasi ketika sedang dikirim (aspek integritas). Digital signature biasa digunakan pada transaksi finansial, distribusi perangkat lunak, dan pendeteksian pemalsuan dan manipulasi berkas digital.

Berkaitan dengan upabab sebelumnya. Pada penggunaan digital signature, sebuah pesan digital diimbuhi dengan kunci privat sang pihak pengirim, dan pesan tersebut dapat diverifikasi oleh pihak manapun dengan menggunakan kunci publik sang pihak pengirim. Hasil verifikasi tersebut membuktikan apakah sang pengirim memiliki akses ke kunci privat, dimana apabila iya, pengirim diasumsikan asli, dan bukan pihak ketiga yang menyamar sebagai pengirim. Selain itu, dengan pengimbuhan digital signature ke dalam pesan digital, penerima bisa mengetahui apakah ada pihak ketiga yang memodifikasi pesan tersebut. Perubahan bida terdeteksi karena message digest pesan tersebut berubah, sehingga gagal diverifikasi. Sebuah skema digital signature memiliki tiga komponen algoritma utama, yakni: algoritma generator kunci yang berfungsi untuk membangkitkan kunci privat dan kunci publik, algoritma signer yang berfungsi untuk membentuk signature, dan algoritma verifyer yang berfungsi untuk mengecek signature dan menilai otentitasnya.



Gambar 3 Proses Signing dan Verifying Digital Signature

C. Cryptocurrency

Pembahasan mengenai cryptocurrency akan meliputi tiga buah topik yang kerap kali salah dimengerti oleh khalayak umum, sehingga penggunaan terminologinya kerap kali tertukar, yakni digital currency (cryptocurrency), electronic money, dan virtual money.

Electronic money adalah nilai mata uang yang digunakan dalam transaksi melalui media elektronik, yang meliputi penggunaan jaringan komputer, internet, dan sistem penyimpanan data digital. Contoh dari electronic money adalah deposit bank, transfer uang antar akun, prosesor pembayaran online (contoh: visa, paypal). Selain itu, cryptocurrency juga tergolong sebagai electronic money.

Virtual money adalah mata uang yang umumnya digunakan pada dunia virtual, kerap digunakan untuk bertransaksi barang digital dalam dunia maya. Virtual money secara umum terbagi menjadi tiga tipe, yakni: closed, unidirectional flow, dai bidirectional flow. Closed virtual money tidak memiliki hubungan apa-apa dengan uang dalam dunia nyata, pada umumnya diterapkan pada permainan video bergenre MMORPG. Pada ekonomi virtual bertipe unidirectional flow, orang bisa membeli virtual money dengan mata uang asli/fisik, namun tidak bisa sebaliknya. Pada ekonomi virtual bertipe bidirectional flow, orang bisa membeli virtual money dengan mata uang asli/fisik, dan juga sebaliknya. Ciri khas dari virtual money ialah, mata uang virtual memiliki nama nominal tersendiri (misal: gold pada permainan WoW), berbeda dengan mata uang asli (misal: Rupiah, US Dollar).

Keterhubungan konsep electronic money dan virtual money bisa dilihat pada tabel berikut ini:

Status legal	**Tidak teregulasi**	Berberapa tipa mata uang lokal	*Virtual money*
	Teregulasi	Catatan bank dan koin	*Electronic money*
			Deposit
		Fisik	Digital
		Format uang	

Tabel 1 Klasifikasi Jenis Uang

Dari penggolongan tersebut, Digital currency (cryptocurrency) tergolong sebagai irisan dari virtual money dan electric money. Hal ini dikarenakan cryptocurrency dapat digunakan untuk bertransaksi di berberapa tempat dalam dunia nonvirtual melalui media elektronik, cryptocurrency memiliki nama nominal tersendiri, dan dari proses akuisisinya, cryptocurrency bisa dibilang didapat secara virtual, karena prosesnya dilakukan secara peer-to-peer dengan jaringan dan pengguna lainnya.

Dari status legal, cryptocurrency tidak diregulasi oleh badan keuangan resmi negara manapun, namun masih tetap mengikuti aturan yang ditetapkan oleh Financial Crimes Enforement Network (FinCen), sebua biro cabang dari Departemen Keuangan AS. Aturan tersebut dimuat dalam dokumen yang berisikan petunjuk interpretatif mengenai replikasi penggunaan aturan Bank Secrecy Act (BSA) bagi individu yang membuat, dan bertransaksi cryptocurrency.

