

MENGENAL BITCOIN & CRYPTOCURRENCY

DIMAZ A. WIJAYA

Memahami Bitcoin & Cryptocurrency

Dimaz Ankaa Wijaya



Mengenal Bitcoin dan Cryptocurrency
Hak cipta © 2016 Dimaz Ankaa Wijaya

Diterbitkan pertama kali oleh Puspantara
Jalan Abadi Komplek Abadi Place Blok E-01,
Tanjung Rejo, Medan, Sumatera Utara, Indonesia
info@puspantara.org | puspantara.org

Editor: Fauzan Nur Ahmadi, Vinsensius Sitepu
Desainer grafis: MahapalaMultimedia.com

ISBN: 978-602-73634-4-1

*Dilarang keras menerjemahkan, memfotokopi, atau
memperbanyak sebagian atau seluruh isi buku ini
tanpa izin tertulis dari penerbit.*

DAFTAR ISI

PENGANTAR PENULIS — 1

KATA PENGANTAR OSCAR DARMAWAN — 4

■ PENDAHULUAN — 9

Uang — 9

Kriptografi — 10

Public Key Cryptography — 11

Tanda Tangan Elektronik — 12

Fungsi Hash — 14

Bitcoin — 15

Blockchain — 18

Double Spending — 20

Proof of Work — 21

Penambangan — 21

Node Bitcoin — 22

Jaringan Peer-to-peer — 23

Pengembang Perangkat Bitcoin — 24

Alamat Bitcoin — 25

Dari Kunci Publik ke Alamat Bitcoin — 26

Bitcoin Vanity Address — 26

Transaksi Bitcoin — 27

Script Transaksi — 30

Biaya Transaksi — 32

Komunitas dan Sumber Informasi Bitcoin — 33

■ DOMPET BITCOIN — 34

Dompot Bitcoin Web — 35

Dompot Bitcoin Smartphone — 40

Dompot Bitcoin Desktop — 46

Bitcoin Core — 49

Dompot Panas dan Dingin — 51

Dompot Otak — 51

■ MENDAPATKAN BITCOIN — 53

Bitcoin Indonesia — 53

Bitcoin Faucet — 58

Bitcoin ATM — 59

Menambang Bitcoin — 60

Cara Lain — 66

■ MENGGUNAKAN BITCOIN — 68

Bitcoin sebagai Alat Pembayaran — 68

Transaksi Standar — 69

Transaksi Escrow — 69

Konfirmasi Transaksi — 70

Ajang Promosi Usaha — 70

Status Bitcoin di Indonesia — 70

Bitcoin sebagai Alat Investasi & Komoditas Perdagangan — 70

Bitcoin dan Inovasi Teknologi — 72

Pembuktian Eksistensi Dokumen — 74

Kontrak — 75

E-voting — 76

■ KONTROVERSI BITCOIN — 78

Satoshi Nakamoto — 78

Ketiadaan Inflasi — 79

Mt. Gox — 79

Silk Road — 80

Inefisiensi Energi — 81

Ukuran Blok — 81

Jumlah Node Semakin Berkurang — 82

■ **ALTCOIN — 83**

Ripple — **83**

Litecoin — **86**

Dogecoin — **87**

Peercoin — **89**

Ethereum — **90**

Berspekulasi Dengan AltCoin — **92**

Cross Chain Trading — **93**

■ **PERKEMBANGAN TERKINI — 94**

Masuk Bursa Saham — **94**

Perbankan — **95**

Startup — **95**

Blockchain-as-a-service — **95**

REFERENSI — **96**

TENTANG PENULIS — **96**

PENGANTAR PENULIS

BITCOIN MENAWARKAN TEROBOSAN DALAM DUNIA FINANSIAL YANG TIDAK MEMERLUKAN PERBANKAN SEBAGAI LEMBAGA PERANTARA DALAM TRANSAKSI KEUANGAN. BITCOIN MEMILIH UNTUK MENGGABungkan TEKNIK KRIPTOGRAFI DAN JARINGAN PEER-TO-PEER UNTUK MENYEDIAKAN SUATU ALTERNATIF SISTEM PEMBAYARAN YANG BERBEDA DARI APA YANG TELAH KITA KENAL SELAMA INI.

Bitcoin yang disebut juga sebagai mata uang Internet semakin berkembang pesat dan penggunaannya semakin meluas bahkan hingga ke tanah air, sehingga pengetahuan seputar Bitcoin dapat meningkatkan nilai kompetitif usaha yang Anda miliki, atau mungkin setelah berkenalan dengan Bitcoin, Anda tertarik untuk memulai karir sebagai *trader* Bitcoin. Dengan karakteristiknya yang mirip dengan emas, Bitcoin sangat cocok jika dikategorikan sebagai komoditas yang tentu saja dapat diperjualbelikan.

Buku ini disusun untuk memperkenalkan Anda pada Bitcoin, memandu Anda untuk mulai menggunakan Bitcoin untuk ber-

bagai keperluan dengan penjelasan dan gambar langkah demi langkah.

Buku ini disusun dengan struktur sebagai berikut:

- **Bagian Pertama** membahas tentang Bitcoin, latar belakang, teknologi yang digunakan, dan bagaimana transaksi keuangan dapat dilakukan menggunakan Bitcoin. Di sini Anda juga akan mengetahui seluk beluk tentang alamat Bitcoin.
- **Bagian Kedua** mengenalkan Anda pada berbagai jenis *wallet*, yaitu perangkat lunak (*software*) yang dapat membantu Anda untuk mengorganisasikan dan mengelola alamat Bitcoin dan dana yang ada di dalamnya.
- **Bagian Ketiga** berbicara tentang cara mendapatkan Bitcoin. Anda bisa memperoleh informasi di mana Anda bisa membeli Bitcoin, atau bahkan mendapatkannya secara cuma-cuma melalui berbagai cara di Internet. Bagian ini juga menerangkan tentang penambangan (*mining*) Bitcoin, apa dan bagaimana hal tersebut dilakukan. Anda pun bisa turut menambang!
- **Bagian Keempat** berisi tentang cara pemanfaatan Bitcoin yang Anda miliki. Anda bisa memperlakukan Bitcoin layaknya uang, atau bahkan Anda bisa menyimpan Bitcoin milik Anda untuk mendapatkan nilai tambah di masa yang akan datang sebagai investasi. Anda pun akan diajak untuk melihat peluang Bitcoin untuk digunakan dalam memecahkan permasalahan-permasalahan yang lebih luas.
- **Bagian Kelima** menjelaskan tentang kontroversi-kontroversi yang ada dalam sistem Bitcoin. Sebab tentu saja tidak ada sistem yang sempurna di dunia ini, begitu juga dengan Bitcoin.
- **Bagian Keenam** membahas AltCoin, yakni *alternative coin*, jenis-jenis *cryp-*

tocurrency lain yang berkembang seiring kesuksesan Bitcoin. Pokok bahasan bagian ini terbatas pada 5 *cryptocurrency* terbesar, yakni Ripple, Litecoin, Dogecoin, Peercoin, Ethereum. Pada bagian ini Anda juga dapat menemukan peluang untuk melakukan jual beli lintas mata uang dalam *cryptocurrency*.

- **Bagian Ketujuh** menggambarkan bagaimana teknologi blockchain semakin berkembang di berbagai industri. Perbankan misalnya, tertarik mengadopsi blockchain untuk meningkatkan transparansi dan mengurangi biaya transaksi di dalam sistem mereka.

Penulis mengucapkan terima kasih kepada Dr. Joseph Liu dan Dr. Ron Steinfeld sebagai *thesis supervisor*, Dr. Phu Dung Le sebagai *advisor*, Oscar Darmawan dan Vinsensius Sitepu yang telah memberi berbagai saran yang sangat bermanfaat. Bung Vinsen juga saya kenal cukup aktif menulis artikel tentang Bitcoin di *Analisa* dan *Kontan* (Kelompok Kompas-Gramedia) sejak 2014. Terima kasih pula saya ucapkan kepada Bang Fauzan sebagai editor buku ini.

Juga kepada penerbit Puspantara atas kepercayaannya kepada penulis terhadap penyusunan buku ini. Ucapan terima kasih juga kepada Lembaga Pengelola Dana Pendidikan Kementerian Keuangan Republik Indonesia, yang telah membiayai pendidikan penulis di negeri seberang.

Penulis berharap semoga buku ini bermanfaat bagi perkembangan teknologi di tanah air.

Melbourne, 2016

Dimaz Ankaa Wijaya

KATA PENGANTAR

OSCAR DARMAWAN

SEBUAH KONSEP SISTEM KEUANGAN YANG TERDESENTRALISASI ADALAH SESUATU YANG SAYA IDAMKAN SEBELUMNYA JAUH BAHKAN SEBELUM SAYA MENGENAL BITCOIN, MATA UANG UNIK INI, PADA TAHUN 2012.

Saat itu saya merasa itu adalah sesuatu yang mustahil adanya sebuah mata uang digital, tetapi dapat berjalan terdesentralisasi, tanpa ada pihak yang mengatur dan tetap berjalan dengan sangat aman. Saya ikut menjadi saksi sejarah dalam 10 tahun terakhir bagaimana dua raksasa e-money sentralisasi tumbang dan sebagai pengguna di Indonesia menjadi salah satu orang yang dirugikan; e-gold dan liberty reserve.

Saya adalah *forex trader* dan konsultan IT, yang karena kedua *passion* saya tersebut membuat saya menggunakan e-money lintas negara tersebut. Tidak ada perlin-

dungan hukum yang berarti bagi kita orang Indonesia dan “Big Brother” bisa dengan mudahnya menutup perusahaan e-money yang dirasa tidak berjalan dengan baik membuat saya merasa sentralisasi e-money untuk international bukan lah opsi yang memungkinkan

Perkenalan saya dengan Bitcoin pertama kali dari sahabat saya, William Sutanto, sekarang menjadi CTO Bitcoin.co.id, justru membuat saya cenderung skeptis seperti kebanyakan orang, karena pengalaman-pengalaman buruk saya di e-money tersebut. Membuat saya merasa sok tahu dan mengang-gap bitcoin cuma sekedar e-money lainnya.

Saya merasa tidak mungkin dan tidak berusaha mempelajarinya terlebih dahulu, tetapi saya merasa beruntung tidak berhenti di titik skeptis tersebut. Saya mencoba memperlajarinya pada akhirnya, dan wow! seperti tertembak sebuah peluru di otak saya, ketika memahami bagaimana konsep dan cara kerja Bitcoin. Sebuah jawaban dari sesuatu yang saya harapkan dulu: sistem keuangan desentralistik, sebuah emas digital, sebuah mata uang desentralistik: sistem alat bantu pembayaran internet yang ideal; sebuah pencatatan buku besar transaksi yang terdesentralisasi.

Saya berharap Anda seperti saya dahulu yang tidak berhenti hanya di satu titik: skeptis seperti 99% masyarakat dunia, tapi jadilah berani untuk mempelajarinya, karena seperti banyak semboyan para orang sukses: Kesuksesan itu hanya diperoleh oleh orang yang berani berlari ke garis *finish*, bukan oleh orang yang berhenti di garis *start*.

Bitcoin masih dalam tahap yang sangat baru. Inovasi teknologi dalam kurun waktu 7 tahun hanyalah seperti tahap percobaan. Dan tahukah Anda kalau bitcoin sendiri memang masih dalam tahap uji coba (*beta version*), yang memiliki *capital market* hampir sebesar 7 miliar dolar AS.

Inovasi teknologi sistem keuangan Bitcoin yang disebut dengan *blockchain* sendiri saat ini menjadi sebuah percobaan inovasi teknologi yang melibatkan berbagai perusahaan ternama: Microsoft, IBM, Samsung, Dell dan puluhan bank raksasa: Barkeley, Visa, Mastercard, Standard Chartered, Morgan Stanley, UBS, dan Citibank. Bahkan bursa efek Nasdaq sudah memulai mencatat transaksinya ke dalam *blockchain*.

Bahkan tidak jarang sekarang MLM mulai memanfaatkan ketenaran Bitcoin untuk menipu berbagai orang awam yang tidak paham Bitcoin dan ingin menjadi bagian dari sistem keuangan terdesentralisasi ini. Berhati-hatilah justru mendapatkan info dari orang yang salah dan membuat anda menjadi sebuah korban dari sistem Ponzy ini.

Buku Bitcoin yang ditulis Dimaz ini menurut saya sangat menarik, karena mencoba menceritakan Bitcoin secara sederhana di luar dari kompleksitas teknologi Bitcoin. Dimaz berhasil menjelaskan kesalahpahaman yang terjadi di tengah-tengah masyarakat awam mengenai Bitcoin.

Saya mengenal Dimaz sendiri sudah cukup lama, dan saya kira Dimaz adalah seseorang yang dapat membantu Anda memahami tentang teknologi Bitcoin ini. Saya harapkan buku ini menjadi salah satu sumber informasi mengenai Bitcoin di Indonesia.

Oscar Darmawan

CEO Bitcoin Indonesia (Bitcoin.co.id)

For the love of my life, Indah and Sophia.

Di dalam buku ini, penggunaan kata **Bitcoin** dan **bit-coin** merujuk pada hal yang berbeda. **Bitcoin** dengan huruf kapital di awal kata, merujuk pada sistem pembayaran elektronik yang terdesentralisasi dan merupakan pionir dari sistem *cryptocurrency* atau mata uang berbasis kriptografi. Sementara **bitcoin** tanpa huruf kapital di awal kata merujuk pada uang elektronik yang digunakan untuk bertransaksi.

PENDAHULUAN

SIAPA SIH YANG TIDAK BUTUH UANG? ANDA DAN SAYA TENTUNYA, PERLU UANG. UANG MERUPAKAN BAGIAN YANG TAK TERPISAHKAN DALAM KEHIDUPAN MANUSIA.

Menurut teori makroekonomi sebagaimana disampaikan oleh Mankiw (2014), uang memiliki 3 fungsi, yakni sebagai alat tukar, sebagai alat penyimpan nilai untuk masa yang akan datang, dan sebagai satuan nilai. Sebagai alat tukar, uang digunakan untuk menukar barang yang satu dengan barang yang lain, atau antara barang dan jasa. Sebagai alat penyimpan nilai, uang berfungsi dalam kegiatan menabung untuk dapat dibelanjakan di masa depan. Sebagai satuan nilai, uang dipakai untuk menunjukkan nilai sebuah barang atau jasa, misalnya sebuah apel yang memiliki nilai setara dengan Rp. 10 ribu.

Uang

Sejak munculnya peradaban manusia, kebutuhan akan adanya uang sebagai sarana tukar-menukar dalam kegiatan perdagangan semakin mendesak. Sebagaimana kita baca dalam buku-buku sejarah, uang sebagai alat tukar memiliki banyak bentuk, mulai dari garam, kepingan kerang, sampai pada logam berharga seperti emas dan perak. Kemudian dengan semakin majunya kehidupan manusia, dikenal adanya uang kertas dan koin seperti yang biasa dipakai dalam kehidupan sehari-hari sekarang ini.

Perkembangan teknologi yang semakin pesat memungkinkan penciptaan jenis uang baru yang disebut uang digital. Uang digital, sebagaimana tercermin dalam namanya, hanya ada dalam ruang lingkup dunia digital. Anda yang hobi bermain game *online* tentunya pernah mendengar bahwa uang yang dihasilkan dalam game *online* dapat diperjualbelikan atau ditukar dengan rupiah, atau sebaliknya, menukar rupiah dengan uang dalam game *online*. Sementara uang dalam game *online* tersebut dapat dipakai untuk membeli barang-barang yang dijual dalam game, seperti senjata maupun obat penyembuh.

Uang digital juga semakin banyak digunakan untuk menggantikan uang fisik yang berbentuk koin maupun kertas. Uang digital atau *e-cash* tersebut merupakan representasi dari mata uang yang dimiliki. Sebagai contoh kita mengenal kartu Flazz dari Bank BCA, Brizzi dari Bank BRI, maupun Mandiri e-Money. Demikian pula uang digital yang dibuat oleh operator telekomunikasi seperti T-Cash dari Telkomsel, Dompetku dari Indosat, dan XL Tunai dari XL Axiata (Bangsaid, 2015). Uang digital diciptakan untuk mempermudah transaksi tanpa harus menyediakan uang fisik yang sulit dibawa dalam jumlah yang banyak. Uang digital juga lebih aman dalam hal mengurangi risiko menjadi target kejahatan seperti perampokan dan penjabretan.

Uang fisik dalam bentuk kertas maupun koin yang diterbitkan oleh bank sentral disebut dengan uang fiat (*fiat currency*). Sebagai contoh uang fiat adalah rupiah (Rp) yang diterbitkan oleh Bank Indonesia dan dolar AS (US\$) yang diterbitkan oleh The Fed. Sementara uang digital seperti yang telah disebut di atas juga termasuk dalam kategori uang fiat, karena nilainya sama dengan uang fisik yang direpresentasikannya. Uang digital merupakan cikal bakal munculnya cryptocurrency, mata uang berbasis kriptografi. Untuk membantu Anda memahami perbedaan antara uang fiat dan cryptocurrency, berikut adalah tabel perbandingan karakteristik di antara keduanya.

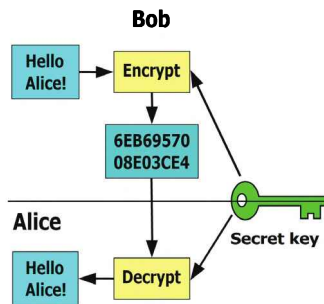
Karakteristik	Uang Fiat	Cryptocurrency
Bentuk	Fisik maupun Digital	Digital
Perantara transaksi	Perbankan dan Jasa Keuangan	Peer-to-peer
Pencetakan uang baru	Bank Sentral	Penambang
Validator	Perbankan dan Jasa Keuangan	Node dan Miner
Sistem Validasi	Identitas	Tanda tangan digital
Suplai uang	Tidak terbatas	Terbatas
Penjamin	Pemerintah	Tidak Ada
Penentu nilai tukar	Pasar Uang dan Pemerintah	Pasar

Kriptografi

Kriptografi adalah sebuah cabang ilmu komputer yang mempelajari cara menyembunyikan informasi. Melalui kriptografi, sebuah pesan rahasia diacak menjadi pesan yang seolah-olah tidak berbentuk, dan dikirimkan kepada pihak yang dituju. Sementara itu,

hanya pihak yang dituju sajalah yang dapat mengartikan pesan acak tersebut dan mengubahnya kembali menjadi pesan rahasia dari sang pengirim.

Sederhananya begini. Anda, berperan sebagai agen rahasia, sedang menyusup ke sebuah organisasi kriminal. Dalam penyamaran, Anda mengetahui bahwa organisasi yang Anda susupi sedang merencanakan serangan ke pusat perbelanjaan terbesar di tanah air. Tentunya Anda harus mengirim pesan pada dinas rahasia yang mengutus Anda, namun tidak menginginkan orang-orang dalam organisasi kriminal tersebut mengetahui pesan itu. Di sinilah Anda memanfaatkan kriptografi, yakni melakukan enkripsi pesan rahasia menjadi pesan acak dan mengirimkan pesan acak tersebut pada dinas rahasia. Sementara, untuk memecahkan pesan acak tersebut, dinas rahasia melakukan dekripsi dan mengubah pesan acak kembali menjadi pesan rahasia yang dapat dimengerti. Salah satu pengaplikasian teknik kriptografi yang terkenal oleh militer Jerman menggunakan mesin Enigma, dapat Anda saksikan dalam film berjudul “The Imitation Game” yang diluncurkan pada tahun 2014.



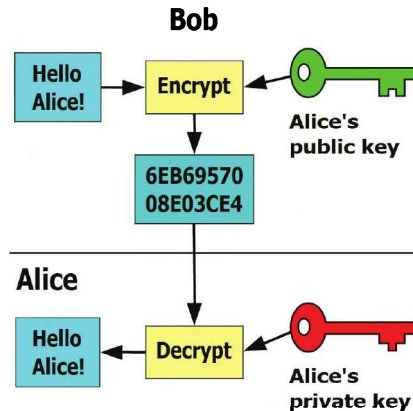
Gambar 1. Ilustrasi Kriptografi simetris. Sumber: Wikipedia

Public Key Cryptography

Public key cryptography (PKC) merupakan teknik kriptografi yang memerlukan 2 jenis kunci, yakni kunci publik (*public key*) dan kunci privat (*private key*) yang pertama kali dicetuskan oleh Diffie and Hellman (1976). Kunci publik boleh disebarluaskan, sementara kunci privat harus disimpan dengan baik. PKC sering disebut juga dengan kriptografi asimetris, karena karakteristiknya yang memiliki 2 buah kunci, berbeda dengan kriptografi simetris yang hanya memerlukan 1 kunci rahasia. Kunci-kunci ini berupa deretan angka-angka yang memiliki panjang tertentu.