Berikut ini adalah daftar cryptocurrency yang saat ini ada:

Mata Uang	Simbol	Tahun Dibuat	Pembuat	Situs	Basis Keuangan	Implementasi
Bitcoin	BTC	2009	Satoshi Nakamoto	Bitcoin.org	$1 miliyar	Decentralized ledger currency, SHA-256 proof-of-work
Litecoin	LTC	2011	Coblee	Litecoin.org	$38 juta	Scrypt proof-of-work
Namecoin	NMC	2011	Vinced	Dot-bit.org	$4.5 juta	Decentralized DNS, SHA-256 proof-of-work
PPCoin	PPC	2012	Sunny King	Ppcoin.org	$4 juta	SHA-256 proof-of-work/proof-of-stake

Tabel 2 Daftar Cryptocurrency yang Saat Ini Beredar

Secara umum, berikut ini adalah prasyarat ideal yang perlu dimiliki oleh sebuah implementasi cryptocurrency agar dapat memiliki kredibilitas/tingkat kepercayaan pengguna yang tinggi:

- Open Protocol
  Bagaimana mekanisme mata uang tercipta, dipertukarkan, dan dihancurkan oleh jaringan cryptocurrency tersebut haruslah dipublikasi sebagai open protocol. Software pendukung client jaringan haruslah dapat dibuat dengan detail spesifikasi yang disediakan secara terbuka/cuma-cuma.
- Anonim
  Identitas pengguna jaringan cryptocurrency haruslah terproteksi ketika sedang bertransaksi. Ketika seorang pengguna mengirimkan sejumlah uang ke pengguna lain, transaksi tersebut sepatutnya tidak bisa digunakan untuk melacak pengirim.
- Sangat resisten terhadap pemalsuan
  Kapabilitas perentas untuk membuat uang baru haruslah seminim mungkin, sebatas teknologi yang tersedia
- Proteksi dari pencurian
  Aset digital sangatlah mudah untuk dicuri, baik itu dengan duplikasi, maupun dengan penyalinan dan penghapusan. Perlindungan sistem terhadap hal tersebut merupakan suatu keharusan
- Multipoint authenticity
  Otentitas dari sejumlah berapapun uang yang sedang bersirkulasi di jaringan, harus bisa diverifikasi melalui setidaknya dua mekanisme yang saling independen.
- Efisien
  Operasi terhadap cryptocurrency haruslah efisien, wanpa memerlukan processing overhead yang tinggi.
- Tahan banting
  Dalam kondisi ideal, jaringan cryptocurrency harus tahan terhadap sejumlah kegagalan sistem. Desentralisasi sistem bisa menangani hal tersebut. Namun harus ditemukan titik keseimbangan, karena sistem yang terlalu terdesentralisasi mudah direntas, sementara sistem yang terlalu tersentralisasi tidak mampu menghadapi banyak kegagalan sistem.

D. Bitcoin

Gambar 4 Logo Bitcoin

Bitcoin adalah cryptocurrency pertama yang dapat digunakan untuk transaksi digital, walau konsepnya sudah dibangun oleh berberapa purwarupa sebelumnya. Purwarupa pertama, yakni sebuah sistem kriptografik untuk pembayaran digital yang tak terlacak, digagas oleh Davin Chaum pada tahun 1982. Purwarupa tersebut terus dikembangkan oleh Chaum, hingga pada tahun 1990, menjadi sebuah sistem uang digital kriptografik yang anonim, yang dikenal sebagai "ecash". Pada tahun 1982, Wei Dai mempublikasikan sebuah purwarupa lain, yakni sistem distribusi uang elektronik anonim yang diberi nama "b-money". Pada rentang waktu yang berdekatan, Nick Szabo menciptakan "bit gold".

Sama seperti Bitcoin, bit gold ialah sebuah sistem mata uang, dimana pengguna saling berkompetisi untuk menyelesaikan permasalahan proof-of-work, yang melingkupi validasi transaksi antar pihak-pihak yang menggunakan bit gold. Solusi yang ditemukan secara kriptografis menyambung satu dengan lainnya. Serupa dengan bit gold, yakni "Reusable Proofs of Work", diimplementasikan oleh Hal Finney.

Jaringan Bitcoin sendiri diciptakan pada 3 Januari 2009, bersamaan dengan rilis Bitcoin pertama dan client Bitcoin pertama, yakni wxBitcoin. Penciptaan Bitcoin didasarkan pada tulisan mengenai Bitcoin protocol yang dibuat oleh Satoshi Nakamoto pada tahun 2008. Jaringan Bitcoin merupakan koneksi peer-to-peer semua pemilik Bitcoin, dan semua Bitcoin miner. Proses transaksi dengan menggunakan Bitcoin langsung menggunakan koneksi ini, tidak melalui perantara/pihak ketiga, maka dari itu kredibilitas partisipan transaksi merupakan sepenuhnya tanggung jawab dan penilaian dari pengguna masing-

masing.

Secara umum, proses transaksi dengan menggunakan Bitcoin dalah sebagai berikut:

- Misal ada dua orang pemilik Bitcoin, Bob dan Alice. Alice ingin membeli suatu barang dari Bob dengan menggunakan Bitcoin yang ia miliki.
- Alice dan Bob memiliki Bitcoin wallet pada komputer mereka masing-masing. Mereka berdua juga terkoneksi dengan jaringan Bitcoin ketika melakukan transaksi.
    - Wallet tersebut adalah sebuah berkas digital yang memiliki akses ke berberapa address Bitcoin.
    - Address itu sendiri berupa string sepanjang 33 karakter alphanumerik, dan selalu diawali dengan integer 1 atau 3. Address bisa diibaratkan sebagai tumpukan koin, dimana nilainya bisa berbeda-beda.
- Bob membuat sebuah address Bitcoin baru untuk menerima pengiriman Alice
    - Ketika Bob menciptakan address baru, ia menciptakan sepasang kunci asimetri (kunci privat dan publik). Address yang baru ia ciptakan bisa diibaratkan sebagai kunci publik, sementara kunci privatnya tersimpan di wallet.
- Alice memerintahkan client Bitcoin miliknya bahwa ia ingin transfer sejumlah Bitcoin ke address baru Bob.
    - Client Bitcoin Alice akan mengimbuhi address Bitcoin yang digunakan untuk transaksi, dengan digital signature Alice, menggunakan private key address tersebut.
    - Dikarenakan proses signing dilakukan dengan private key, maka semua orang di dalam jaringan Bitcoin dapat memverifikasi bahwa permintaan transaksi berasal dari orang yang memiliki otorisasi terhadap address tersebut.
- Permintaan (request) transaksi kemudian diteruskan ke jaringan Bitcoin, untuk kemudian diverifikasi, dan dilakukan proses proof-of-work.

Proses verifikasi sendiri merupakan proses yang unik dan panjang. Verifikasi dilakukan oleh kelompok pengguna lain yang disebut sebagai miner. Semua permintaan transaksi yang masuk ke proses verifikasi, akan mengakumulasikan sebuah bukti transaksi, yang disebut transaction block. Proses pembaharuan transaction block dilakukan setiap 10 menit secara konkuren untuk seluruh peer jaringan Bitcoin. Berikut adalah prosesnya:

- Para Bitcoin miner menerima berberapa request transaksi dalam rentang waktu 10 menit.
- Setelah 10 menit, semua transaksi yang terkumpul di-bundle, membentuk sebuah transaction block baru, yang berisikan detail seluruh transaksi, berikut address-address yang terlibat, dan jumlah Bitcoin yang berpindah address.
- Komputer miner bersiap untuk melakukan kalkulasi fungsi hash kriptografik.
    - Fungsi hash disini berfungsi untuk menghasilkan sebuah string alphanumerik dengan panjang yang tetap.
    - Perubahan pada bundle akan menyebabkan perubahan nilai hash, dan secara praktis, mustahil untuk menebak seperti apa bundle apabila diketahui nilai hashnya.
    - Untuk membentuk hash yang berbeda dengan nilai bundle yang sama, digunakan “nonces”, yakni bilangan acak yang ditambahkan ke bundle untuk mengubah hasil fungsi hash.
- Fungsi hash dieksekusi secara berantai, dalam artian hasil fungsi hash yang sebelumnya, ditambah dengan bundle, dan ditambah dengan nonces, menghasilkan nilai hash yang baru, dan begitu seterusnya untuk setiap 10 menit.
    - Permasalahan yang timbul adalah, protokol Bitcoin mengharuskan hash yang dihasilkan untuk memiliki berberapa integer 0 sebagai penyusunnya.
    - Para miner tidak mungkin mengetahui nonces seperti apa yang dapat menghasilkan hash yang memenuhi syarat tersebut. Maka dari itu, eksekusi fungsi hash dilakukan secara brute force sehingga ditemukan nonces yang sesuai.
    - Proses menemukan nonces yang sesuai membutuhkan sumber daya komputasi yang tinggi. Disinilah kegunaan miner mulai terlihat.
    - Semua miner secara kolektif mengkontribusikan processing power komputer mereka untuk memproses nonces. Penemuan nonces akan menghasilkan Bitcoin baru, dan Bitcoin baru tersebut dihadiahkan kepada miner yang berhasil menemukan nonces.