Kriptografi asimetris memiliki keuntungan jika dibandingkan dengan kriptografi simetris dalam hal pertukaran kunci. Ketika menggunakan kriptografi simetris, pihak-pihak yang berkomunikasi harus menjaga agar kunci rahasia tidak bocor ke tangan orang yang tidak

berhak. Oleh karena itu terkadang menjadi kesulitan tersendiri dalam mengirim informasi kunci rahasia di antara pihak-pihak tersebut secara aman. Dengan menggunakan kriptografi asimetris, pertukaran informasi kunci rahasia tidak diperlukan.



Gambar 2. Public Key Cryptography. Sumber: Wikipedia

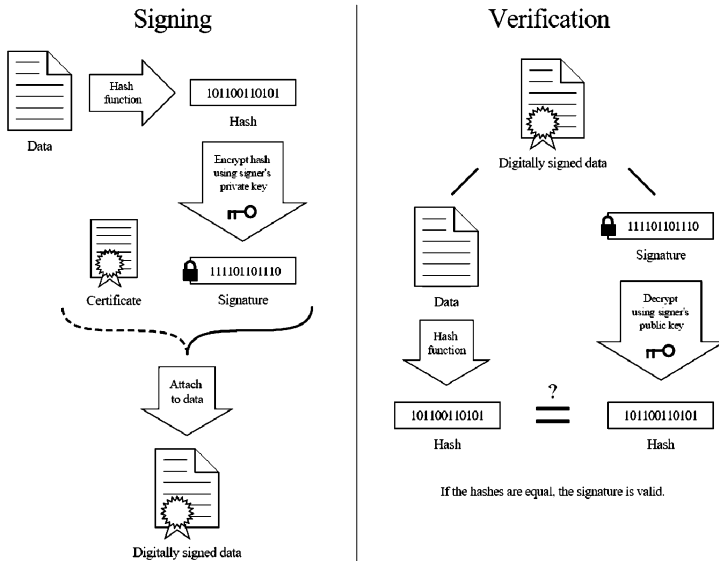
Cara kerja PKC dapat diilustrasikan seperti pada gambar 2. Misalnya, Bob ingin mengirim pesan pada Alice. Pertama-tama, Alice membuat sepasang kunci, yakni kunci privat dan kunci publik. Kunci privat disimpan oleh Alice, sementara kunci publik dikirimkan kepada Bob. Menggunakan kunci publik milik Alice, Bob melakukan enkripsi atas pesan yang ingin dikirimkannya pada Alice kemudian mengirimkan hasil enkripsi tersebut pada Alice. Setelah menerima informasi dari Bob, maka Alice dapat melakukan proses dekripsi dengan menggunakan kunci privat milik Alice, kemudian menghasilkan pesan yang sama seperti yang diinginkan oleh Bob.

Terdapat beberapa teknik PKC yang ada, di antaranya RSA (Rivest, Shamir, & Adleman, 1978), ElGamal (ElGamal, 1985), dan Elliptic Curve (Koblitz, 1987; Miller, 1985). Bitcoin sendiri menggunakan metode Elliptic Curve dalam sistemnya karena tingkat keamanan yang baik dan panjang kunci yang rasional. Kunci privat yang dihasilkan oleh Elliptic Curve disimpan dan dikelola oleh aplikasi dompet Bitcoin, sementara kunci publik diproses lebih lanjut menjadi alamat Bitcoin. Oleh sebab itu, menyebarkan alamat Bitcoin tidak akan menyebabkan uang pengguna dicuri, sebab kunci publik memang aman untuk disebarluaskan. Selama kunci privat dijaga dengan baik, uang yang berada di dalam alamat Bitcoin akan aman.

Tanda Tangan Elektronik

Tanda tangan elektronik dapat diibaratkan seperti tanda tangan di atas sebuah cek.

Saat seseorang ingin mencairkan uang menggunakan cek, maka orang tersebut menuliskan nominal yang diinginkan dan membubuhkan tanda tangannya. Bank kemudian melakukan verifikasi atas tanda tangan tersebut dan membandingkannya dengan tanda tangan pada saat orang tersebut membuka rekening giro. Apabila verifikasi berhasil, maka bank mencairkan uangnya, namun bila tanda tangan tersebut tidak berhasil diverifikasi, maka permintaan pencairan uang ditolak.



Gambar 3. Cara kerja tanda tangan elektronik. Sumber: wikipedia

Tanda tangan elektronik merupakan teknik kriptografi yang memanfaatkan PKC untuk memverifikasi identitas seseorang atas sebuah dokumen atau informasi elektronik. Tujuannya adalah untuk menentukan apakah dokumen tersebut dibuat oleh orang yang sah. Tanda tangan elektronik berasumsi bahwa kunci privat yang digunakan untuk membuat tanda tangan elektronik hanya diketahui oleh orang yang bersangkutan. Proses tanda tangan elektronik terdiri atas 2 bagian, yaitu proses penanda tangan (*signing*) dan proses verifikasi (*verification*).

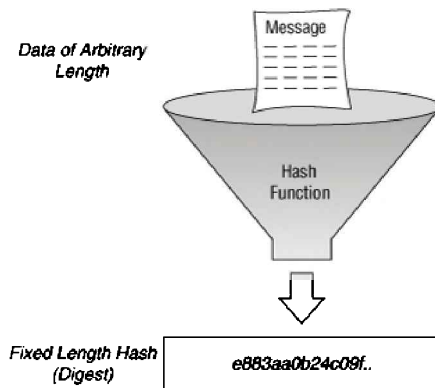
Proses penanda tangan dimulai dari penyiapan dokumen elektronik. Kemudian, dokumen elektronik tersebut dihitung nilai *hash*-nya. Nilai *hash* tersebut kemudian dienkripsi menggunakan kunci privat yang dimiliki. Hasil enkripsi inilah yang disebut dengan tanda tangan elektronik. Tanda tangan elektronik yang ditempelkan pada dokumen elektronik tersebut kemudian dikirimkan kepada orang yang berkepentingan.

Proses verifikasi dimulai dari perolehan dokumen elektronik beserta tanda tangan elektroniknya. Kemudian, dokumen tersebut dihitung nilai hash-nya. Sementara atas tanda tangan elektronik dilakukan proses dekripsi menggunakan kunci publik milik pembuat dokumen. Hasil dekripsi tersebut adalah nilai hash. Kedua nilai hash ini kemudian dibandingkan, apabila nilainya sama maka tanda tangan elektronik tersebut sah.

Bitcoin memanfaatkan teknik tanda tangan elektronik ECDSA (Elliptic Curve Digital Signature Algorithm) (Bitcoin Wiki, 2013a) dengan spesifikasi secp256k1 (Brown, 2010). Tanda tangan elektronik ini digunakan untuk memastikan apakah pengguna merupakan pemilik sah atas uang yang berada dalam alamat Bitcoin yang diklaim oleh pengguna tersebut.

Fungsi Hash

Fungsi *hash* (*hash function*) merupakan salah satu teknik kriptografi untuk menghitung nilai unik dari sebuah data. Fungsi *hash* dapat diibaratkan sebagai sidik jari elektronik (*digital fingerprint*) dari informasi elektronik. Sidik jari elektronik berguna untuk menentukan orisinalitas sebuah dokumen elektronik. Dua dokumen elektronik yang berbeda akan memiliki nilai hash yang berbeda, itulah sebabnya apabila sebuah dokumen telah mengalami perubahan, maka nilai *hash* juga akan berubah. Sebuah dokumen dengan panjang berapapun akan menghasilkan nilai *hash* dengan panjang tertentu sesuai dengan spesifikasi fungsi *hash* yang digunakan.



Gambar 4. Ilustrasi Fungsi Hash (Tesauro, 2015)

Bitcoin menggunakan beberapa fungsi *hash* dalam aplikasinya, di antaranya RIPEMD160 (Bitcoin Wiki, 2014b) dan SHA256 (Wikipedia, 2015f). RIPEMD160 digunakan salah satunya dalam proses penghitungan alamat Bitcoin, sementara SHA256 digunakan dalam penghitungan nilai *hash* transaksi Bitcoin.

Bitcoin

Bitcoin merupakan pionir dalam *cryptocurrency*. Ia diciptakan oleh seseorang yang menyebut dirinya Satoshi Nakamoto, walaupun sampai saat ini tidak ada yang mengetahui jati diri sebenarnya dari Satoshi Nakamoto. Satoshi meletakkan prinsip-prinsip dasar *cryptocurrency* melalui *whitepaper* yang berjudul “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008). Walaupun Bitcoin bukan satu-satunya *cryptocurrency* yang ada di dunia ini, Bitcoin masih tetap memiliki nilai jual paling tinggi dibandingkan *cryptocurrency* lainnya.

Bitcoin disusun oleh Satoshi Nakamoto untuk menghapus kebutuhan akan adanya pihak pengendali pusat yang mengontrol seluruh sistem keuangan. Beberapa konsep yang digunakan adalah adanya sebuah basis data bernama *blockchain*, yaitu berupa “buku besar” (*ledger*) yang dapat dilihat oleh semua orang, sehingga semua orang dapat melihat dan memvalidasi transaksi keuangan yang dilakukan di dalam *blockchain* tersebut (Antonopoulos, 2014). Buku besar ini mencatat seluruh transaksi yang terjadi, sehingga alur transaksi dapat dilihat dengan mudah. *Blockchain*, atau terjemahan bebasnya rantai blok, sesuai namanya tersusun atas blok-blok yang dihubungkan satu sama lain.

Sebuah blok bernomor n terhubung dengan blok bernomor $n-1$ dan blok bernomor $n+1$. Blok-blok tersebut berisi transaksi-transaksi Bitcoin yang dikumpulkan dalam selang waktu tertentu. Transaksi-transaksi tersebut divalidasi terlebih dahulu sebelum dimasukkan ke dalam sebuah blok. Kemudian, sebuah blok yang berisi kumpulan transaksi harus divalidasi juga melalui proses yang disebut mining (menambang) yang dilakukan oleh penambang dengan menggunakan komputer atau alat yang biasa disebut dengan ASIC (Application Specific Integrated Circuit).

Banyak orang tertarik pada Bitcoin karena berbagai alasan. Bisa karena alasan tertarik pada teknologi, pada fungsionalitasnya, atau pada peluangnya untuk mendapat keuntungan atas selisih harga di pasaran. Bitcoin menawarkan solusi atas permasalahan-permasalahan di bidang keuangan dengan menggunakan teknologi yang murah dan mudah diimplementasikan dan diintegrasikan ke dalam sistem yang sudah ada.



Gambar 5. Logo Bitcoin. Sumber : Bitcoin Wiki

Bitcoin adalah uang. Tetapi, tidak seperti rupiah yang Anda miliki sekarang ini, Bitcoin memiliki cara kerja yang sangat berbeda. Jika kita mengenal adanya Bank Indonesia se-

bagai bank sentral yang mengelola peredaran uang rupiah, Anda tidak akan menemukan bank sentral apapun di dalam sistem Bitcoin yang mengelola peredaran Bitcoin. Bitcoin juga tidak diterbitkan oleh negara manapun atau pihak manapun di dunia ini.

Jadi, bagaimana kita bisa yakin kalau Bitcoin adalah uang jika tidak ada yang mengaturnya? Sayangnya, kita tidak memiliki jaminan bahwa Bitcoin akan tetap lestari sebagai uang. Sebagaimana ketika kita menggunakan uang dalam game *online*, kita pun tidak tahu apakah kita dapat tetap membeli barang-barang dalam game atau tidak jika suatu saat pengelola game tersebut menutup layanan game miliknya. Bahkan di masa lampau, bagaimana kita yakin kalau alat tukar seperti kepingan kerang dapat diterima oleh orang lain sebagai ganti barang-barang yang dijualnya?

Bitcoin tidak memiliki apapun atau siapapun untuk menjaminnya, dan komunitas pengguna Bitcoin-lah yang sepakat menggunakannya sebagai uang. Sebagai ilustrasi, dulu semasa kecil, kami sering bermain masak-masakan dan menggunakan pecahan genting rumah, atau biasa kami sebut *kereweng*, sebagai uang. Kami sebagai komunitas bersepakat menerima *kereweng* tersebut sebagai alat tukar dan jadilah itu sebagai uang. Demikian juga dengan Bitcoin, dimulai dari komunitas kecil di dunia maya, Bitcoin mulai diterima oleh lebih banyak lagi komunitas sebab mereka bersepakat menerima Bitcoin sebagai alat tukar.

Lalu, jika Bitcoin disebut dengan uang, seperti apa bentuknya? Untuk menjawab pertanyaan ini, kita perlu memahami prinsip uang digital. Uang digital tidak berbentuk. Selayaknya kita mentransfer menggunakan SMS banking, kita dapat melihat jumlah uang yang didebet di layar ponsel. Proses itu terhubung dengan *server* bank terkait yang menyimpan data uang digital kita. Demikian halnya Bitcoin, jumlah uang kita tersimpan di dalam jaringan internet, bukan di komputer *server* manapun. Walaupun demikian tidak ada orang lain yang bisa membelanjakan bitcoin itu tanpa sepengetahuan kita, sebab kita menyimpan kunci rahasia sebagaimana telah dijelaskan tentang prinsip kriptografi. Menggunakan kunci rahasia ini, kita dengan bebas menggunakan bitcoin milik kita sendiri tanpa takut orang lain mencuri bitcoin kita meskipun mereka mengetahui alamat Bitcoin dan jumlah bitcoin yang kita miliki. Itulah sebabnya, selama kunci rahasia ini aman, maka bitcoin milik kita juga aman.

Kunci rahasia ini bertindak seperti kombinasi PIN ATM. Seseorang yang mengetahui nomor PIN ATM dan memiliki kartu ATM kita, dapat mengambil dengan bebas uang dari rekening kita. Untuk itulah, menjaga kunci rahasia Bitcoin menjadi hal yang sangat penting, apalagi bila Anda berencana untuk memiliki sejumlah besar bitcoin. Apalagi, kita tidak bisa mengembalikan kunci rahasia Bitcoin andaikata kunci itu hilang, sebab hanya itulah yang menjadi bukti kepemilikan bitcoin kita, sebab telah dijelaskan pula bahwa di dalam sistem Bitcoin, tidak ada pihak yang memiliki kontrol atas bitcoin. Oleh karena itu, jika kunci rahasia Bitcoin itu hilang, maka bitcoin yang kita miliki tidak akan

pernah bisa dibelanjakan lagi.

Bitcoin merupakan uang yang berbasis Internet. Artinya, untuk melakukan transaksi dengan Bitcoin, kita harus terhubung dengan Internet. Oleh karena itu, kita dapat bertransaksi dengan siapapun di dunia ini selama kita mengetahui alamat Bitcoin tujuan. Bitcoin tidak mengenal jarak, dan oleh sebab itu dapat digunakan dalam transaksi internasional.

Namun demikian, Bitcoin sama sekali berbeda dengan layanan perbankan maupun layanan keuangan lain seperti PayPal. Sebab, Bitcoin sendiri adalah uang, dan hal ini sangatlah berbeda dengan PayPal yang hanya menyediakan fasilitas bertransaksi atas mata uang dan ia sendiri bukan merupakan uang. Meskipun begitu, Bitcoin memiliki fleksibilitas yang sama bahkan lebih baik dibandingkan PayPal, sebab tidak memerlukan verifikasi identitas diri dan persyaratan-persyaratan tertentu, yang bagi banyak orang hal itu merupakan sebuah kesulitan tersendiri. Untuk memulai penggunaan Bitcoin, kita hanya perlu melakukan instalasi dompet Bitcoin (*Bitcoin wallet*) di dalam komputer atau *smartphone* kita, dan kemudian kita siap untuk berpartisipasi untuk membeli koin dan membelanjakannya di toko-toko yang menerima pembayaran dalam bentuk Bitcoin.

Mengapa Bitcoin memiliki nilai? Alstyne (2014) menyampaikan 4 alasan mengapa Bitcoin dapat diterima sebagai uang. *Pertama*, aspek teknis. Teknologi Bitcoin dianggap mampu mengatasi permasalahan di mana Bitcoin tidak bisa serta-merta disalin seperti halnya dokumen elektronik yang kemudian dibelanjakan lagi. Karena Bitcoin memiliki sistem transparan, maka semua transaksi dapat diaudit dan dilihat asal muasalnya, sehingga tidak ada orang yang asal memasukkan uang ciptaannya sendiri ke dalam sistem Bitcoin.

Kedua, ongkos transaksi yang murah memberi kesempatan bagi toko-toko *e-commerce* kecil untuk memperoleh keuntungan yang lebih besar karena penjualan mereka tidak banyak mengalami pemotongan seperti halnya jika mereka menerima pembayaran menggunakan kartu kredit.

Ketiga, sistem Bitcoin mampu mengatasi masalah pemalsuan yang terjadi pada kartu kredit. Sepanjang kunci rahasia dapat dijaga dengan baik, maka pengguna tidak akan kehilangan uangnya.

Keempat, Bitcoin memiliki nilai karena banyak orang mengakuinya sebagai uang, dan semakin banyak pula toko-toko yang menerima pembayaran dalam bentuk Bitcoin.

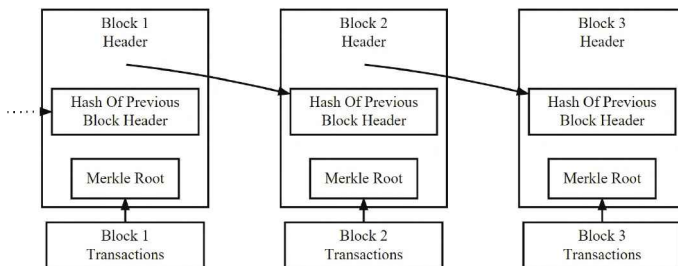
Terdapat berbagai alasan mengapa Bitcoin lebih unggul dibandingkan uang tradisional, salah satunya adalah biaya transaksi yang sangat rendah. Sebuah transaksi internasional biasanya dikenai biaya sekitar 5% dari total nilai yang ditransaksikan. Namun menggunakan Bitcoin, biaya tersebut bisa ditekan menjadi sangat rendah tergantung

pada ukuran transaksi. Mudah-mudahan, sebuah transaksi yang hanya melibatkan 1 alamat pengirim dan 1 alamat tujuan hanya menghabiskan biaya sekitar 5 sen dolar atau Rp 500 berapapun jumlah bitcoin yang dikirimkan. Biaya yang dikenakan pada setiap transaksi Bitcoin dibayarkan kepada para penambang Bitcoin yang memverifikasi transaksi tersebut. Transaksi Bitcoin juga dapat dilakukan dengan instan. Bila transaksi pada sistem keuangan tradisional membutuhkan waktu beberapa jam sampai beberapa hari, transaksi Bitcoin hanya membutuhkan waktu sekitar 10 menit.

Bitcoin memiliki keunggulan dalam hal nilainya yang cenderung semakin menanjak. Pada krisis Yunani yang terjadi beberapa waktu yang lampau, dengan nilai tukar mata uang lokal yang semakin melemah dibandingkan mata uang luar negeri, masyarakat mulai banyak yang beralih dengan Bitcoin yang dianggap lebih stabil nilai tukarnya. Nilai Bitcoin cenderung lebih dipengaruhi oleh jumlah permintaan dan penawaran pasar dan tidak dipengaruhi oleh kondisi politik sebuah negara tertentu, oleh sebab itu beberapa orang menganggap bahwa Bitcoin menjadi alat investasi menarik. Meski demikian, Bitcoin sebagai alat investasi memiliki risiko tinggi atas kehilangan nilai pasarnya.

Blockchain

Sebagaimana telah dijelaskan, Bitcoin menyimpan seluruh informasinya dalam sebuah basis data yang disebut *blockchain* di dalam jaringan Internet. Seperti namanya, *blockchain* tersusun atas blok-blok yang saling terkait satu sama lain dan memiliki nomor berurutan. Blok-blok tersebut saling terkait karena nilai *hash* sebuah blok akan dimasukkan dalam proses pembuatan blok berikutnya. Dengan menggunakan teknik ini, maka usaha untuk mengubah informasi di dalam sebuah blok akan semakin sulit sebab harus mengubah blok-blok berikutnya juga. Hal ini dikarenakan nilai *hash* akan berubah ketika ada perubahan sesedikit apapun pada data yang ada di dalam blok. Setiap blok dalam *blockchain* terhubung satu sama lain. Blok pertama dalam *blockchain* disebut *genesis block*. Blockchain memiliki struktur sebagai berikut.