Apabila ingin dilakukan manipulasi terhadap transaksi Alice dan Bob, maka sang pelaku harus mereka ulang seluruh pekerjaan miner, yang membutuhkan sumber daya kolektif yang tinggi. Selain itu, seiring dengan waktu, transaction block yang memuat transaksi Alice dan Bob akan digunakan untuk pembentukan hash-hash berikutnya, semakin lama, proses verifikasi semakin irreversibel, dan kerahasiaan transaksi Alice dan Bob semakin terjaga. Inilah kelebihan utama dari cryptocurrency pada umumnya, dan Bitcoin pada khususnya. Ketidakadaan pihak antara (seperti bank) yang meregulasi transaksi, serta jaringan yang peer-to-peer, berkontribusi terhadap hal tersebut.

Karena tidak ada pihak regulator, pengadaan Bitcoin dilakukan secara otomatis oleh jaringan. Jaringan Bitcoin diprogram untuk meningkatkan persediaan Bitcoin

mengikuti seri geometrik, hingga persediaan Bitcoin mencapai 21 juta BTC. Pada tahun 2012, sudah 10 juta Bitcoin yang diedarkan di jaringan. Semakin banyak Bitcoin yang tersedia, hadiah untuk miner juga akan semakin berkurang. Pada tahun 2012, hadiah untuk miner yang menemukan nonces adalah 25 BTC. Karena keberadaan hadiah tersebut, banyak orang yang berlomba-lomba mining untuk menemukan nonces hash. Meski begitu, karena sumber daya yang dibutuhkan untuk menemukan nonces tinggi, kerap kali miner bergabung menjadi miner pool, menggabungkan processing power komputer mereka. Barang siapa diantara mereka ada yang menemukan nonces, hadiah yang diterima dibagi ke seluruh anggota miner pool. Harga BTC pada tahun 2012 kurang lebih ekivalen dengan 10 USD. Dengan mempertimbangkan ekivalensi tersebut, dan jumlah Bitcoin yang sudah "ditambang", nilai yang beredar di jaringan Bitcoin sudah mencapai 110 juta USD.

E. Litecoin

Gambar 5 Logo Litecoin

Litecoin merupakan mata uang digital alternatif (cryptocurrency) yang didasarkan pada Bitcoin. Satu alasan penciptaan Litecoin adalah dirasa perlunya cryptocurrency lain yang memiliki algoritma mining yang berbeda dengan bitcoin, agar harga hadiah mining bitcoin tidak cepat turun, karena terlalu banyak yang melakukan mining. Harapannya, dengan pembuatan cryptocurrency baru, komunitas miner dapet lebih tersebat.

Perbedaan Litecoin dengan Bitcoin terletak pada berberapa aspek, antar lain: proof-of-work (proses verifikasi), waktu pembentukan transaction block, limitasi jumlah coin, dan penamaan address. Pada proses proof-of-work, digunakan algoritma yang intensif penggunaan memorinya, untuk mengurangi efisiensi paralellisasi GPU yang umum dilakukan pada mining Bitcoin. Hal ini dilakukan untuk mengurangi kecepatan mining, agar nilai Litecoin tidak cepat jatuh. Selain itu, digunakan Scrypt sebagai pengganti SHA256 yang digunakan pada Bitcoin. Jarangnya pemanfaatan Scrypt pada implementasi-implementasi kriptografi lain, diharapkan membuat perentas menjadi tidak terbiasa dengan skema jaringan tersebut.

Ketimbang Bitcoin, waktu pembentukan transaction block pada skema Litecoin jauh lebih cepat, yakni 2.5 menit. Hal ini menguntungkan pedagang pada umumnya, karena mendapat konfirmasi transaksi yang lebih cepat, tidak harus menunggu 10 menit. Kekurangan dari hal tersebut adalah, kekuatan fungsi hash tidak sekuat hash Bitcoin, karena ukutan transaction block lebih kecil, sehingga lebih reversibel. Untuk jumlah coin maksimum, jaringan Litecoin memiliki batas yang lebih tinggi ketimbang Bitcoin, yakni 84 juta. Selain itu, penamaan address Litecoin menggunakan karakter L sebagai karakter pertama address Litecoin.

III. RUMUSAN MASALAH

Bitcoin belakangan ini kerap kali muncul namanya pada pemberitaan teknologi, dikarenakan harga Bitcoin yang fluktuatif, naik dan turun dengan drastis. Hal tersebut menimbulkan perdebatan akan relevansi Bitcoin (secara khusus) dan cryptocurrency (secara umum) sebagai medium transaksi dan dampaknya pada perekonomian negara. Pada makalah yang penulis ajukan, penulis akan menganalisis Bitcoin sebagai cryptocurrency, dan membandingkannya dengan Litecoin, sebuah cryptocurrency yang serupa.

IV. ANALISIS PERBANDINGAN

Berikut akan diamati aspek perbedaan dari Bitcoin dan Litecoin, dan bagaimana perbedaan tersebut mempengaruhi performa masing-masing cryptocurrency.

A. Proses Verifikasi

Seperti yang sudah dibahas padabab sebelumnya, perbedaan verifikasi Bitcoin dan Litecoin ada pada fungsi hash yang digunakan, dan juga adanya algoritma penghambatan efisiensi miner. Dengan adanya penghambatan efisiensi miner, tingkat inflasi nilai Litecoin bisa ditekan, ketimbang Bitcoin yang tidak memiliki metode tersebut. Selain itu, pada penggunaan fungsi hash, didapat bahwa Scrypt yang digunakan oleh Litecoin menggunakan sumber daya yang tinggi, sehingga mudah merusak GPU. Hal demikian tidak berlaku untuk Bitcoin yang menggunakan SHA-256. Dengan kombinasi dua hal tersebut, banyak miner lebih memilih Bitcoin ketimbang Litecoin, walau tentu nilai jual cryptocurrency dari Bitcoin juga berpengaruh terhadap prefeferensi para miner.

B. Pembentukan Transaction Block

Pembentukan transaction block Litecoin yang 75% lebih cepat ketimbang Bitcoin, membuat respon verifikasi yang cepat. Dalam konteks bisnis dan perdagangan sehari-hari, hal ini tentu menguntukan pebisnis yang menggunakan cryptocurrency tersebut. Minimnya waktu konfirmasi transaksi dapat diasumsiskan meningkatkan jumlah transaksi yang dilakukan oleh pebisnis tersebut. Meski begitu, ukuran transaction block kecil menimbulkan resiko keamanan, karena transaksi menjadi mudah dilacak, sehingga menyebabkan kerahasiaan pengguna terbongkar. Mengenai hal tersebut, sepenuhnya merupakan preferensi pengguna.

C. Batas Jumlah Koin

Bitcoin memiliku batas jumlah koin sebesar 21 juta, sementara Litecoin 84 juta. Besarnya batas tersebut, membuat Litecoin memiliki tinkat inflasi yang rendah, ketimbang Bitcoin, karena persentase nilai coin yang ditemukan bertambah dengan tingkat yang lebih kecil pada Litecoin. Mengingat Bitcoin sudah hampir mencapai setengahnya yang sudah ditemukan, mining Litecoin menjadi prospek yang menarik bagi para miner. Selain karena tingkat inflasi yang rendah, persaingan masih sedikit (setidaknya untuk tahun ini), sehingga bagi yang terlebih dahulu berinvestasi, dapat meraup keuntungannya kemudian ketika penggunaan Litecoin sudah umum.

D. Popularitas dan Penggunaan

Dari berberapa aspek yang dibahas pada upabab sebelumnya. Dalam jangka pendek, mining Bitcoin masih jauh lebih menguntungkan ketimbang Litecoin, dikarenakan penggunaan sumber daya yang relatif lebih ringan, lebih aman, dan pasar yang sudah cukup terbentuk. Namun apabila melihat jangka panjang, Litecoin bisa menjadi alternatif bagi pada miner, dikarenakan tingkat inflasinya yang rendah. Statistik basis keuangan pun menunjukkan hasil demikian, basis keuangan Bitcoin sejumlah 1 miliyar USD, sementara Litecoin sebesar 38 juta USD. Semua hal ini belum mempertimbangkan cryptocurrency lain yang beredar di pasar, seperti Namecoin dan PPCoin, yang juga memiliki potensi untuk menggantikan Bitcoin sebagai cryptocurrency yang dominan.

REFERENSI

[1] Rinaldi Munir. Presentasi Kuliah IF3058 Kriptografi
[2] European Central Bank. *Virtual Currency Schemes*. Oktober: 2012
[3] http:// en.Bitcoin.it
[4] http://www.ecb.int/stats/money/aggregates/emon/html/index.en.html
[5] https://www.x.com/devzone/articles/how-crypto-currencies-transform-money
[6] http://www.zerohedge.com/sites/default/files/images/user3303/imageroot/2013/05/20130512_BTC.jpg

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, 19 Mei 2013

Rubiano Adityas
13510041