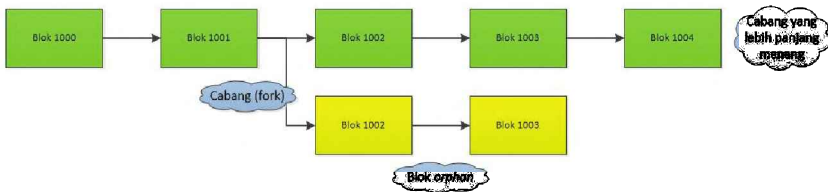


Gambar 6. Struktur Blockchain (Harding, 2015)

Struktur *blockchain* memang sangat berbeda dibandingkan dengan struktur basis data biasa, di mana Anda bisa menemukan konsep *field* (kolom) dan *record* (baris) dalam basis data relasional. Bitcoin tidak menggunakan struktur basis data relasional, sebab memerlukan proteksi yang kuat atas data yang ada di dalamnya. *Blockchain* tidak memerlukan fitur edit (ubah) seperti halnya basis data biasa, karena semua informasi yang sudah dimasukkan dalam *blockchain* bersifat final dan tidak dapat diubah kembali. Untuk menambahkan informasi baru dalam *blockchain* tidak dapat serta merta menggunakan perintah *insert* (tambah), namun blok baru perlu memenuhi kriteria tertentu yang disebut dengan tingkat kesulitan (*difficulty level*). Tingkat kesulitan ini ditentukan oleh aplikasi Bitcoin *core* setiap kira-kira 2 minggu sekali.

Blok-blok baru yang ditambahkan ke dalam *blockchain* dibuat oleh para penambang dalam proses menambang menggunakan peralatan komputasi *hash*. Para penambang ini berkompetisi untuk membuat blok baru yang sah dan sesuai kriteria tingkat kesulitan yang ditentukan. Pada umumnya, sebuah blok baru dihasilkan oleh seorang (atau sekelompok) penambang, namun ada kalanya lebih dari 1 blok baru yang dihasilkan oleh penambang yang berbeda yang sama-sama memenuhi kriteria yang ditentukan.

Hal ini membuat *blockchain* menjadi bercabang (*fork*). Pada saat hal ini terjadi, maka dimulailah proses *voting* oleh para penambang. Caranya, para penambang memilih 1 di antara beberapa blok baru ini dalam proses menambang mereka. Setelah selang beberapa waktu, maka akan ada 1 cabang rantai yang lebih panjang dibandingkan cabang rantai yang lain. Saat hal ini terjadi, maka seluruh sistem Bitcoin akan menggunakan cabang yang paling panjang tersebut dan menghapus seluruh cabang yang lain. Blok-blok yang berada dalam cabang yang tidak terpakai disebut blok *orphan* ("yatim piatu") dan menjadi tidak berlaku. Sementara semua transaksi yang telah terekam dalam blok-blok *orphan* akan dimasukkan ke dalam blok baru.



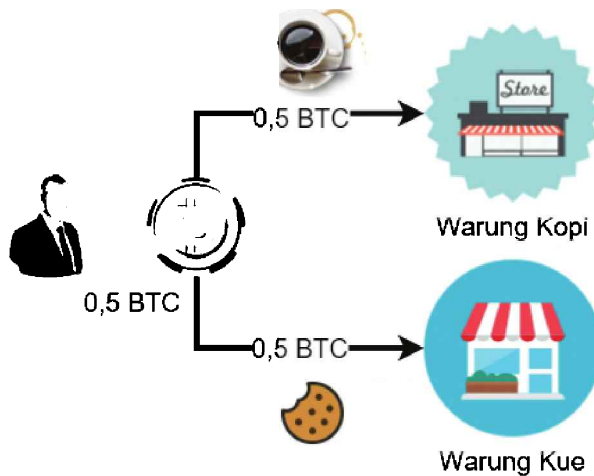
Gambar 7. Blok orphan pada Blockchain

Selain *blockchain*, terdapat sebuah basis data lain dalam sistem Bitcoin yang disebut dengan UTXO (Unspent Transaction Output). UTXO memuat informasi seluruh output yang belum digunakan. Artinya, jika Anda memiliki saldo pada alamat Bitcoin Anda, maka informasi saldo tersebut berada dalam basis data UTXO. UTXO memiliki fungsi

yang berbeda dibandingkan dengan *blockchain*. Ketika informasi dalam *blockchain* bersifat permanen, informasi dalam UTXO bersifat sementara (*temporer*). Ketika sebuah *output* telah digunakan, maka informasi *output* tersebut dihapus dari UTXO. UTXO tidak disimpan di dalam *harddisk*, melainkan di dalam RAM, agar akses informasinya lebih cepat. Dan sama halnya dengan *blockchain*, UTXO akan dikelola oleh *node* Bitcoin.

Double Spending

Double spending merupakan kejadian di mana uang yang sama dibelanjakan lebih dari 1 kali, yang tentu saja tidak diinginkan. *Double spending* tidak akan terjadi dalam sistem uang fisik, namun bisa timbul dalam sistem mata uang elektronik, sebab data elektronik memiliki sifat mudah disalin/ digandakan sebanyak yang diinginkan.



Gambar 8. Ilustrasi Double Spending

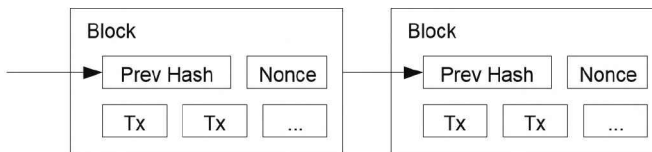
Ilustrasi pada Gambar 8 menjelaskan tentang *double spending*. Misalnya Bob memiliki uang sebanyak 0,5 BTC. Ia membelanjakan uangnya untuk membeli secangkir kopi di warung kopi seharga 0,5 BTC. Pada saat yang sama, ia membeli sepotong kue seharga 0,5 BTC di warung kue. Tentu saja hal ini tidak boleh dilakukan, karena Bob hanya berhak membelanjakan uangnya untuk membeli kopi saja atau kue saja.

Sistem Bitcoin memastikan bahwa uang yang dimiliki seseorang hanya bisa dibelanjakan 1 kali saja. Bitcoin menyusun sistemnya sedemikian rupa sehingga *double spending* tidak mungkin terjadi dalam transaksi Bitcoin. Caranya adalah dengan mempublikasikan *blockchain* yang merupakan catatan atas seluruh transaksi yang terjadi dalam sistem Bitcoin. Dengan informasi yang terbuka seperti ini, maka sebelum menerima pemba-

garan, dana tersebut dapat diaudit dengan menelusuri seluruh rekaman transaksi yang telah dilakukan sebelumnya.

Proof of Work

Konsep tentang buku besar terbuka pertama kali dipaparkan oleh Dai (1998) dalam konsep uang yang disebut dengan B-money yang turut andil dalam terbentuknya *cryptocurrency*. Kemudian, *cryptocurrency* juga dilengkapi dengan teknik *proof-of-work* (PoW) yang disampaikan oleh Back (2002) dalam sistem yang disebut dengan Hashcash. Hashcash pertama kali digunakan untuk memerangi *email spam*. PoW yang terdapat pada Hashcash merupakan sebuah teknik di mana komputer harus melakukan perhitungan matematis dengan tingkat kesulitan tertentu sebelum diperbolehkan mengirim email. Dengan demikian, waktu yang diperlukan oleh spammer semakin besar dan pada akhirnya jumlah *email spam* akan berkurang. Demikian pula dengan PoW yang terdapat pada Bitcoin digunakan untuk melindungi buku besar (*blockchain*) dari perubahan yang tidak diinginkan.



Gambar 9. Proof of Work (Nakamoto, 2008)

PoW pada Bitcoin bekerja dengan cara berikut. Seluruh informasi yang ada di dalam sebuah calon blok dihitung nilai *hash*-nya. Nilai *hash* yang dihasilkan ini harus memenuhi kriteria tingkat kesulitan (*difficulty*) yang telah ditentukan oleh sistem. Apabila nilai *hash* tersebut tidak memenuhi kriteria, maka perhitungan akan diulang dengan melakukan perubahan nilai *nonce* (*number once*). *Nonce* merupakan nilai yang sebenarnya tidak memiliki makna apapun, namun sengaja ditambahkan ke dalam blok agar menghasilkan nilai *hash* sesuai ketentuan. Apabila nilai *hash* belum memenuhi ketentuan, maka nilai *nonce* diubah lagi, demikian seterusnya sampai penambang tersebut menemukan sebuah nilai *hash* yang memenuhi kriteria.

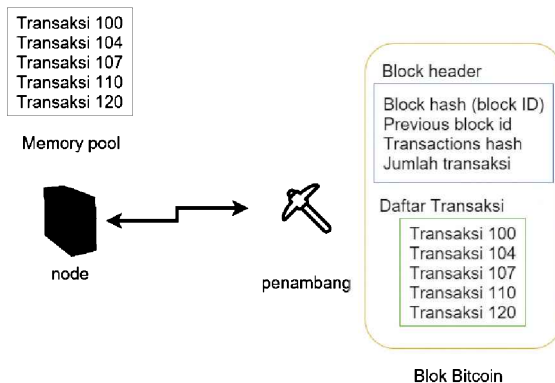
Proses PoW jelas membutuhkan sumber daya (waktu, listrik, mesin) yang tidak sedikit, apalagi jika tingkat kesulitannya sangat tinggi, seperti yang terjadi sekarang ini. Oleh karena itu, para penambang menginvestasikan lebih banyak sumber daya agar bisa mencetak lebih banyak blok. Semakin tinggi tingkat kesulitan, maka informasi di dalam *blockchain* akan semakin aman dari perubahan yang tidak sah.

Penambangan

Proses penambangan (*mining*) yang ada pada sistem Bitcoin merupakan usaha untuk

melakukan perhitungan matematis seperti dalam Hashcash agar sebuah blok baru dapat diterima ke dalam *blockchain*. Pada saat hasil tersebut dapat diterima, maka blok baru tersebut ditambahkan ke dalam *blockchain*. Di sinilah peran PoW untuk melindungi *blockchain*. Dengan tingginya tingkat kesulitan, maka siapapun yang berniat mengubah transaksi yang telah tercatat dalam sebuah blok, maka ia harus melakukan perhitungan ulang atas blok tersebut dan juga blok-blok berikutnya, karena sebagaimana telah dijelaskan bahwa sebuah blok dihubungkan dengan blok-blok lain yang membentuk sebuah rantai. Jadi ketika sebuah mata rantai hendak diubah, maka mata rantai berikutnya juga harus ikut diubah. Oleh karena itu, transaksi dalam Bitcoin sangat sulit dibatalkan apabila telah dimasukkan dalam *blockchain*.

Penambang Bitcoin adalah mereka yang menyediakan peralatan komputasi untuk membantu melakukan perhitungan dalam membuat blok baru. Penambang Bitcoin akan memperoleh bayaran dalam bentuk Bitcoin atas usaha mereka.



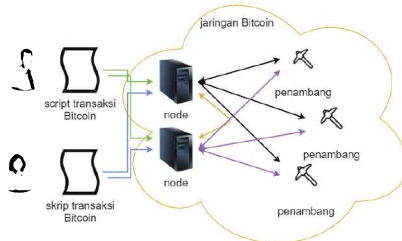
Gambar 10. Proses menambang blok

Penambang berkomunikasi dengan node Bitcoin untuk memperoleh informasi tentang transaksi-transaksi baru yang harus dimasukkan ke dalam blok baru.

Node Bitcoin

Komponen Bitcoin yang kedua adalah *node* Bitcoin. *Node* Bitcoin merupakan komputer-komputer yang menjalankan aplikasi *Bitcoin core* dan terhubung dengan Internet. *Node* Bitcoin memelihara basis data *blockchain* dan UTXO. *Node* Bitcoin memiliki peran vital dalam sistem Bitcoin, karena menyediakan salinan lengkap atas *blockchain* dan UTXO, juga melayani permintaan informasi transaksi yang telah terekam dalam *blockchain* dan UTXO. Oleh karena itu selain memerlukan ruang *harddisk* dan RAM yang besar, *node* Bitcoin juga memerlukan koneksi Internet yang stabil. *Node* Bitcoin tidak memper-

oleh bayaran atas jasa yang disediakan. Umumnya penyedia node Bitcoin adalah para penambang, pedagang besar, maupun mereka yang peduli dengan keberlangsungan sistem Bitcoin. Semakin banyak node Bitcoin maka semakin stabil pula sistem Bitcoin.

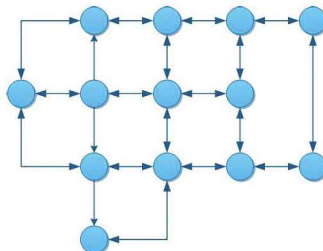


Gambar 11. Node Bitcoin dalam jaringan Bitcoin

Node Bitcoin membentuk jaringan *peer-to-peer* Bitcoin yang saling berkomunikasi untuk bertukar informasi atas *blockchain*, UTXO, dan transaksi-transaksi baru yang harus dikonfirmasi ke dalam *blockchain*. Node Bitcoin tersebut kemudian menyampaikan transaksi-transaksi baru tersebut kepada para penambang agar para penambang dapat memasukkannya ke dalam blok baru.

Jaringan Peer-to-peer

Jaringan *peer-to-peer* merupakan struktur di mana setiap anggota jaringan tersebut berkedudukan setara dan tidak ada *server* terpusat; setiap *node* dapat menjadi *server* yang menyediakan data sekaligus *client* yang meminta data. Struktur *peer-to-peer* dipopulerkan oleh layanan berbagi *file* seperti Napster dan Torrent, yang kemudian diadopsi oleh Bitcoin. Dengan menggunakan struktur ini, maka apabila ada 1 *node* mati, *node* yang lain dapat menggantikan posisi *node* tersebut dengan mudah. Di dalam sistem Bitcoin di mana setiap *node* menyimpan informasi *blockchain* dan UTXO yang sama persis, maka setiap pengguna Bitcoin dapat meminta informasi dari node manapun dan menghasilkan informasi yang sama pula. Keuntungan ini tidak akan didapatkan apabila menggunakan struktur *client-server* yang terpusat di mana apabila *server* mati, maka *client* tidak akan dapat memperoleh informasi yang diminta.



Gambar 12. Ilustrasi jaringan *peer-to-peer*. Setiap bulatan mewakili node Bitcoin.

Setiap bulatan biru merupakan *node* Bitcoin. Karena tidak memiliki bank sentral, Bitcoin mengandalkan jaringan yang populer disebut *peer-to-peer* atau P2P untuk menjalankan sistemnya.

P2P pada intinya merupakan sebuah kumpulan komputer yang membagi informasi satu sama lain. Berbeda dengan jaringan *client-server*, P2P tidak mengenal peran *server* terpusat yang mengendalikan informasi. Dengan P2P, semua informasi dibagi sama rata dan semua komputer dalam P2P tersebut memiliki informasi yang sama. Informasi yang dimaksud di sini adalah seluruh transaksi yang terjadi dalam sistem Bitcoin, termasuk alamat Bitcoin milik Anda, saya, dan semua orang di dunia yang menggunakan Bitcoin.

Hal yang menarik dari Bitcoin adalah Anda dapat melihat seluruh transaksi bitcoin tanpa memerlukan izin khusus. Artinya, tidak seperti kebijakan bank tradisional yang hanya memperbolehkan pemiliknya melihat transaksi yang dilakukan, di dalam sistem Bitcoin semua orang boleh melihat transaksi manapun. Hanya saja, kita tidak akan mendapatkan informasi nama maupun alamat dalam transaksi Bitcoin (Nakamoto, 2008).

Pengembang Perangkat Bitcoin

Pengembang perangkat Bitcoin adalah mereka yang berkecimpung dalam usaha pengembangan sistem Bitcoin. Terdapat beberapa kategori pengembang perangkat Bitcoin, yakni pengembang perangkat lunak Bitcoin *core* dan pengembang perangkat pendukung Bitcoin. Pengembang perangkat lunak Bitcoin *core* adalah kumpulan para programmer yang mendedikasikan waktunya untuk memelihara kode sumber dan menambahkan fitur-fitur baru dalam aplikasi Bitcoin *core* yang bersifat *open source*. Beberapa di antara para programmer yang terkenal adalah Gavin Andresen, Pieter Wuille, Gregory Maxwell, Luke Dashjr, dan Mike Hearn.

Meskipun dikelola oleh sekelompok programmer, para programmer ini tidak memiliki kewenangan untuk melakukan perubahan atas perangkat lunak Bitcoin *core* sebelum mendapatkan persetujuan dari para penambang. Hal pertama yang harus mereka lakukan sebelum melakukan implementasi sebuah ide dan fitur baru ke dalam Bitcoin *core* adalah dengan membuat dokumen BIP (Bitcoin Improvement Proposal) untuk mendapatkan komentar dan masukan dari sesama programmer dan aktivis Bitcoin.

Setelah ide tersebut dirasa matang, maka implementasi dikerjakan ke dalam sistem Bitcoin *core* untuk dipublikasikan menjadi versi baru. Versi baru tersebut kemudian akan di-*voting* oleh para penambang. Apabila mayoritas penambang setuju dengan versi baru, mereka akan melakukan update versi terbaru, namun jika tidak maka mereka akan tetap menggunakan versi sebelumnya. Hal ini menunjukkan karakteristik desentralisasi dan demokrasi sistem Bitcoin, di mana pengembang Bitcoin *core* pun tidak berkuasa mengatur jalannya sistem Bitcoin.

Sementara pengembang perangkat pendukung Bitcoin adalah mereka yang menyediakan aplikasi pihak ketiga yang menggunakan teknologi Bitcoin, seperti dompet Bitcoin dan layanan jual beli Bitcoin. Pihak ketiga ini menyediakan layanan mereka dengan gratis maupun berbayar.

Alamat Bitcoin

Alamat Bitcoin bertindak seperti nomor rekening bank. Untuk memulai bertransaksi di bank, tentunya Anda harus membuka rekening dahulu kan? Demikian halnya dengan Bitcoin, Anda harus memiliki alamat Bitcoin (*Bitcoin address*) agar dapat mengirim dan menerima bitcoin.

Alamat Bitcoin terdiri atas 34 karakter kombinasi angka, huruf kapital, dan huruf normal. Tentunya akan sulit untuk menghafalkan dan menulis dengan benar alamat Bitcoin sepanjang ini, oleh karena itu biasanya dompet Bitcoin dilengkapi dengan *scanner* QRcode. QRcode mempermudah pengguna untuk memasukkan alamat Bitcoin dengan benar dan menghindari kesalahan saat mengetikkan alamat Bitcoin. Hal ini penting karena tidak seperti saat kita melakukan transfer uang melalui ATM atau internet banking, di mana mesin akan memastikan nama pemilik rekening sebelum finalisasi transfer, Bitcoin tidak mengetahui nama asli pemilik alamat Bitcoin.

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	1KKxcGQB8SYgn6W6pXZZpAltztPh5n8eV4	No. Transactions	2
Hash 160	c5082bb08c8ba55f253b4db6a253d6793d98c5bf	Total Received	0.02659841 BTC
Tools	Taht Analysis - Related Tags - Unspent Outputs	Final Balance	0 BTC
		Request Payment	Donation Button



Transactions (Oldest First)

172c0f997650b4c3d5f7a9acc047ef3410f5b8e4c58a95531c493a6c0b0

1KKxcGQB8SYgn6W6pXZZpAltztPh5n8eV4 (0.02659841 BTC - Output)

452c6114ca3b141c9587026025623b713bb7a6b14341a13c4d45067e75ac63

1FAv42GaDuQwSzEzSbxeA1K1uVWpQUY (0.09110672 BTC - Output)

(Fee: 0.000025 BTC - Size: 226 bytes) 2015-11-04 21:44:29

17V1GHuLxQvvn54Dq74uFJdKHMZnOE7s - (Unspent) 0.0001 BTC

1P4KVve7GKrcavpvgAjaPKWY1YFM99gVQ8 - (Unspent) 0.02647341 BTC

0.02659841 BTC

(Fee: 0.00015 BTC - Size: 226 bytes) 2015-08-09 23:14:50

1KKxcGQB8SYgn6W6pXZZpAltztPh5n8eV4 - (Spent) 0.02550841 BTC

1CQuTRvRvq3ZBd5cUHL7MmqvVGRySMJH - (Spent) 0.06435831 BTC

0.02659841 BTC

Gambar 13. Informasi Alamat Bitcoin

Untuk mendapatkan alamat Bitcoin, Anda tidak perlu melakukan pendaftaran seperti ketika Anda membuka rekening Bank. Siapapun bisa memiliki alamat Bitcoin, bahkan jika Anda tidak melakukan transaksi apapun. Gambar berikut menunjukkan sebuah alamat Bitcoin yang belum pernah digunakan. Di dalam sistem Bitcoin, semua orang dapat dengan bebas membuat alamat Bitcoin sebanyak yang diinginkan. Kita tidak perlu mengetahui bagaimana caranya membuat alamat Bitcoin dengan benar, sebab *software*

dompet Bitcoin akan melakukannya untuk kita secara otomatis.

Bitcoin Address

Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	16NCz556NPmouJHuEgq7dron7aZuF5mN	No. Transactions	0
Hash 160	3adb5a2a16900483d82c6ec8683c6239e6d0c08	Total Received	0 BTC
Tools	Taint Analysis - Related Tags - Unspent Outputs	Final Balance	0 BTC
		Request Payment	Donation Button



Transactions (Oldest First)

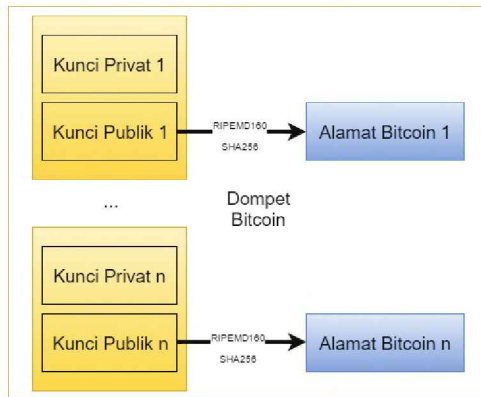
No transactions found for this address. It has probably not been used on the network yet.

▼ Filter

Gambar 14. Alamat Bitcoin kosong

Dari Kunci Publik ke Alamat Bitcoin

Alamat Bitcoin bukanlah kunci publik dalam skema Public Key Cryptography (PKC) seperti yang telah dibahas. Terdapat sebuah prosedur lain dalam Bitcoin untuk menghitung alamat Bitcoin dari kunci publik yang telah dibuat. Prosedur tersebut di antaranya melibatkan fungsi hash RIPEMD160 dan SHA256 sebagaimana telah dibahas sebelumnya.



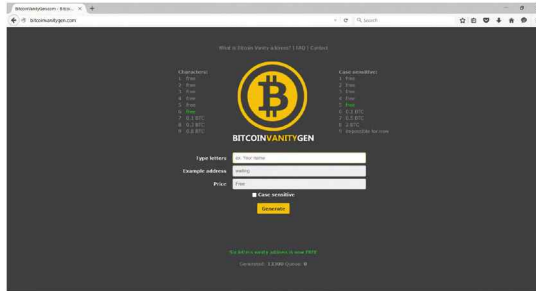
Gambar 15. PKC ke Alamat Bitcoin

Detail tentang penghitungan kunci publik menjadi alamat Bitcoin tidak akan dibahas di sini. Jika Anda tertarik, Anda dapat melihat rincian teknisnya di Bitcoin Wiki (2011b). Alamat Bitcoin disebut juga dengan istilah Public Key Hash, karena alamat Bitcoin memang merupakan nilai hash dari kunci publik dari pasangan kunci yang disimpan dalam dompet Bitcoin.

Bitcoin Vanity Address

Meskipun alamat Bitcoin dapat dibuat secara otomatis oleh dompet Bitcoin, dapat pula

dibuat alamat Bitcoin yang menarik. Sama seperti halnya dengan plat nomor kendaraan yang dapat dimodifikasi, Anda bisa pula menggunakan alamat Bitcoin yang terkustomisasi. Alamat Bitcoin yang terkustomisasi ini disebut dengan vanity Bitcoin *address*. Anda dapat mencobanya melalui BitcoinVanityGen (<http://bitcoinvanitygen.com>). Meskipun tidak semua karakter dalam alamat Bitcoin dapat terkustomisasi, Anda bisa menentukan sampai dengan 5 karakter dengan gratis.



Gambar 16. Membuat Alamat Bitcoin Terkustomisasi

Misalnya Anda menginginkan ada unsur nama Anda sendiri atau nama usaha Anda pada alamat Bitcoin, sebagai contoh “DMZ”, maka Anda bisa mendapatkan alamat Bitcoin kustom yang pemberituannya dikirim lewat email, hasilnya adalah 11DMZFeAyR-8MEXN6vDnVhEP6um49qz2TR. Tentu saja Anda akan mendapatkan kunci rahasia untuk alamat Bitcoin tersebut.

Transaksi Bitcoin

Sebagai sebuah sistem uang, Bitcoin juga mengenal pecahan uang. Jika dalam rupiah kita mengenal beberapa denominasi rupiah seperti 100 ribu, 50 ribu, 20 ribu, dan seterusnya, Bitcoin juga dapat dipecah. Satu satuan utuh bitcoin yang bersimbol BTC yakni 1 BTC dapat dipecah menjadi unit-unit yang lebih kecil, yakni mili-bitcoin (mBTC) di mana 1 BTC = 1.000 mBTC, mikro-bitcoin (µBTC) dengan 1 BTC = 1 juta µBTC, dan satuan terkecil disebut satoshi, di mana 1BTC = 100juta satoshi.

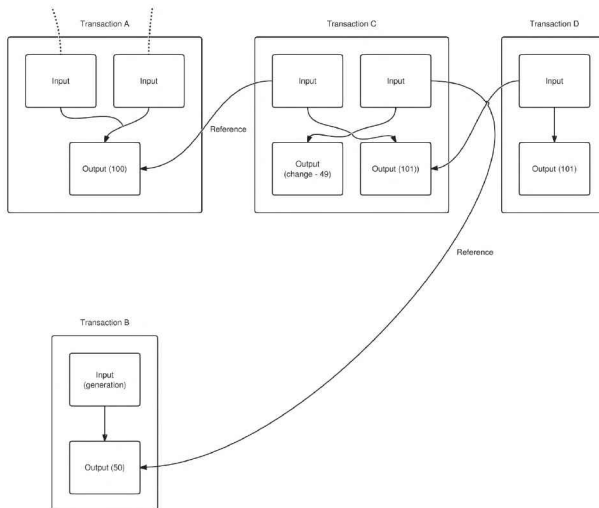
Di dalam sebuah transaksi, Anda harus memiliki uang yang sama banyak dengan harga barang, atau dapat pula Anda memiliki uang yang lebih banyak dibandingkan harga barang dan Anda akan mendapatkan kembalian sebesar selisih nilai uang dan nilai barang. Sederhananya, jika Anda memiliki total uang 1 juta rupiah yang terdiri atas 5 lembar pecahan uang 100 ribu rupiah dan membeli sebuah barang dengan harga 25 ribu rupiah, maka Anda menyerahkan 1 lembar pecahan uang 100 ribu rupiah pada penjual dan akan mendapatkan uang kembalian dari si penjual sebesar 75 ribu rupiah.

Transaksi dalam Bitcoin memiliki persamaan dan perbedaan dibanding transaksi rupiah

dalam ilustrasi di atas. Semisal Anda memiliki 1,2 BTC dalam sebuah alamat Bitcoin dan membeli barang senilai 0,5 BTC, maka dompet Bitcoin Anda akan membayar barang tersebut sebanyak 1,2 BTC dan akan mendapatkan kembalian sebanyak 0,7BTC ke alamat Bitcoin lain yang disebut *change address*.

Change address ini juga dikelola oleh dompet Bitcoin dan dapat digunakan untuk melakukan transaksi lagi. Sebagai ilustrasi lain, Anda memiliki total 1,2 BTC dalam 6 alamat Bitcoin yang berbeda, masing-masing bernilai 0,2 BTC. Ketika Anda membeli barang senilai 0,5 BTC maka dompet Bitcoin akan melakukan pembayaran menggunakan 3 alamat Bitcoin dengan total nilai 0,6 BTC dan akan mendapat kembalian sebesar 0,1BTC melalui *change address*.

Namun ketika Anda memiliki 4 alamat Bitcoin dengan nilai masing-masing 0,1 BTC, 0,3 BTC, 0,35 BTC, dan 0,45 BTC, tidak ada aturan baku tentang bagaimana dompet Bitcoin membayar barang senilai 0,5BTC dari bitcoin yang Anda miliki. Bisa saja dompet Bitcoin Anda menggunakan 2 alamat yang bernilai 0,3 BTC dan 0,35 BTC dengan mendapatkan kembalian sebesar 0,15 BTC, atau menggunakan 2 alamat yang bernilai 0,1 BTC dan 0,45 BTC dengan mendapatkan kembalian sebesar 0,05 BTC.



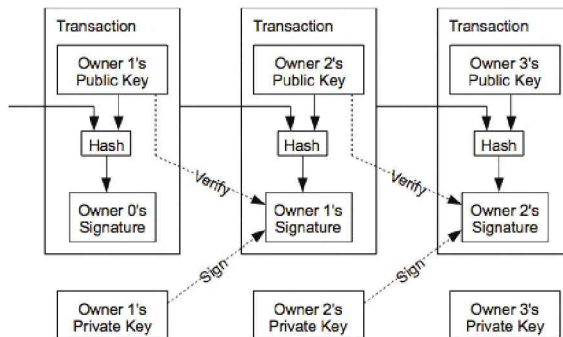
Gambar 17. Transaksi dalam Bitcoin. (Bitcoin Wiki, 2013c)

Ilustrasi pada Gambar 17 menggambarkan cara kerja transaksi Bitcoin. A melakukan pembayaran kepada C sebanyak 100 BTC, B juga melakukan pembayaran kepada C sebanyak 50 BTC. Kini C memiliki uang sebanyak 150 BTC, kemudian melakukan pem-

bayaran kepada D sebanyak 101 BTC, yang mendapatkan kembalian (*change*) sebanyak 49 BTC. Ilustrasi di atas menunjukkan bahwa input transaksi merupakan referensi dari *output* transaksi sebelumnya.

Sebagai contoh, input transaksi C mereferensi output transaksi A dan transaksi B. Pengecualian pada transaksi B di mana ia tidak mereferensi output transaksi manapun, karena uang yang dimiliki oleh B merupakan uang baru yang diciptakan dari hasil penambangan.

Selain melakukan referensi atas *output* transaksi sebelumnya, pemilik uang juga harus memberikan tanda tangan elektronik yang valid. Tanda tangan elektronik tersebut akan dibubuhkan pada script transaksi yang dikirimkan kepada jaringan Bitcoin. Apabila script tersebut berhasil diverifikasi, maka transaksi akan diteruskan kepada penambang untuk dimasukkan ke dalam *blockchain*. Sebagaimana dijelaskan pada gambar di bawah ini, pada transaksi (*transaction*) kotak kedua, pihak 1 hendak mengirim uang pada pihak 2. Maka pihak 1 menyebutkan alamat yang dimiliki pihak 2 sebagai alamat tujuan, dan membuat tanda tangan elektronik atas transaksi tersebut untuk menunjukkan bahwa uang yang dibayarkan kepada pihak 2 adalah benar-benar milik pihak 1, yang dibuktikan dengan tanda tangan elektronik tersebut.



Gambar 18. Tanda tangan elektronik pada transaksi Bitcoin (Nakamoto, 2008)

Transaksi dalam Bitcoin memiliki keunggulan dibandingkan transaksi dalam sistem keuangan tradisional. Pengguna Bitcoin dapat membuat transaksi yang terkustomisasi untuk memenuhi kebutuhan tertentu. Sebagai contoh transaksi yang terkustomisasi adalah transaksi yang memerlukan kata kunci (*password*) tertentu sebelum dananya dapat digunakan. Tipe transaksi seperti ini tentunya tidak dapat dilakukan pada sistem keuangan tradisional. Salah satu contoh transaksi terkustomisasi Bitcoin adalah *multisignature*, yaitu transaksi yang memerlukan tanda tangan lebih dari 1 pihak sebelum

dapat menggunakan dana yang tersedia. Transaksi Bitcoin juga dapat dimanfaatkan untuk mengirim pesan pendek dengan menggunakan fitur OP_RETURN.

Script Transaksi

Untuk dapat membuat transaksi terkustomisasi, pengguna Bitcoin tidak memerlukan izin apapun. Yang diperlukan adalah pengetahuan tentang bagaimana membuat *script* transaksi yang terdiri atas *scriptPubKey* dan *scriptSig*. Detail teknis tentang *script* Bitcoin tidak akan dibahas di dalam buku ini, namun apabila Anda tertarik mempelajari *script* Bitcoin, Anda dapat merujuk pada laman Bitcoin Wiki (2013b). Hanya saja, Anda harus berhati-hati ketika menggunakan *script* terkustomisasi, karena apabila *script* tersebut *error*, maka dana yang ada di dalamnya tidak dapat diambil kembali selamanya. Anda juga harus berhati-hati ketika menggunakan *script* yang tidak menggunakan tanda tangan elektronik, karena tanpa tanda tangan elektronik, dana tersebut bisa dicuri oleh pihak lain.

Transaksi Bitcoin yang tersusun atas *script* direpresentasikan dalam kode-kode heksadesimal. Berikut adalah contoh *script* transaksi Bitcoin yang menggunakan struktur *multisignature*.

```
010000000156751bf4c4530624071c9ca68f-
5fe5cdfb1ebd2e216aec60aabc46451e2f-
97c000000000fd200100473044022036050f7fe1b1a-
723f3eeea15b1997721eeae19d0b82a993d9c8cb-
9cf4b08af0802202cc2ea62693264a05f10f7125f-
2964453381c0a95230235a7eb4320d170d175b014
83045022100afdf12f12fed4b2b2e6d2685407bf-
30029cac510274d30b54f3fffb1165857040220018fca38e51a-
4911c33969ac9f9407337d1a984e859e9ed05722af4438afaf-
0c01514c8b635221020b6df2beb4bd59a072786e5ea66d2f-
da3da56f1de568801f18aa06b3c719a4a5210265c0023ee6b-
fe4ec31f902bc5f64c003c0f5af9be37397623b16e9639420
520121028a382c159f04b6655accec0ade85459b203544a0a-
2fa995e9b924f81ecc9c450b53ae6703310506b17576a9149ce-
822a6cc7e208f9d64f4681cbf5984778c3f1788ac68ffffff-
f01102700000000000001976a91499bb74fd689ca03b29af1ae-
7fa3d113d2a029aec88ac00000000
```

Script transaksi di atas tentu saja sulit dibaca oleh mata manusia, karena memang ditujukan untuk perangkat lunak komputer. Untuk membaca skrip di atas, diperlukan alat bantu perangkat lunak lain yang dapat menterjemahkannya menjadi informasi yang lebih mudah dibaca seperti berikut.

```

transaction
{
    hash cd0ae2c5895elfd05b6b7bde7ee90724fb8545eb2c322e6e809c0f-
d91848c88b
    inputs
    {
        input
        {
            previous_output
            {
                hash c0972f1e4546bcaa60ec6a212ebd1efbcde55f-
8fa69c1c07240653c4f41b7556
                index 0
            }
            script "zero [ 3044022036050f7fe1b1a723f3eeea-
15b1997721eeae19d0b82a993d9c8cb9cf4b08af0802202c-
c2ea62693264a05f10f7125f2964453381c0a95230235a7eb4320d
170d175b01 ] [ 3045022100afdf12f12fed4b2b2e6d2685407b-
f30029cac510274d30b54f3fffb1165857040220018fca38e51a-
4911c33969ac9f9407337d1a984e859e9ed05722af4438afaf0c01 ] 1 [
635221020b6df2beb4bd59a072786e5ea66d2fda3da56f1de568801f18aa06b-
3c719a4a5210265c0023ee6bfe4ec31f902bc5f64c003c0f5af9be-
37397623b16e9639420520121028a382c159f04b6655acec0ade-
85459b203544a0a2fa995e9b924f81ecc9c450b53ae-
6703310506b17576a9149ce822a6cc7e208f9d64f4681cbf5984778c-
3f1788ac68 ]"
            sequence 4294967295
        }
    }
    lock_time 0
    outputs
    {
        output
        {
            address 1Flrx6EMefZfrZmAhp4HyDCbuEf7RWbfMP
            script "dup hash160 [ 99bb74fd689ca03b29af1ae-
7fa3d113d2a029aec ] equalverify checksig"
            value 10000
        }
    }
    version 1
}

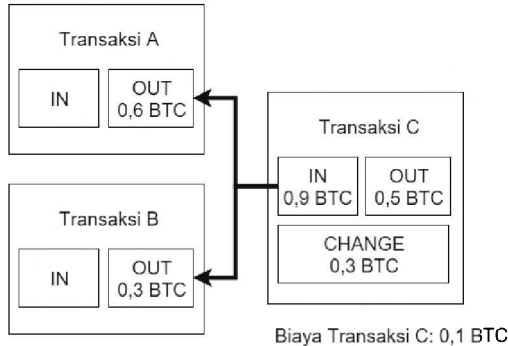
```

Terdapat 2 bagian besar dalam *script* transaksi di atas. Bagian pertama disebut *inputs*, merupakan bagian yang merujuk transaksi sebelumnya atas alamat Bitcoin pengirim. Bagian kedua disebut *outputs*, merupakan bagian yang mengatur tujuan pengiriman dana. Pada bagian ini juga dapat diatur *change address*, yakni alamat untuk mengirim sisa uang pembayaran.

Biaya Transaksi

Biaya transaksi merupakan sejumlah bitcoin yang dibayarkan kepada para penambang. Biaya transaksi yang dibayar oleh pengguna Bitcoin merupakan salah satu komponen insentif yang diterima oleh para penambang atas jasanya melakukan kegiatan penambangan. Berbeda dengan transaksi kartu kredit yang menghitung biaya transaksi atas dasar jumlah uang yang ditransaksikan, biaya transaksi Bitcoin dihitung berdasarkan besaran *script* transaksi yang dihitung dalam satuan byte.

Meskipun pengguna tidak dibebankan kewajiban untuk selalu mencantumkan biaya transaksi, saat ini terdapat kesepakatan umum yang menyatakan bahwa biaya transaksi minimal adalah sebanyak 10.000 satoshi atau 0,0001 BTC (Bitcoin Wiki, 2011c) untuk setiap 1.000 byte *script* transaksi. Apabila transaksi berukuran 1.001 byte, maka biaya transaksinya menjadi 20.000 satoshi atau 0,0002 BTC, karena perhitungan biaya transaksi adalah kelipatan 1.000 byte dibulatkan ke atas.



Gambar 19. Biaya transaksi dalam Bitcoin

Sebagaimana dijelaskan pada Gambar 19, biaya transaksi tidak dicantumkan secara eksplisit di dalam sebuah transaksi Bitcoin. Biaya transaksi dihitung berdasarkan selisih antara jumlah *input* dan jumlah *output*. Pada ilustrasi di atas, A dan B melakukan pembayaran pada C masing-masing sejumlah 0,6 BTC dan 0,3 BTC. Kemudian C membuat transaksi C yang menggunakan uang yang diperoleh dari A dan B dengan total 0,9 BTC dengan rincian 0,5 BTC dibayarkan kepada orang lain, 0,3 BTC merupakan uang kembalian milik C, sedangkan selisihnya 0,1 BTC menjadi biaya transaksi. Biaya transaksi

ini akan diambil oleh siapapun penambang yang pertama kali berhasil memasukkan transaksi ini ke dalam sebuah blok valid.

Komunitas dan Sumber Informasi Bitcoin

Meskipun Bitcoin sebagai alat pembayaran masih belum digunakan secara luas, Anda bisa bergabung dengan komunitas-komunitas Bitcoin yang telah ada. Komunitas Bitcoin pertama dan terbesar adalah forum Bitcointalk (<https://bitcointalk.org>), di mana Anda bisa menemukan banyak sekali informasi tentang Bitcoin termasuk informasi teknis dan hal-hal baru yang dibahas oleh para anggota yang berasal dari seluruh dunia. Forum ini berbahasa Inggris, namun demikian ada juga subforum lokal Bahasa Indonesia, yang menunjukkan eksistensi orang-orang Indonesia yang berkecimpung dalam sistem Bitcoin. Anda juga bisa menemukan hampir semua jenis *cryptocurrency* mempromosikan *cryptocurrency* ciptaan mereka dari forum ini.

Selain Bitcointalk, Anda dapat juga bergabung dalam Forum Bitcoin Indonesia (<https://forum.bitcoin.co.id>) yang berbahasa Indonesia dan memiliki banyak topik dan informasi menarik seputar trading, *faucet*, dan penambangan Bitcoin. Di luar forum khusus yang membahas Bitcoin dan *cryptocurrency*, komunitas Bitcoin juga berkumpul dalam forum-forum umum, dan salah satu yang populer dan berpengaruh adalah r/Bitcoin yang merupakan salah satu subforum Reddit (<https://www.reddit.com/r/Bitcoin>). Dalam r/Bitcoin, banyak pengguna ikut berdiskusi tentang isu-isu terbaru Bitcoin, yang tentunya bisa menambah pengetahuan Anda seputar Bitcoin.

Untuk mengetahui informasi perkembangan Bitcoin, Anda dapat mengunjungi situs CoinDesk (<http://www.coindesk.com>) sebagai salah satu sumber informasi terdepan Bitcoin dan teknologi blockchain. Berbagai isu tentang Bitcoin juga selalu dibahas di situs tersebut dengan narasumber terpercaya dan dengan ulasan yang lengkap. Konferensi internasional yang membahas Bitcoin juga diinfokan dalam CoinDesk. Selain itu ada pula Bitcoin Magazine (<https://bitcoinmagazine.com>), Cryptocoins News (<https://cryptocoinsnews.com>), dan News Bitcoin (<https://news.bitcoin.com>) yang selalu menyajikan informasi menarik tentang Bitcoin dan *cryptocurrency*. Beberapa situs berbahasa Indonesia yang memiliki topik Bitcoin dan *cryptocurrency* di antaranya Bitcoin.or.id (<http://bitcoin.or.id>) dan Kriptologi (<http://kriptologi.com>). •

DOMPET BITCOIN

DOMPET BITCOIN HANYALAH MEMBANTU PENGGUNA UNTUK MENGELOLA ALAMAT-ALAMAT BITCOIN YANG DIMILIKI DAN MEMPERMUDAH TRANSAKSI. KETIKA ANDA MEMINTA INFORMASI TENTANG JUMLAH SISA BITCOIN YANG ANDA MILIKI DALAM DOMPET BITCOIN, MAKA DOMPET BITCOIN AKAN MELAKUKAN PERMINTAAN INFORMASI ATAS TOTAL NILAI BITCOIN DARI SETIAP ALAMAT BITCOIN YANG DIKELOLA OLEH DOMPET BITCOIN ANDA DAN MENJUMLAHKAN NILAINYA.

Sebelum dapat menggunakan Bitcoin, Anda harus memiliki dompet Bitcoin (*Bitcoin wallet*) untuk mempermudah kita melakukan transaksi. Walaupun disebut dengan istilah dompet, dompet Bitcoin memiliki fungsi yang tidak sama dengan dompet rupiah kita. Uang berbentuk bitcoin tidak tersimpan dalam dompet Bitcoin, sebab seluruh informasi mengenai transaksi dan saldo bitcoin (sisa uang yang dapat dibelanjakan) terdapat di dalam jaringan. Dompet Bitcoin hanyalah membantu pengguna untuk mengelola alamat-alamat Bitcoin yang dimiliki dan mempermudah transaksi. Ketika Anda meminta informasi tentang jumlah sisa bitcoin yang Anda miliki dalam dompet Bitcoin, maka dompet Bitcoin akan melakukan permintaan informasi atas total nilai bitcoin dari setiap alamat Bitcoin yang dikelola oleh dompet Bitcoin Anda dan menjumlahkan nilainya.

Dengan menggunakan dompet Bitcoin, Anda tidak perlu repot-repot mengelola setiap alamat Bitcoin yang Anda miliki, menghitung jumlahnya masing-masing, dan membuat transaksi secara manual. Dengan menggunakan dompet Bitcoin, semua pekerjaan tersebut dapat dikerjakan de-

ngan sangat mudah.

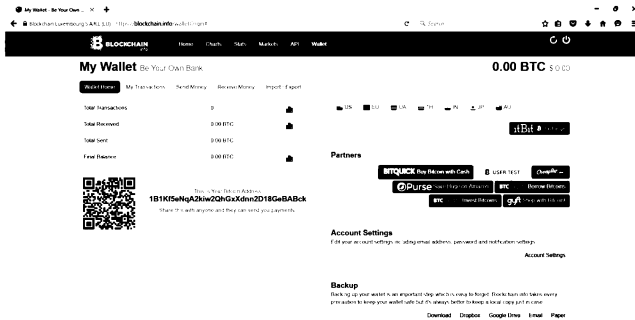
Terdapat beberapa jenis dompet Bitcoin yang dapat Anda gunakan, di antaranya berbasis web, berbasis desktop, dan berbasis *smartphone*. Seluruh aplikasi dompet Bitcoin yang dibahas dalam buku ini dapat digunakan dengan gratis.

Dompet Bitcoin Web

Keunggulan dompet berbasis web adalah fleksibilitasnya. Kita tidak perlu khawatir kehilangan data seperti halnya dompet berbasis desktop maupun *smartphone*. Kita bisa mengakses dompet berbasis web di manapun hanya dengan menggunakan peramban (*browser*) favorit kita. Salah satu dompet berbasis web yang memiliki fitur lengkap adalah [blockchain.info](https://blockchain.info/wallet/new). Anda dapat melakukan registrasi dengan mengakses alamat <https://blockchain.info/wallet/new> melalui peramban Anda yang akan membawa Anda pada laman seperti pada Gambar 20.

Gambar 20. Mendaftar akun baru di *blockchain.info*

Setelah melakukan pendaftaran, Anda dapat mengakses dompet Bitcoin (*wallet*) Anda. Tampilan dompet Bitcoin dapat Anda lihat pada Gambar 21.



Gambar 21. Dompot Bitcoin Web dari blockchain.info

Apabila Anda sudah selesai melakukan registrasi, maka Anda dapat mengakses dompet Bitcoin web Anda kapanpun melalui alamat <https://blockchain.info/wallet>. Sekarang akan kita bahas satu-persatu fitur-fitur yang ada di dalamnya. Wallet home merupakan akumulasi informasi atas total jumlah bitcoin yang Anda miliki saat ini dalam dompet Bitcoin milik Anda, juga total jumlah transaksi yang pernah dilakukan, total bitcoin yang pernah diterima dan pernah dibelanjakan. Dompot Bitcoin dari blockchain.info juga secara otomatis memberitahukan nilai bitcoin yang Anda miliki dalam denominasi dolar Amerika, sehingga dapat membantu Anda mengambil keputusan saat hendak membelanjakan bitcoin Anda. Dompot Bitcoin web ini memiliki 5 menu, yaitu Wallet Home yang telah dibahas, My Transactions, Send Money, Receive Money, dan Import/Export yang akan dibahas satu-persatu.



Gambar 22. Dompot Bitcoin Web - My Transaction

Gambar di atas merupakan laman yang akan menunjukkan daftar transaksi yang pernah Anda buat melalui dompet ini. Sangat penting untuk mengawasi daftar transaksi yang keluar dan masuk dompet Bitcoin Anda, apalagi jika Anda menggunakan dompet ini untuk kegiatan bisnis. Anda dapat memastikan bahwa pembayaran telah Anda terima dan diverifikasi oleh jaringan Bitcoin.



Gambar 23. Dompot Bitcoin Web - Send Money

Gambar 22 menunjukkan fitur untuk mengirim bitcoin dari dompet yang Anda miliki ke alamat Bitcoin lain, misalnya ketika Anda membeli sesuatu dan Anda ingin membayarnya dengan bitcoin, Anda dapat melakukannya melalui fitur ini. Di dalam fitur ini terdapat 3 submenu. Submenu pertama adalah Quick Send, yakni fitur untuk mengirim bitcoin ke alamat Bitcoin tertentu tanpa pengaturan lebih lanjut.



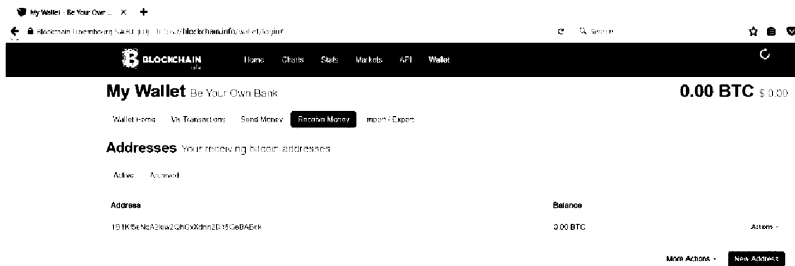
Gambar 24. Dompot Bitcoin Web - Shared Coin

Fitur Shared Coin seperti terlihat pada Gambar 24 di atas merupakan fitur pembayaran bitcoin ke alamat Bitcoin tertentu, tetapi dengan menambahkan fitur anonimitas atau privasi yang disebut shared coin. Shared coin akan meningkatkan privasi transaksi bitcoin kita, namun membutuhkan biaya yang lebih tinggi dibandingkan fitur Quick Send.



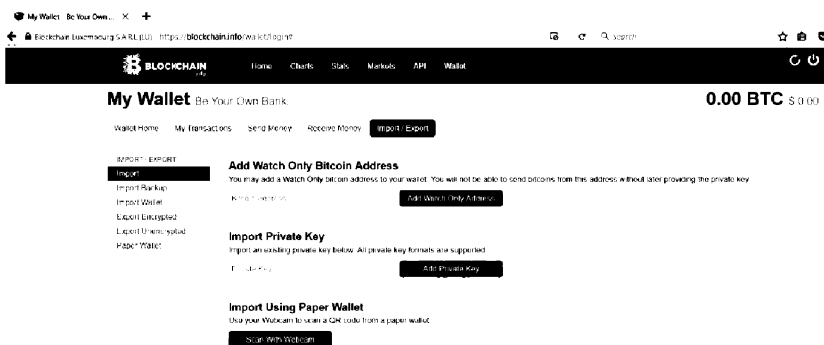
Gambar 25. Dompot Bitcoin Web - Custom Transaction

Gambar 25 menunjukkan fitur kustomisasi transaksi bitcoin yang akan dikirimkan ke alamat Bitcoin lain. Anda dapat melakukan perubahan terhadap beberapa bagian, seperti Miners Fee, Change Address, dan Public Note. Miners Fee adalah biaya transaksi yang harus dibayarkan agar transaksi Anda dapat diproses dalam sistem Bitcoin, sementara *change address* adalah alamat Bitcoin milik Anda untuk menerima kembalian dari pihak yang Anda bayar jika nilai Bitcoin yang Anda miliki lebih besar daripada yang seharusnya dibayarkan. Public Note adalah catatan yang dapat Anda tambahkan dalam transaksi.



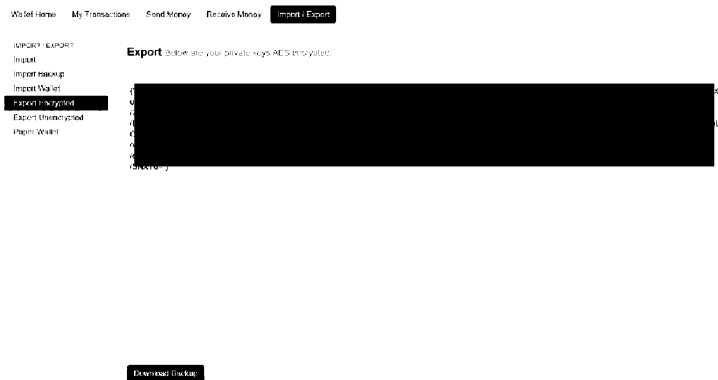
Gambar 26. Dompot Bitcoin Web - Receive Money

Gambar 26 merupakan tampilan fitur *receive money*, yaitu daftar alamat Bitcoin yang pernah menerima pembayaran bitcoin dari pihak lain. Anda dapat mengelola alamat Bitcoin yang Anda miliki melalui fitur ini, memberikan catatan atau label tertentu pada alamat Bitcoin atau menghapus alamat Bitcoin yang sudah tidak terpakai untuk mempermudah pengelolaan.



Gambar 27. Dompot Bitcoin Web - Import/Export

Gambar di atas merupakan fitur Import/Export atas data alamat Bitcoin. Fitur ini merupakan fitur kategori lanjut bagi pengguna yang memiliki dompet Bitcoin lebih dari 1. Sebagai contoh, Anda memiliki dompet Bitcoin web dan dompet Bitcoin *smartphone* atau *desktop*, maka apabila Anda tidak lagi menghendaki penggunaan dompet Bitcoin *smartphone*, maka Anda dapat mengambil informasi tentang alamat Bitcoin pada dompet Bitcoin *smartphone* tersebut (*export*) dan memasukkan informasi tersebut (*import*) ke dalam dompet Bitcoin web ini, demikian pula sebaliknya. Informasi yang terdapat dalam fitur ini sangat sensitif. Anda sebaiknya menjaga dengan baik segala informasi yang ada di dalamnya dan tidak membiarkan orang lain mengaksesnya, sebab melalui fitur ini Anda dapat melihat kunci rahasia dari semua alamat Bitcoin yang Anda miliki. Untuk dapat mengakses fitur ini, Anda harus memasukkan kata kunci dompet Bitcoin web Anda.

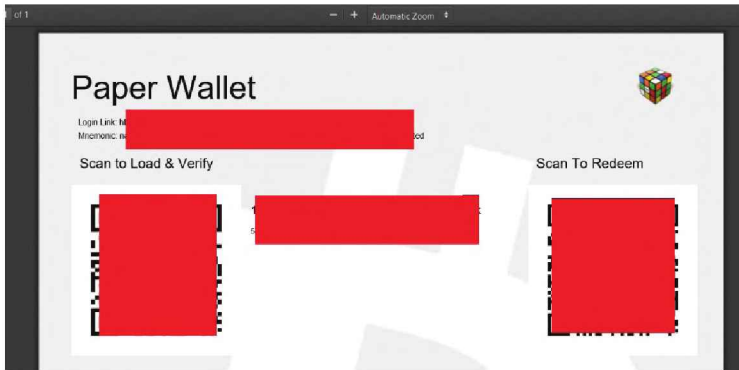


Gambar 28. Dompet Bitcoin web - Export Encrypted



Gambar 29. Dompet Bitcoin web - Export Unencrypted

Terdapat 2 cara untuk melakukan ekspor data alamat Bitcoin beserta kunci rahasianya, yaitu dengan terenkripsi maupun tidak terenkripsi. Metode terenkripsi artinya orang lain tidak akan bisa membaca informasi di dalamnya kecuali memiliki *password* yang sama, cara ini lebih aman namun ada kemungkinan tidak semua dompet Bitcoin dapat menggunakan cara ini. Metode tidak terenkripsi lebih tidak aman dan berbahaya bila sampai jatuh ke tangan orang lain, oleh karena itu harus dilakukan dengan ekstra hati-hati. Metode tidak terenkripsi lebih mudah dipindahkan ke dompet Bitcoin lainnya.



Gambar 30. Paper Wallet

Gambar 30 menunjukkan *paper wallet* atau dompet kertas yang memungkinkan Anda menyimpan informasi ini tanpa menggunakan media digital seperti komputer. *Paper wallet* menghindarkan Anda dari kehilangan bitcoin karena serangan digital seperti kegiatan *hacking* yang berusaha mencuri informasi kunci rahasia dari komputer Anda. Anda dapat menyimpan *paper wallet* ini di tempat-tempat aman misalnya *safe deposit box* di bank jika jumlah bitcoin yang Anda miliki cukup banyak dan Anda tidak berencana membelanjakannya dalam waktu dekat.

Dompet Bitcoin Smartphone

Dompet Bitcoin yang menggunakan *smartphone* memiliki keunggulan dibanding dompet Bitcoin web dan *desktop* dalam hal kemudahan akses. *Smartphone* lebih mudah diakses dan sangat lekat dalam kehidupan sehari-hari. Dengan harga yang semakin terjangkau, hampir semua orang dapat memiliki *smartphone* yang memiliki akses internet. Oleh karena itu, dompet Bitcoin *smartphone* lebih ringkas jika Anda melakukan pembayaran pada toko-toko fisik seperti restoran atau sejenisnya yang menerima Bitcoin.

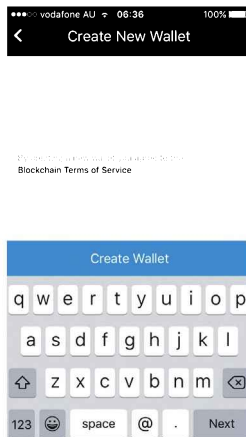
Terdapat banyak pilihan dompet Bitcoin *smartphone*, dan saya akan membahas salah satu di antaranya, yaitu Blockchain yang dibuat oleh pihak yang sama dengan dom-

pet Bitcoin web blockchain.info. Keunggulan dari Blockchain adalah Anda dapat menggunakan akun yang sama dengan dompet Bitcoin web Anda, sehingga alamat-alamat tersebut dapat diakses melalui smartphone maupun melalui web. Blockchain memiliki versi Android maupun iPhone. Apabila Anda sudah memiliki dompet Bitcoin web di blockchain.info, maka Anda tidak perlu membuat akun baru di dalam aplikasi Blockchain di *smartphone* Anda.



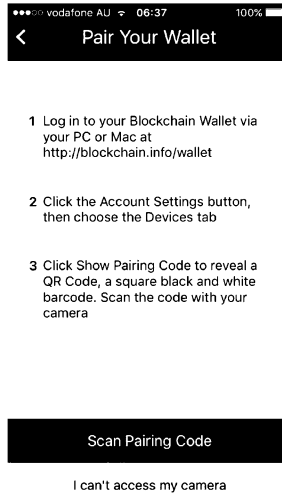
Gambar 31 Aplikasi Blockchain

Setelah Anda melakukan instalasi aplikasi Blockchain di *smartphone* Anda, maka ketika pertama kali menjalankan aplikasi akan muncul form seperti pada gambar 16. Jika Anda belum membuat akun di Blockchain web, maka Anda dapat memilih “Create New Wallet” dan akan muncul form baru seperti pada Gambar 32 berikut.



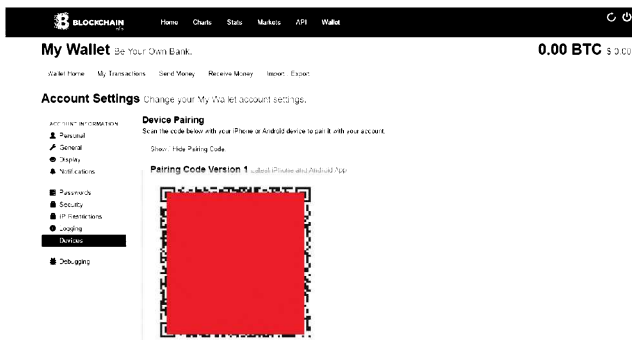
Gambar 32. Blockchain - Membuat dompet baru

Jika Anda ingin menggunakan akun yang sama dengan akun Anda di web, maka Anda dapat memilih “Log in to my wallet” untuk melakukan sinkronisasi dengan akun web Anda seperti tampak pada gambar di bawah ini.



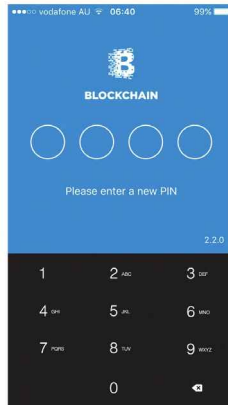
Gambar 33. Dompot Bitcoin smartphone - sinkronisasi akun

Untuk mendapatkan “Pairing Code” seperti yang diminta oleh aplikasi, maka Anda harus masuk ke dalam akun web Anda di <https://blockchain.info/wallet> dan kemudian dari Wallet Home -> Account Settings -> Devices -> Device Pairing -> Show / Hide Pairing Code.



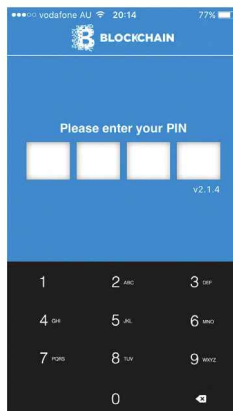
Gambar 34. Dompot Bitcoin smartphone - device pairing

QRcode yang muncul pada laman Device Pairing dapat di-scan menggunakan aplikasi *smartphone* untuk menghubungkan kedua akun Anda, yakni akun web dan akun di aplikasi *smartphone*. Setelah menerima informasi dari QRcode yang tertera pada web, maka aplikasi akan memproses akun Anda. Anda dapat menambahkan PIN sebagai fitur keamanan dalam aplikasi Blockchain.



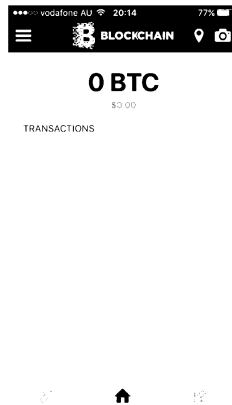
Gambar 35. Dompok Bitcoin smartphone - setting PIN

PIN yang telah Anda setting dapat digunakan untuk melakukan login dalam aplikasi. Aplikasi *smartphone* lebih mudah digunakan karena PIN yang terdiri atas 4 angka lebih singkat dibandingkan ketika kita harus memasukkan *username* dan *password* dalam dompet Bitcoin web.



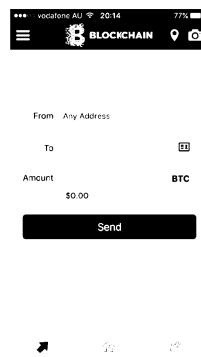
Gambar 36. Dompok Bitcoin smartphone - login

Gambar di atas menunjukkan halaman login aplikasi Blockchain. Anda dapat membuat PIN Anda sendiri untuk mengamankan informasi di dalamnya.



Gambar 37. Dompot Bitcoin smartphone - home

Gambar di atas merupakan tampilan home dari aplikasi Blockchain. Di sini Anda dapat melihat total jumlah Bitcoin yang Anda miliki dalam dompet Bitcoin yang sama dengan daftar transaksi yang pernah Anda lakukan. Terdapat 2 menu lain dalam aplikasi ini, yakni Send (kirim) dengan tanda anak panah ke atas dan Receive (terima) dengan tanda anak panah ke bawah.



Gambar 38. Dompot Bitcoin smartphone - Send

Pada menu Send terdapat pilihan untuk membayar bitcoin ke alamat Bitcoin yang dapat Anda isi secara manual atau dapat pula dengan melakukan scan QRcode menggunakan fitur kamera dalam *smartphone* Anda. Fitur ini dapat Anda aktifkan dengan tap tombol kamera di bagian kanan atas menu ini.



Gambar 39. Dompot Bitcoin *smartphone* - receive

Menu Receive digunakan untuk menerima pembayaran dalam bentuk bitcoin. Anda dapat menyodorkan QRcode dari menu ini ke *smartphone* konsumen Anda, dan otomatis alamat Bitcoin Anda akan terbaca dari *smartphone* konsumen Anda tanpa harus mengetik secara manual.

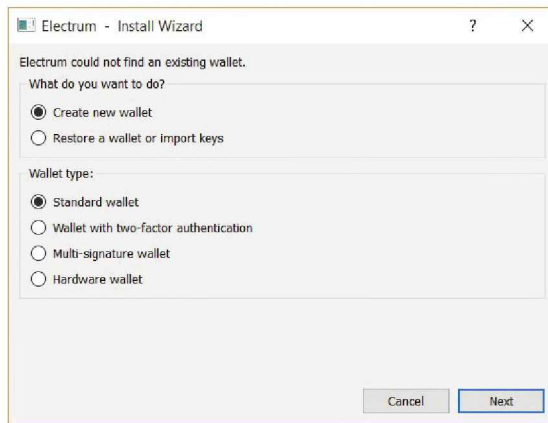


Gambar 40. Dompot Bitcoin *smartphone* - scan QRcode

Gambar di atas menunjukkan contoh saat aplikasi melakukan scanning QRcode untuk mendapatkan informasi berupa alamat Bitcoin.

Dompet Bitcoin Desktop

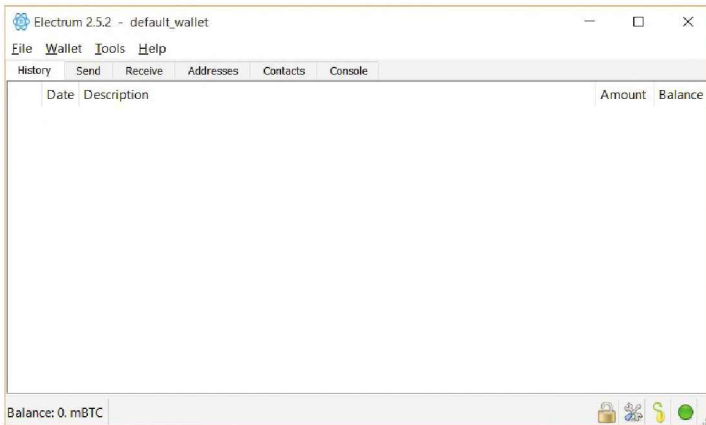
Dompet Bitcoin desktop merupakan aplikasi yang terinstal dalam komputer desktop Anda. Ada beberapa pilihan aplikasi yang tersedia, dan salah satunya adalah Electrum. Electrum sendiri memiliki beberapa pilihan sistem operasi, di antaranya Windows, Linux, OSX, maupun Android. Aplikasinya dapat Anda unduh melalui tautan <https://electrum.org/#download>.



Gambar 41. Electrum - instalasi

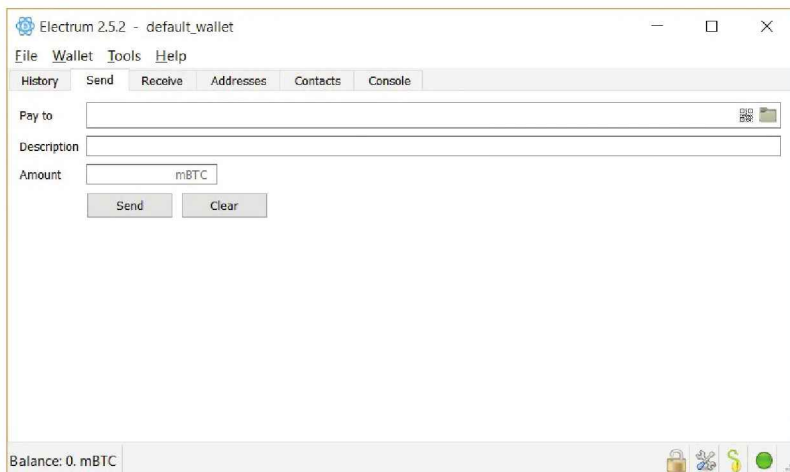
Electrum dapat digunakan untuk beberapa tipe dompet, di antaranya tipe standar, dompet dengan autentikasi 2-faktor (*two-factor authentication*), *multisignature*, dan *hardware*. Dompet tipe standar memiliki fitur standar *send* dan *receive*, sementara dompet dengan *two-factor authentication* merupakan dompet Bitcoin dengan tambahan fitur keamanan serupa token yang biasa digunakan untuk *internet banking*.

Dompet *multi-signature* dapat digunakan untuk pengelolaan dana yang harus mendapatkan persetujuan lebih dari 1 pihak, sehingga salah satu pihak tidak dapat melakukan kecurangan atas bitcoin yang dikelola dalam dompet tersebut. Sementara dompet *hardware* menggunakan perangkat keras khusus, misalnya produk keluaran Trezor. Pada saat instalasi Electrum, aplikasi ini akan membuat deretan kata-kata dalam bahasa Inggris yang disebut *seed*. *Seed* ini dapat digunakan untuk mengembalikan informasi dompet Bitcoin kita seandainya suatu saat nanti Anda kehilangan data atau komputer Anda, oleh karena itu ada baiknya untuk menyimpan dengan baik *seed* ini. Beberapa fitur yang dimiliki oleh Electrum akan dibahas berikut.



Gambar 42. Electrum - Daftar Transaksi

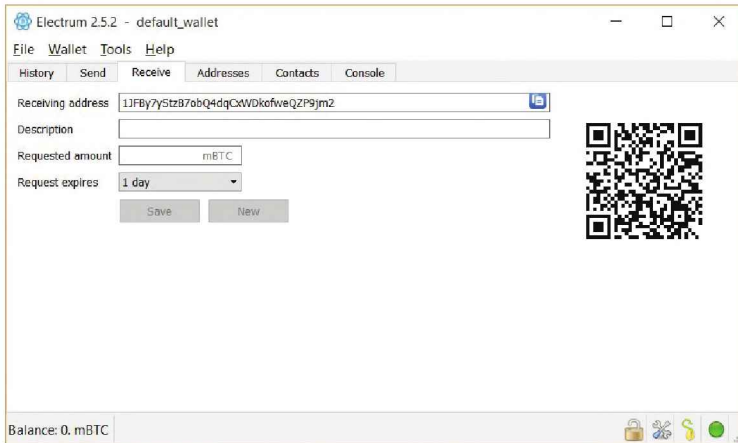
Gambar di atas menunjukkan daftar transaksi yang pernah dilakukan melalui dompet Bitcoin ini. Selain menu History, Electrum juga memiliki beberapa menu penting yang lain seperti Send (kirir), Receive (terima), dan Addresses (alamat).



Gambar 43. Electrum - Send

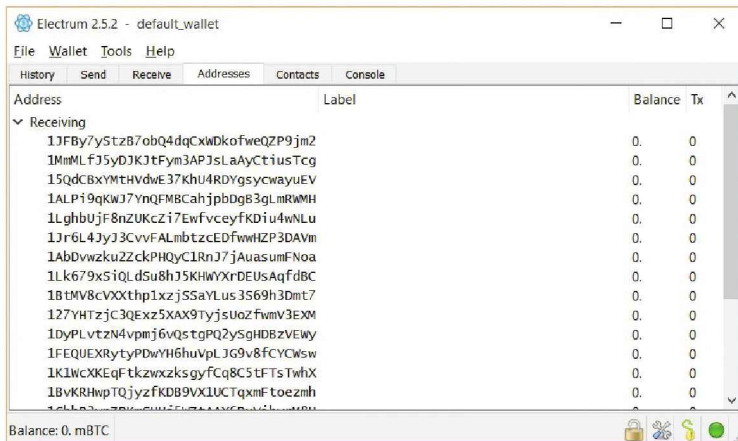
Gambar di atas merupakan menu untuk mengirim bitcoin ke alamat lain. Sedikit permasalahan untuk Electrum versi desktop adalah kesulitan melakukan scan QRcode untuk

mendapatkan alamat Bitcoin tujuan, sehingga harus diisi secara manual.



Gambar 44. Electrum - Receive

Menu Receive pada Electrum digunakan untuk mengorganisasikan bitcoin yang diterima atau akan diterima. Menu ini sangat bermanfaat misalnya jika Anda membuka restoran dan harus mengetahui apakah pembayaran yang dilakukan oleh konsumen Anda telah diterima atau belum.



Gambar 45. Electrum - Daftar Alamat Bitcoin

Electrum memiliki fitur untuk mengawasi seluruh alamat Bitcoin yang dikelolanya dengan setiap jumlah bitcoin yang ada pada masing-masing alamat Bitcoin.

Bitcoin Core

Bagi Anda yang memiliki usaha yang menerima pembayaran dalam bentuk bitcoin dalam jumlah besar, komunitas Bitcoin menyarankan Anda untuk memiliki *full node* sendiri demi meningkatkan keamanan. *Full node* merupakan istilah bagi komputer yang memiliki salinan lengkap dari seluruh informasi transaksi yang ada dalam sistem Bitcoin dari yang terlama hingga terbaru.

Dengan memiliki *full node*, maka Anda dapat terhindar dari beberapa jenis serangan terhadap sistem Bitcoin seperti *double spending*. Untuk membuat *full node*, yang dibutuhkan adalah aplikasi Bitcoin core yang dapat diunduh dengan gratis melalui situs <https://bitcoin.org/id/unduh>, yang dapat disesuaikan dengan versi sistem operasi Anda, misalnya Windows, OSX, atau Linux.

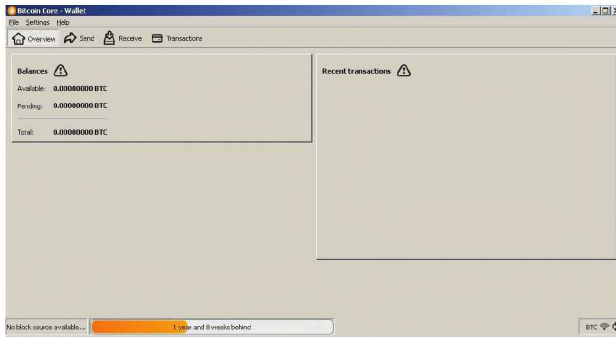
Tidak seperti dompet Bitcoin yang tidak memerlukan kapasitas memori dan *harddisk* besar, *full node* Bitcoin memerlukan sumber daya RAM dan *harddisk* yang cukup besar. Setidaknya komputer dengan sisa ruang *harddisk* berukuran 50 GB harus tersedia dengan ukuran RAM paling tidak 2 GB, dan juga koneksi internet yang bagus dan stabil. Saat ini, ukuran *database* lengkap yang harus diunduh dari jaringan berkisar 20-30 GB, namun karena jumlah transaksi Bitcoin semakin besar volumenya, maka ruang *harddisk* yang disiapkan juga harus lebih besar daripada 30 GB.



Gambar 46. Bitcoin-qt versi Windows

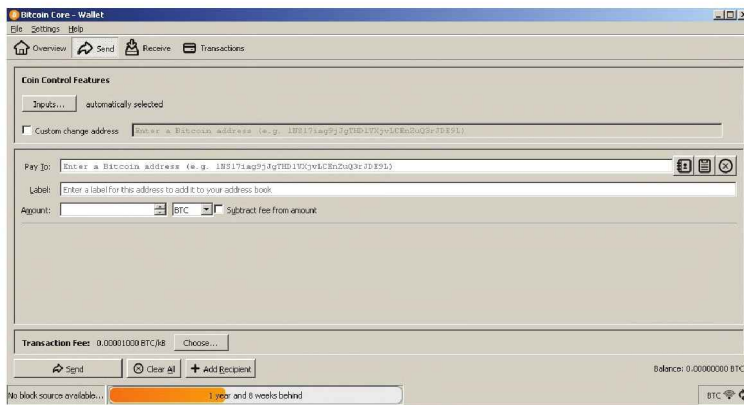
Gambar di atas merupakan tampilan awal aplikasi Bitcoin core atau disebut juga Bit-

coin-qt. Aplikasi ini akan melakukan verifikasi blok atas database yang telah diunduh dan kemudian melakukan pengunduhan atas transaksi-transaksi terbaru yang ada dalam jaringan Bitcoin.



Gambar 47. Tampilan Overview Bitcoin-qt

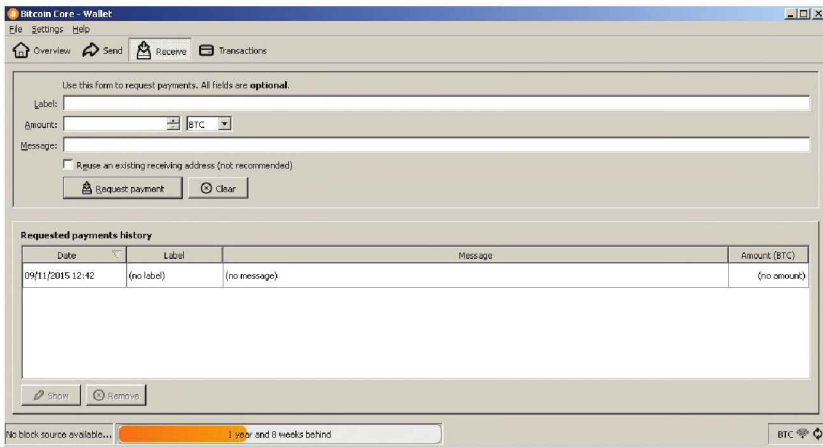
Melalui tampilan *overview* dapat diketahui jumlah total bitcoin yang dimiliki, dan juga informasi beberapa transaksi terakhir yang dilakukan menggunakan aplikasi Bitcoin-qt yang dapat pula bertindak sebagai dompet Bitcoin desktop.



Gambar 48. Fitur Send pada Bitcoin-qt

Sebagaimana juga terdapat pada dompet Bitcoin lainnya, Bitcoin-qt menyediakan fitur untuk mengirim bitcoin ke alamat lain. Fitur unik pada dompet ini adalah terdapat pilihan untuk mengambil biaya transaksi dari total jumlah yang ditransaksikan, misalnya total transaksi sebanyak 0,01 BTC dan biaya transaksi 0,0001 BTC, maka jumlah yang

akan diterima sebesar $0,01-0,0001 = 0,0099\text{BTC}$ atau 99.000 satoshi.



Gambar 49. Fitur Request Payment pada Bitcoin-qt

Fitur Request Payment pada aplikasi Bitcoin-qt dapat digunakan untuk mengelola pembayaran atau piutang yang akan diterima di masa yang akan datang. Melalui fitur ini, penjual barang yang menerima pembayaran dalam bentuk bitcoin dapat mengelola informasi tentang setiap pembayaran yang dilakukan pelanggan.

Dompot Panas dan Dingin

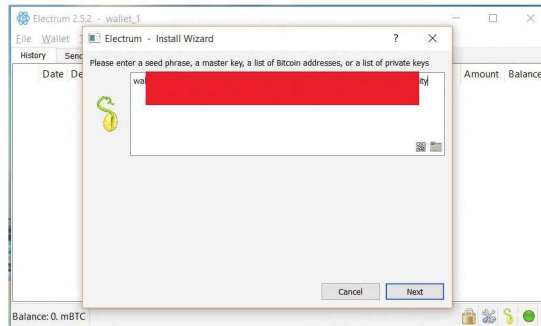
Dompot panas (*hot wallet*) dan dompot dingin (*cold wallet*) merupakan istilah yang dipakai untuk membedakan jenis-jenis dompot Bitcoin. Dompot panas merupakan jenis dompot yang terhubung dalam jaringan internet. Sementara dompot dingin merupakan jenis dompot yang tidak terhubung dengan jaringan internet.

Perbedaan di antara keduanya adalah dari sisi keamanan, di mana dalam hal ini dompot dingin lebih aman dari ancaman *hacker* dibandingkan dengan dompot panas. Namun demikian, dompot dingin lebih sulit diakses sebab tidak terhubung dengan jaringan. Contoh dari dompot dingin adalah dompot kertas (*paper wallet*) dan dompot elektronik yang disimpan di media portabel seperti *flashdisk* yang kemudian disimpan di tempat yang aman yang tidak terhubung dengan komputer. Tentu saja akan sangat berbahaya jika dompot tersebut sampai hilang atau seseorang mencurinya dari tempat penyimpanan.

Dompot Otak

Dompot otak (*brain wallet*) dianggap salah satu dompot yang memiliki tingkat keamanan tertinggi, karena tidak ada seorangpun yang dapat mencurinya kecuali pemilik

dompet tersebut memberikannya pada orang lain. Dompet otak merupakan teknik untuk mengingat kunci rahasia dari dompet Bitcoin dan menghapus dompet Bitcoin dalam versi elektroniknya. Tentu saja tidak mudah mengingat deretan angka dan huruf dalam kunci rahasia tersebut, namun versi terbaru dari dompet Bitcoin biasanya memiliki fasilitas yang disebut dengan seed, yaitu deretan kata-kata berurutan dalam bahasa Inggris yang dapat digunakan untuk mengembalikan informasi sebuah dompet Bitcoin meskipun semua informasi dalam dompet Bitcoin tersebut sudah terhapus.



Gambar 50. Restorasi dompet Bitcoin menggunakan seed pada Electrum

Sebagai contoh, Electrum memiliki fasilitas untuk merestorasi informasi dompet Bitcoin melalui menu New/Restore dari *seed* yang tersedia. •

MENDAPATKAN BITCOIN

SETELAH MENGETAHUI TENTANG BITCOIN DAN BAGAIMANA MENGGUNAKAN DOMPET BITCOIN, KINI SAATNYA MENGISI DOMPET BITCOIN YANG TELAH ANDA BUAT. TERDAPAT BERBAGAI CARA UNTUK MENDAPATKAN BITCOIN PERTAMA ANDA. CARA PALING AMAN DAN PALING MUDAH ADALAH MEMBELINYA DARI *BROKER* BITCOIN SEPERTI BITCOIN INDONESIA ([BITCOIN.CO.ID](http://bitcoin.co.id)). ANDA JUGA DAPAT MEMPEROLEH BITCOIN MELALUI SITUS-SITUS YANG DISEBUT BITCOIN *FAUCET*.

Bitcoin *faucet* akan membayar Anda dengan bitcoin setelah Anda melakukan suatu pekerjaan ringan seperti mengklik iklan atau sejenisnya. Bagi Anda yang berada di Bali, Anda juga dapat membeli bitcoin melalui bitcoin ATM yang mungkin akan tersedia di lebih banyak tempat di masa mendatang saat Bitcoin semakin populer di masyarakat.

Bitcoin Indonesia

Bitcoin Indonesia yang dapat diakses melalui alamat <http://bitcoin.co.id> merupakan pusat perdagangan bitcoin terbesar di Indonesia. Melalui Bitcoin Indonesia, Anda bisa membeli dan menjual bitcoin seperti layaknya perdagangan saham. Tentunya tidak perlu ikut menjadi *trader* bitcoin di sana jika Anda hanya ingin membeli bitcoin, tetapi tidak menutup kemungkinan jika kelak Anda bergabung sebagai trader aktif di bursa bitcoin berbasis rupiah ini.



Gambar 51. Bitcoin Indonesia

Sebelum Anda bisa membeli maupun menjual Bitcoin di dalam sistem VIP Bitcoin Indonesia, terlebih dahulu Anda harus melakukan registrasi melalui <https://vip.bitcoin.co.id/register>.

Isilah dengan lengkap dengan benar

Email

Username

Password ⚠ Dengan generate password yang sama dengan mobile Anda? Password minimal 8 karakter

Ulangi Password

Nomor HP ⚠ Nomor HP untuk verifikasi melalui SMS (one-time authentication)

Nomor Telp. di Laki ⚠ Kami akan menghubungi nomor ini apabila Anda melakukan nomor HP salah

Konfirmasi Persetujuan

PERSetujuan ATAS KETERUNTUN DAN PERSYARATAN

Sebelum membeli maupun menjual Bitcoin, Anda harus memahami bahwa MELAKUKAKAN PEMBELIAN DAN PENJUALAN BITCOIN di Bitcoin.co.id adalah tindakan yang berisiko tinggi. Dengan menggunakan Bitcoin.co.id, Anda akan bertanggung jawab atas keamanan aset digital Anda. Bitcoin.co.id tidak bertanggung jawab atas keamanan aset digital Anda. Bitcoin.co.id tidak bertanggung jawab atas keamanan aset digital Anda. Bitcoin.co.id tidak bertanggung jawab atas keamanan aset digital Anda.

PENGAKHIRAN

Anda memahami bahwa jika Anda telah selesai melakukan pembelian atau penjualan Bitcoin di Bitcoin.co.id, maka Anda akan bertanggung jawab atas keamanan aset digital Anda. Bitcoin.co.id tidak bertanggung jawab atas keamanan aset digital Anda. Bitcoin.co.id tidak bertanggung jawab atas keamanan aset digital Anda. Bitcoin.co.id tidak bertanggung jawab atas keamanan aset digital Anda.

☒ Saya setuju dengan ketentuan dan persyaratan ini

MELAKUKAKAN PEMBELIAN

MELAKUKAKAN PENJUALAN

PT.567 member sudah bergabung, tunggu siapa lagi?

Gambar 52. Bitcoin Indonesia - Register

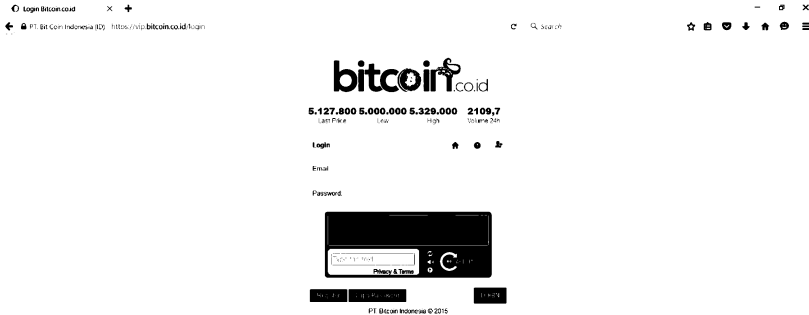
Anda membutuhkan alamat email, *username*, *password*, dan nomor HP untuk melakukan registrasi pada VIP Bitcoin Indonesia sebagaimana ditunjukkan pada gambar. Setelah melakukan registrasi, Anda harus melakukan verifikasi alamat email, verifikasi nomor ponsel, dan kemudian melakukan verifikasi atas data diri. Untuk melakukan verifikasi atas data diri, Anda perlu mengisi data diri lengkap sesuai kartu identitas (semisal KTP)

dan mengambil foto selfie diri Anda sendiri bersama sebuah kertas yang bertuliskan “verifikasi bitcoin.co.id”, nama lengkap, dan tandatangan.



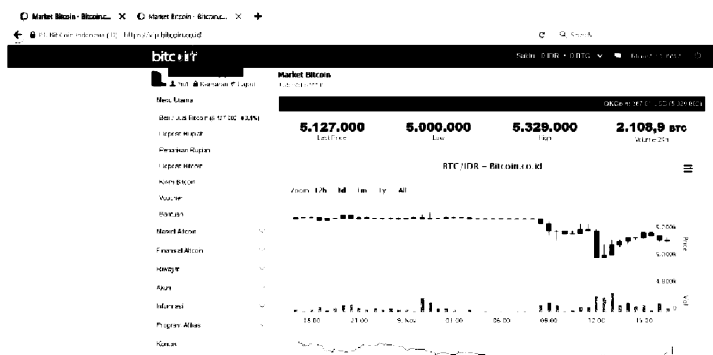
Gambar 53. Contoh selfie untuk verifikasi akun Bitcoin Indonesia

Foto *selfie* bersama bukti kartu identitas ataupun informasi spesifik kini marak digunakan dalam beberapa aplikasi berbasis internet karena dianggap lebih sulit dipalsukan menggunakan *software* pemroses gambar seperti Photoshop.



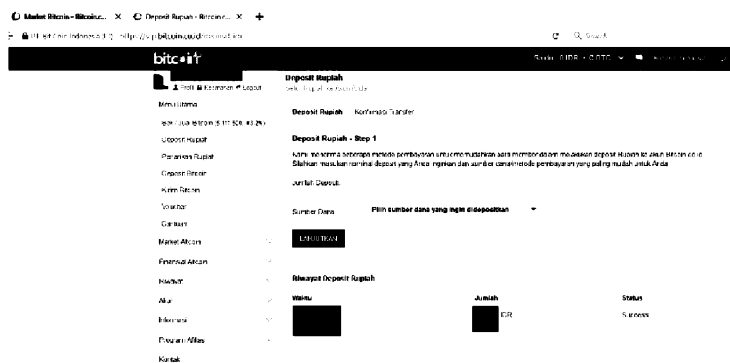
Gambar 54. Bitcoin Indonesia - Login

Halaman login akan tampak seperti pada gambar, Anda dapat masuk ke dalam sistem VIP Bitcoin Indonesia untuk memulai transaksi dengan mengakses situs <https://vip.bitcoin.co.id/login>.



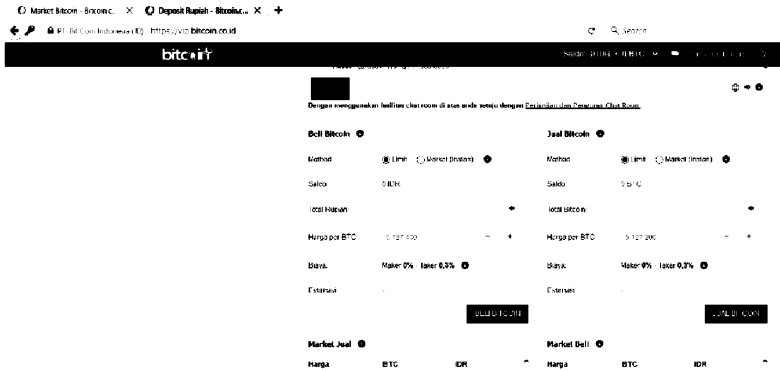
Gambar 55. Bitcoin Indonesia - Menu Utama

Gambar di atas menunjukkan menu utama pada VIP Bitcoin Indonesia. Anda dapat melihat harga bitcoin yang sedang diperdagangkan secara *realtime* dan di-*update* secara terus-menerus. Informasi ini akan membantu Anda dalam melakukan *trading* atau jual beli bitcoin melalui sistem ini. Untuk membeli bitcoin, pertama-tama Anda harus melakukan deposit uang rupiah Anda ke dalam sistem mereka. Anda dapat menuju ke menu “Deposit Rupiah” di bagian kiri tampilan utama.



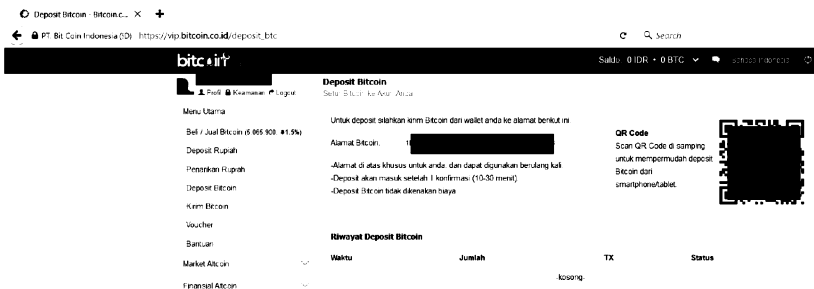
Gambar 56. Bitcoin Indonesia - Deposit Rupiah

Setelah melakukan deposit dan deposit Anda diverifikasi oleh pihak Bitcoin Indonesia, maka Anda bisa mulai membeli bitcoin melalui menu utama di <https://vip.bitcoin.co.id> di bagian bawah tampilan.



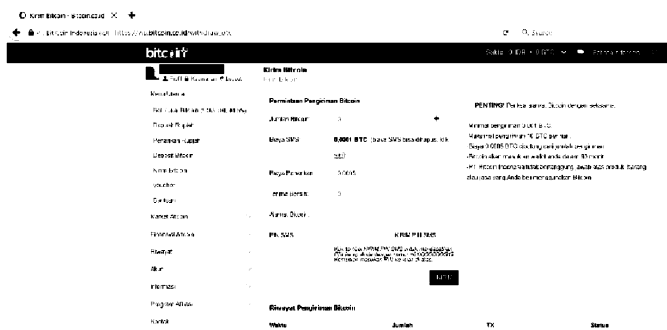
Gambar 57. Bitcoin Indonesia - Beli dan Jual

Untuk membeli bitcoin, Anda dapat menggunakan fitur Beli Bitcoin. Terdapat 2 metode pembelian, yakni Limit dan Market. Metode Limit merupakan metode yang digunakan oleh para pedagang (trader) bitcoin dengan menentukan harga beli mereka sendiri. Artinya, mereka menentukan sebuah harga di mana mereka bersedia membeli bitcoin dengan harga tersebut. Sementara metode Market menggunakan nilai pasar dan transaksi dapat dilakukan pada saat itu juga. Demikian juga ketika Anda ingin menjual bitcoin yang Anda miliki. Anda dapat menggunakan metode Limit dan metode Market. Namun seperti halnya ketika Anda akan membeli bitcoin yang harus melakukan deposit rupiah, sebelum dapat menjual bitcoin, Anda terlebih dahulu harus melakukan deposit bitcoin yang Anda miliki.



Gambar 58. Bitcoin Indonesia - Deposit Bitcoin

Untuk melakukan deposit Bitcoin, Anda dapat menggunakan menu Deposit Bitcoin dan kemudian melakukan pengiriman bitcoin dari alamat Anda ke alamat yang tertera pada laman seperti pada gambar berikut.



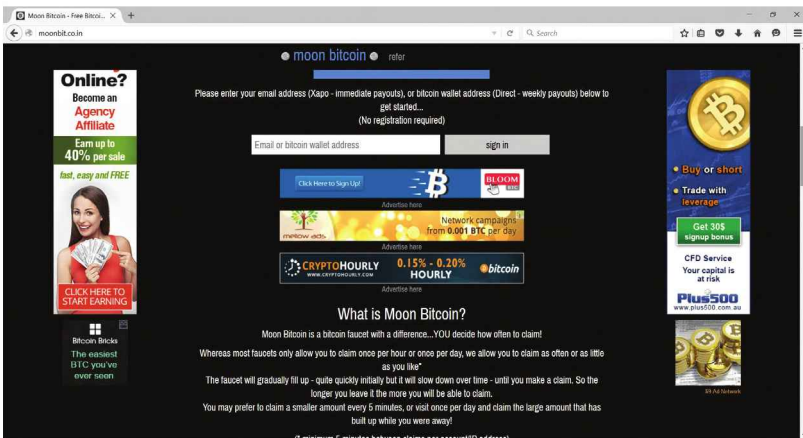
Gambar 59. Bitcoin Indonesia - Kirim Bitcoin

Fitur Kirim Bitcoin yang terdapat pada VIP Bitcoin Indonesia dapat digunakan untuk mengirim saldo bitcoin yang sudah Anda beli dari sistem VIP Bitcoin Indonesia ke alamat lain, misalnya ke salah satu alamat Bitcoin dari dompet Bitcoin Anda. Setelah itu, Anda dapat menggunakannya sekehendak hati.

Bitcoin Faucet

Bitcoin *faucet* merupakan sebutan situs-situs yang menawarkan bitcoin gratis atau menawarkan pembayaran menggunakan bitcoin setelah melakukan pekerjaan tertentu, misalnya dengan mengklik iklan atau mengetik *captcha*. Meskipun kedengarannya mengasyikkan bisa mendapatkan bitcoin gratis, namun pada kenyataannya bermain dengan bitcoin *faucet* membutuhkan waktu yang tidak sedikit, sebab bitcoin gratis yang dibagikan dan bitcoin yang dibayarkan jumlahnya sangat kecil. Demikian pula dengan sisi keamanan. Tidak ada yang dapat menjamin bahwa situs-situs bitcoin *faucet* ini memiliki tingkat keamanan yang dapat dijamin dan tidak menyisipkan skrip berbahaya bagi komputer Anda. Oleh sebab itu tidak disarankan bagi Anda untuk menggunakan Bitcoin *faucet* untuk mengumpulkan bitcoin bagi dompet Bitcoin Anda.

Salah satu contoh Bitcoin Faucet adalah Moon Bitcoin (<http://moonbit.co.in>). Untuk memperoleh bitcoin gratis, Anda harus menunggu setiap 5 menit dan mengisi *captcha*. Bitcoin akan dibayarkan setiap minggu sekali dengan syarat harus sudah mencapai 5500 satoshi. Anda dapat mencobanya sendiri, namun perlu diingat bahwa tidak ada jaminan bahwa bitcoin Anda akan dibayarkan seperti yang dijanjikan. Anda juga perlu berhati-hati terhadap iklan yang muncul dalam situs tersebut, sebab mungkin tidak semua iklan yang ada di sana berasal dari pengiklan yang jujur.



Gambar 60. Moon Bitcoin

Bitcoin ATM

Bitcoin ATM merupakan salah satu teknologi yang dikembangkan untuk mempermudah masyarakat mendapatkan bitcoin. Bitcoin ATM pertama kali dipasang di Vancouver, Kanada. Kemudian, teknologi Bitcoin ATM berkembang dan beberapa ratus mesin telah terpasang di seluruh dunia.



Gambar 61. Bitcoin ATM di Emporium Mall, Melbourne Australia

Terdapat 2 jenis Bitcoin ATM, yakni Bitcoin ATM yang hanya bisa digunakan untuk membeli bitcoin dan Bitcoin ATM yang selain bisa digunakan untuk membeli bitcoin, juga bisa digunakan untuk menjual bitcoin. Untuk membeli bitcoin melalui Bitcoin ATM, Anda dapat memasukkan uang seperti halnya ketika akan membeli minuman kaleng dari vending machine, kemudian lakukan *scan* alamat Bitcoin tujuan dan validasi jumlah bitcoin yang Anda dapatkan, maka transaksi akan segera dilakukan dan bitcoin bertambah dalam dompet Bitcoin Anda.

Mesin-mesin Bitcoin yang ada di Indonesia lebih berupa *vending machine*, di mana konsumen hanya bisa membeli Bitcoin tetapi tidak bisa menjual Bitcoin miliknya pada mesin yang sama. Saat ini, menurut Coin ATM Radar (<http://coinatmradar.com>), terdapat beberapa Bitcoin vending machine di Indonesia, yang berlokasi di Jakarta dan Bali.

Menambang Bitcoin

Selain cara-cara yang sudah disebutkan di atas, menambang Bitcoin merupakan cara lain yang dapat ditempuh untuk memperoleh bitcoin. Apa itu menambang Bitcoin? Untuk menjawab pertanyaan ini, kita perlu beralih ke sedikit hal teknis mengenai sistem Bitcoin. Seperti yang telah dibahas, sistem Bitcoin tidak mengenal bank sentral untuk mengatur transaksi keuangan Bitcoin. Bitcoin sendiri berjalan di dalam sistem yang mengandalkan kontrol terdistribusi untuk melakukan verifikasi atas seluruh transaksi yang terjadi di dalam sistem. Verifikasi tersebut dilakukan oleh para penambang dengan menggunakan peralatan mereka dalam melakukan kalkulasi matematis.

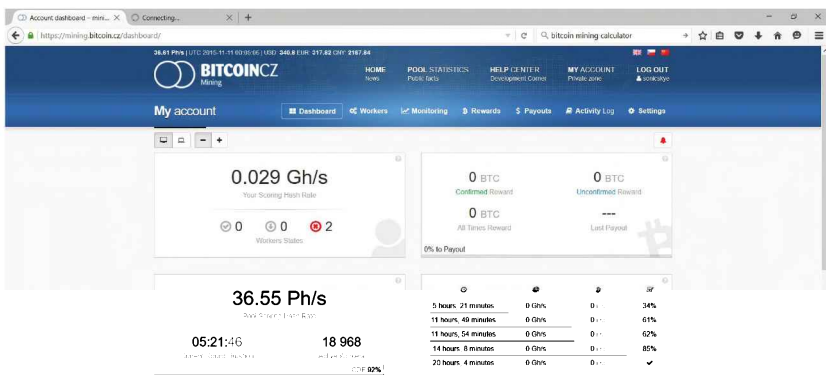
Seluruh transaksi yang dilakukan pada suatu waktu dikumpulkan ke dalam sebuah blok dan mereka menghitung nilai tertentu dari blok tersebut, sebelum diakui sebagai transaksi yang sah. Kalkulasi yang dilakukan tersebut dinamakan proses menambang (*mining*). Nah, karena proses menambang dalam sistem Bitcoin dilakukan menggunakan kalkulasi matematis, tentunya semua orang yang memiliki komputer dapat melakukannya. Namun demikian, dengan tingkat persaingan yang sangat tinggi sekarang ini di dalam sistem Bitcoin, menggunakan komputer rumahan saja tidak akan membuahkan hasil yang memuaskan.



Gambar 62. ANTMINER S7. Sumber : bitmaintech.com

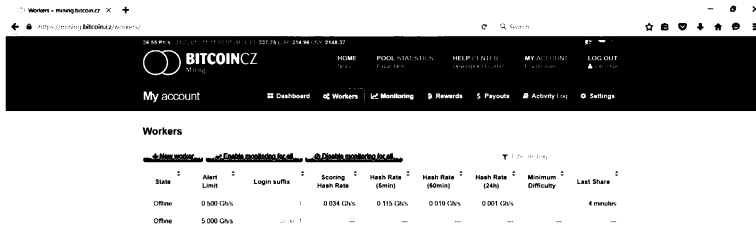
Dengan perkembangan teknologi, kini para penambang tidak lagi menggunakan komputer atau laptop biasa, melainkan menggunakan alat khusus yang disebut ASIC (Application Specific Integrated Circuit), yaitu sirkuit elektronika, khusus yang dibuat untuk melakukan perhitungan matematis yang digunakan dalam sistem Bitcoin. Dengan menggunakan ASIC, para penambang dapat menghasilkan bitcoin dengan lebih efisien dari sisi biaya, sebab ASIC memiliki kemampuan kalkulasi spesifik yang lebih tinggi dibandingkan komputer biasa dengan konsumsi listrik yang rendah. Untuk dapat menghasilkan bitcoin dengan jumlah signifikan, dengan tingkat persaingan saat ini, diperlukan investasi yang tidak sedikit untuk membeli peralatan ASIC, menyiapkan ruangan berpendingin yang memadai, dan membayar tagihan listrik. Karena tingkat persaingan yang tinggi, para penambang kecil biasanya bergabung dalam semacam *broker* yang disebut *mining pool*. Dengan bergabung dalam *mining pool*, para penambang bisa memperoleh hasil yang lebih besar dibandingkan jika harus menambang bitcoin sendirian.

Apabila Anda tertarik untuk menambang dengan komputer Anda sendiri, tidak ada salahnya mencoba walaupun mungkin tidak menghasilkan bitcoin dengan nilai yang cukup signifikan. Anda dapat menggunakan aplikasi GUIMiner yang mudah digunakan karena memiliki antarmuka grafis (*graphical user interface*). Informasi lebih lanjut tentang aplikasi ini dapat dilihat di <https://guiminer.org>. Anda dapat mengunduh aplikasi GUIMiner melalui alamat <https://github.com/downloads/Kiv/poclbm/guiminer-20121203.exe>. Kemudian Anda harus melakukan registrasi ke salah satu mining pool. Terdapat beberapa *mining pool* populer yang dapat Anda gunakan, salah satunya Slush. Untuk melakukan registrasi, Anda dapat mengunjungi situs <https://mining.bitcoin.cz/accounts/register/>. Anda memerlukan *username*, *password*, dan alamat email dalam melakukan registrasi. Kemudian, Anda dapat memverifikasi alamat email tersebut dengan mengklik *link* yang dikirimkan ke alamat *e-mail* Anda tadi.



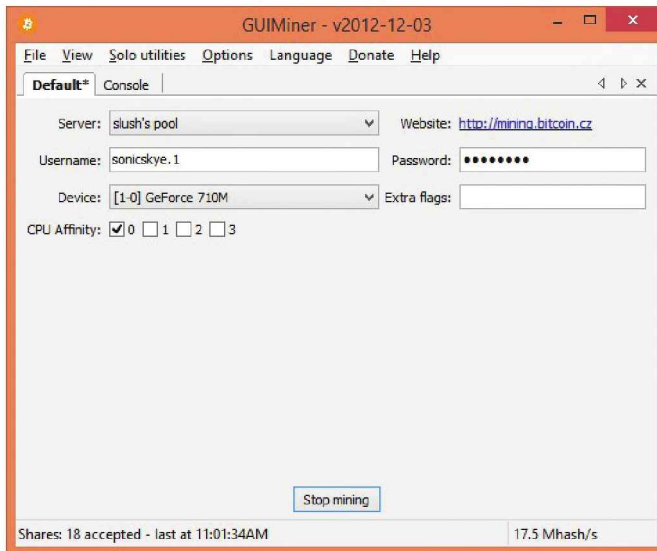
Gambar 63. Slush Dashboard

Slush memiliki fitur lengkap yang dapat digunakan untuk memonitor kinerja pertambangan Anda. Sebelum menjalankan aplikasi GUIMiner, Anda harus membuat *workers*, yaitu subakun yang digunakan oleh aplikasi Anda agar sistem Slush dapat memonitor kinerja para *workers* milik Anda. Akun Slush Anda sudah memiliki 1 *worker* sebagai *default*, yakni *worker1*. Anda dapat menambahkan *worker* lain sebanyak yang Anda inginkan.



Gambar 64. Daftar worker Slush

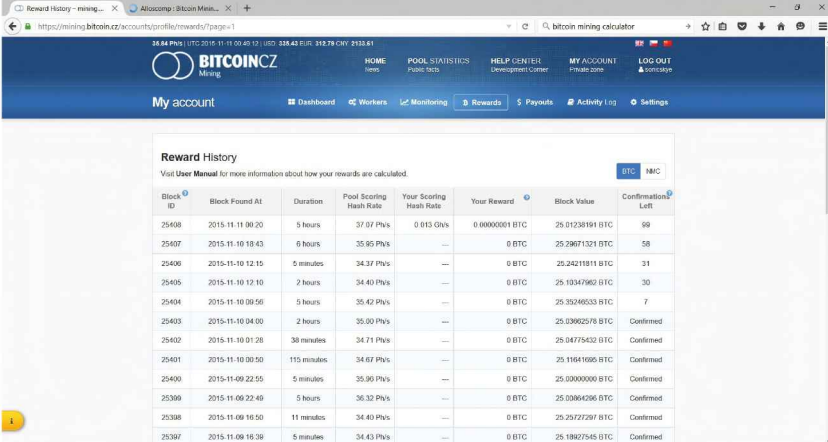
Setelah meregistrasikan worker Anda, Anda dapat memulai kegiatan pertambangan menggunakan aplikasi GUIMiner yang telah disiapkan sebelumnya.



Gambar 65. GUIMiner

Melalui aplikasi GUIMiner, beberapa *setting* harus Anda buat. Untuk *server*, gunakan *server* “slush’s pool”. *Username* diisi dengan format *Username.Worker* dan *password*

dapat diisi *password* akun Anda. Misalnya *username* Anda adalah “Aku123” dan memiliki *worker* bernama “worker1”, maka *username* pada GUIMiner dapat diisi dengan “Aku123.worker1”. Untuk *device*, Anda dapat memilih apakah akan menambang menggunakan CPU (prosesor) atau GPU (kartu grafis). Secara umum, kartu grafis memiliki kinerja lebih baik dibandingkan CPU. Setelah semuanya diisi, klik Start mining.



Block ID	Block Found At	Duration	Pool Scoring Hash Rate	Your Scoring Hash Rate	Your Reward	Block Value	Confirmations
25408	2015-11-10 09:20	5 hours	37.07 P/s	0.013 G/s	0.00000001 BTC	25.01238191 BTC	99
25407	2015-11-10 18:43	8 hours	35.95 P/s	---	0 BTC	25.29671321 BTC	58
25406	2015-11-10 12:15	5 minutes	34.37 P/s	---	0 BTC	25.24211911 BTC	31
25405	2015-11-10 12:10	2 hours	34.40 P/s	---	0 BTC	25.19347960 BTC	30
25404	2015-11-10 08:56	5 hours	35.42 P/s	---	0 BTC	25.35246003 BTC	7
25403	2015-11-10 04:00	2 hours	35.00 P/s	---	0 BTC	25.03962579 BTC	Confirmed
25402	2015-11-10 01:28	38 minutes	34.71 P/s	---	0 BTC	25.04775432 BTC	Confirmed
25401	2015-11-10 00:50	115 minutes	34.67 P/s	---	0 BTC	25.11641995 BTC	Confirmed
25400	2015-11-09 22:55	5 minutes	35.90 P/s	---	0 BTC	25.00000000 BTC	Confirmed
25399	2015-11-09 22:49	5 hours	36.30 P/s	---	0 BTC	25.00964096 BTC	Confirmed
25398	2015-11-09 16:50	11 minutes	34.40 P/s	---	0 BTC	25.25272797 BTC	Confirmed
25397	2015-11-09 16:39	5 minutes	34.43 P/s	---	0 BTC	25.19827545 BTC	Confirmed

Gambar 66. Slush Reward

Setelah beberapa saat menjalankan aplikasi, Anda dapat melihat hasilnya melalui menu Rewards seperti pada gambar di atas. Dengan tingkat komputasi 0,1 GHash/s, dalam waktu 5 jam hanya diperoleh upah 0,00000001 BTC atau setara dengan 1 satoshi, jumlah yang sangat kecil dan bahkan tidak cukup untuk membayar biaya transaksi Bitcoin.

Untuk dapat memperkirakan hasil yang didapatkan pada usaha pertambangan Anda, Anda dapat menggunakan Bitcoin Mining Calculator seperti tampak pada gambar di bawah ini.

Bitcoin Mining Calculator

Got your shiny new ASIC miner? Wondering when it will pay off? If you enter your hash rate below, this page will calculate your expected earnings in both Bitcoins and dollars over various time periods (day, week, and month). It will not attempt to extrapolate difficulty or price changes – it provides only instantaneous calculations (how much you'd make if all conditions remained as they were right now).

An API is available at <https://alloscomp.com/bitcoin-calculator/join>

Next difficulty retarget occurs at block 383039.0 (eta 12.8 hrs): 62253862449.8 / +0.0% (est.)

Difficulty Factor 62253862449.8

Hash Rate: 0.1 GH/s

Exchange Rate: 343.1 (\$/BTC) [use]

BTC / Block: 25.00000000

Calculate

This Difficulty		Next Difficulty (estimated)	
Coins	Dollars	Coins	Dollars
per Day 0.00000081 BTC	\$0.00	per Day 0.00000081 BTC	\$0.00
per Week 0.00000567 BTC	\$0.00	per Week 0.00000567 BTC	\$0.00
per Month 0.00001759 BTC	\$0.01	per Month 0.00001759 BTC	\$0.01
this diff (est) 0.00000043 BTC	\$0.00		

Has this service helped you? BTC: 1K6QhmrjEY7ghSB6kvLFH32v1KqJ

Gambar 67. Bitcoin Mining Calculator. Sumber: alloscomp.com

Bitcoin Mining Calculator menunjukkan bahwa dibutuhkan usaha ekstra untuk menghasilkan cukup banyak bitcoin, dan dengan kondisi saat ini, menambang bitcoin tidak ditujukan bagi semua orang sebab membutuhkan modal dan infrastruktur yang memadai.

Selain membeli mesin sendiri untuk menambang, Anda bisa juga menyewa mesin milik orang lain melalui layanan Cloud Mining. Perusahaan yang menyediakan layanan cloud mining memperbolehkan pengguna menggunakan peralatan milik mereka, tentunya dengan biaya yang mereka tetapkan pada setiap layanan mereka. Pengguna bisa mendapatkan keuntungan dari hasil penambangan Bitcoin dari layanan tersebut, namun perlu diketahui bahwa tidak sedikit layanan *cloud mining* yang hanya menghasilkan kerugian bagi para penggunanya atau bahkan menawarkan layanan yang tidak sesuai harapan.

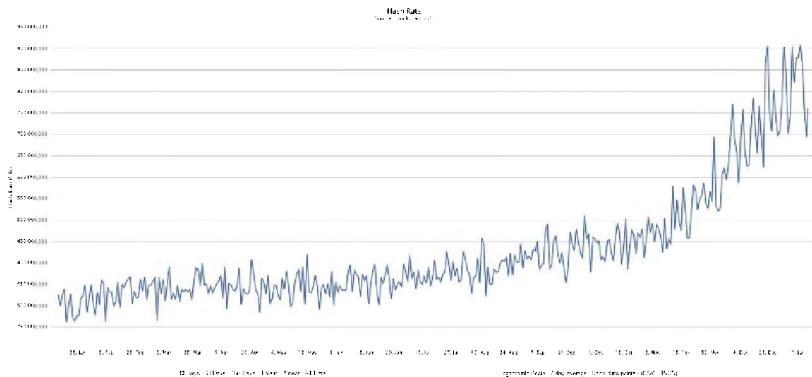
Penambangan Bitcoin sendiri memiliki risiko tinggi, dan menyewa mesin orang lain yang tidak diketahui kualitasnya menambah risiko yang sudah ada. Contoh *cloud mining* adalah Genesis Mining (<http://www.genesis-mining.com>) dan CEX.IO (<https://cex.io/cloud-mining>). Sehubungan dengan semakin tingginya tingkat komputasi yang ada dalam jaringan Bitcoin, maka membeli layanan dengan tingkat komputasi 1-2 GHash/s saja memiliki potensi keuntungan yang sangat kecil dan harus dipertimbangkan masak-masak.

Beberapa hal yang perlu Anda ketahui sebelum berkecimpung dalam usaha penambangan Bitcoin, di antaranya *hash rate* dan *difficulty*. *Hash rate* merupakan total kekuatan komputasi yang ada di dalam sistem Bitcoin. Mudahnya, *hash rate* diibaratkan sebagai jumlah total kemampuan alat pertambangan yang dimiliki oleh para penambang Bitcoin di seluruh dunia, baik yang menambang menggunakan komputer biasa maupun yang

menambang menggunakan peralatan terbaru.

Saat buku ini ditulis, *hash rate* total berada di kisaran angka 325 PH/s (Peta Hash per detik) di mana 1 Peta Hash setara dengan 1000 Tera Hash, dan 1 Tera Hash sama dengan 1000 Giga Hash, 1 Giga Hash sama dengan 1000 Mega Hash, sehingga 325 PH/s setara dengan 325 kuadriliun hash per detik.

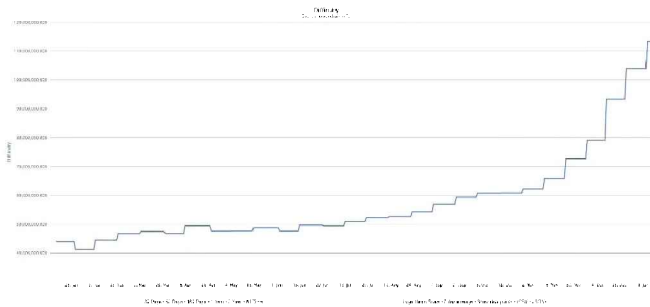
Tentunya angka ini bukanlah angka maksimal, sebab peningkatan harga pasar Bitcoin akan menarik investasi lebih banyak pada peralatan pertambangan yang lebih baik, dan sebagai akibatnya *hash rate* akan semakin tinggi. Penambang Bitcoin yang tidak mampu bersaing dengan kenaikan *hash rate* tentu saja akan tergerus pendapatannya jika tidak mampu menginvestasikan lebih banyak dana untuk mencapai *hash rate* yang lebih tinggi.



Gambar 68. Grafik Hash Rate. Sumber: blockchain.info

Difficulty sangat berhubungan dengan *hash rate* pada jaringan Bitcoin. Bitcoin akan menyesuaikan dengan tingkat *hash rate* rata-rata selama 2 minggu sebelum dilakukan penyesuaian. Semakin tinggi *hash rate*, maka semakin tinggi pula *difficulty* yang ada. Tujuan kenaikan *difficulty* adalah agar sebuah blok ditambang setiap 10 menit, tidak lebih dan tidak kurang. Oleh karena itu, apabila *hash rate* meningkat, maka sebuah blok dapat ditambang kurang dari 10 menit dan untuk itulah *difficulty* akan ditingkatkan.

Demikian pula, apabila sebuah blok ditambang lebih dari 10 menit, maka *difficulty* akan diturunkan. Grafik *difficulty* menunjukkan kesamaan pola dengan grafik *hash rate*. Semakin tinggi *hash rate*, maka *difficulty* akan semakin tinggi pula.



Gambar 69. Grafik Difficulty. Sumber: blockchain.info

Ketika Anda memutuskan untuk ikut menambang Bitcoin, secara umum ada 2 pilihan buat Anda. *Pertama*, Anda menambang sendiri, atau pilihan *kedua* Anda bisa bergabung dengan komunitas yang disebut dengan mining pool, salah satunya adalah Slush sebagaimana telah dibahas.

Kedua pilihan tersebut memiliki kelebihan dan kekurangan. Ketika Anda menambang sendiri, maka seluruh keuntungan yang didapat dari menghasilkan blok baru akan Anda nikmati sendiri, yaitu sebesar *block reward* yang saat ini sejumlah 25 BTC ditambah dengan *transaction fee* (biaya transaksi) dari semua transaksi yang ada dalam blok tersebut.

Kekurangannya, menambang sendiri sangatlah sulit, sebab tingkat persaingan sangat tinggi, seperti yang telah dijelaskan bahwa *hash rate* sudah sedemikian tinggi dan secara teoretis dibutuhkan waktu berbulan-bulan, bahkan bertahun-tahun untuk menghasilkan sebuah blok dari menambang sendiri.

Pilihan kedua adalah bergabung dengan *mining pool*, yakni komunitas para penambang yang dikoordinasikan oleh operator mining pool, bekerja bersama-sama untuk memenangkan sebuah blok. Ketika sebuah blok dimenangkan oleh *mining pool* tersebut, maka keuntungan akan dibagi-bagi di antara para penambang sesuai dengan kontribusinya. Terdapat beberapa sistem bagi hasil yang umum dipakai, namun kebanyakan di antaranya didasarkan pada jumlah share yang berhasil diselesaikan oleh mesin penambang tersebut.

Cara Lain

Apakah ada cara lain untuk mendapatkan bitcoin? Tentu saja. Anda bisa menjual sesuatu pada orang lain dan menerima bitcoin sebagai bayarannya. Sederhana. Atau, Anda juga bisa membeli bitcoin langsung dari orang lain, misalnya dari teman atau kenalan Anda sendiri.

Apabila Anda tidak mengenal satu orangpun yang bersedia menjual bitcoin, Anda dapat mencarinya melalui Localbitcoins.com (<https://localbitcoins.com>), situs di mana orang-orang bisa langsung menjual bitcoin miliknya dengan harga yang mereka tentukan sendiri. Localbitcoins.com akan merekomendasikan beberapa penjual bitcoin berdasarkan lokasi Anda. Melalui Localbitcoins.com, Anda tidak hanya bisa membeli bitcoin, namun juga bisa menjual bitcoin milik Anda pada mereka yang menawarkan suatu harga beli. Para penjual ini juga menentukan berapa batas nilai minimal dan maksimal yang dapat mereka layani. Terdapat pula beberapa metode pembayaran yang tersedia, seperti PayPal dan transfer bank.

Ada beberapa hal yang perlu Anda siapkan apabila Anda berminat untuk menerima pembayaran dalam bentuk bitcoin untuk barang maupun jasa yang Anda jual pada pelanggan. *Pertama*, tentu saja perangkat lunak (*software*) yang dapat membantu Anda melakukan pengaturan pembayaran dan juga mengkonversi harga ke dalam nilai bitcoin.

Beberapa perangkat lunak dapat digunakan, di antaranya XBTerminal (<https://xbterminal.io/id>) yang tersedia dalam versi *desktop* maupun *mobile* dan Coinbox yang tersedia di Google Play (<https://play.google.com/store/apps/details?id=com.coinbox&hl=in>) untuk perangkat mobile.

Kedua, tentunya koneksi Internet untuk menghubungkan perangkat lunak tersebut dengan jaringan Bitcoin untuk kepentingan *update* nilai kurs dan konfirmasi transaksi. Meskipun perangkat lunak tersebut dapat membantu Anda untuk menerima pembayaran dalam bentuk bitcoin, Anda bisa juga melakukan proses tersebut secara manual. Hal yang penting adalah Anda menyediakan informasi alamat Bitcoin dengan cara yang mudah terbaca misalnya dengan format QRCode. Untuk membuat QRCode, Anda dapat menggunakan perangkat online gratis yang tersedia, misalnya QR Code Generator (<http://www.qr-code-generator.com/>). Kemudian Anda menentukan sendiri nilai kurs rupiah ke bitcoin atau dapat juga merujuk ke bitcoin exchange seperti Bitcoin Indonesia (<https://www.bitcoin.co.id/>) atau dapat juga menggunakan Google dengan kata kunci “X IDR to BTC”, dengan huruf X merupakan harga barang atau jasa dalam nominal rupiah, misalnya harga barang Rp 10 ribu maka kata kunci yang dapat dipakai adalah “10000 IDR to BTC” (tanpa tanda petik). •

MENGGUNAKAN BITCOIN

TERDAPAT BANYAK CARA UNTUK MENGGUNAKAN BITCOIN YANG ANDA MILIKI. ANDA DAPAT MENGGUNAKANNYA SEBAGAI ALAT PEMBAYARAN SEBAGAIMANA UANG RUPIAH, TETAPI ADA PULA BERBAGAI MACAM PENGGUNAAN BITCOIN SELAIN SEBAGAI UANG DIGITAL, YANG AKAN DIBAHAS PADA BAB INI.

Anda dapat membeli barang dari toko-toko yang menerima Bitcoin sebagai alat pembayaran. Anda dapat membeli barang dari toko *online* maupun *offline*. Pada umumnya, toko-toko yang menerima Bitcoin memasang gambar khusus, misalnya pada gambar berikut.



Gambar 70. Logo Menerima Bitcoin

Bitcoin sebagai Alat Pembayaran

Tentunya untuk melakukan pembayaran dengan Bitcoin, Anda perlu meminta alamat Bitcoin dari toko tersebut, mengisi jumlah bitcoin, dan membuat transaksinya dari dompet Bitcoin Anda. Tentunya terdapat kelebihan dan kekurangan saat melakukan pembayaran menggunakan bitcoin.

Daftar toko dan usaha yang menerima bitcoin di seluruh dunia dapat Anda lihat di <https://en.bitcoin.it/wiki/Trade>, sementara untuk daftar di Indonesia, Anda dapat merujuk ke <http://blog.bitcoin.co.id/toko/>. Meskipun Bitcoin makin banyak dipakai dalam transaksi, namun jumlah maupun nominalnya masih jauh di bawah transaksi uang fiat.

Transaksi Standar

Kelebihan dari transaksi menggunakan Bitcoin adalah keamanan dari sisi penjual. Sebagaimana diketahui bahwa transaksi menggunakan PayPal dapat dibatalkan oleh pihak pembeli melalui fasilitas *dispute*, begitu juga dengan transaksi kartu kredit yang membutuhkan waktu yang cukup lama untuk menyelesaikan sebuah transaksi. Namun dengan menggunakan Bitcoin, transaksi pembayaran tersebut akan dapat diselesaikan dalam waktu 10-60 menit. Juga, transaksi menggunakan Bitcoin tidak dapat dibatalkan oleh pembeli. Artinya dana yang telah dibayarkan ke penjual tidak dapat ditarik kembali kecuali penjual mengizinkan pengembalian dana tersebut dengan membuat transaksi baru (Darmawan, 2014).

Sementara itu, kekurangan dari transaksi menggunakan Bitcoin adalah dari sisi pembeli, sebab dengan tiadanya jaminan dari pihak manapun, sebuah transaksi tidak dapat dibatalkan ketika sesuatu tidak berjalan dengan semestinya. Misalnya Anda membeli sebuah barang dari toko *online* dan ternyata Anda tidak mendapatkan barang dengan kualitas sebagaimana dijanjikan, maka pembayaran tersebut tidak dapat ditarik kembali sebab tidak ada bank yang menjamin transaksi tersebut.

Transaksi Escrow

Meskipun dalam transaksi standar Bitcoin tampaknya tidak ada jaminan perlindungan bagi pembeli maupun penjual karena sifatnya yang tidak dapat dibatalkan, Bitcoin sebenarnya memiliki fasilitas bagi mereka yang ingin membuat mediator (*escrow*) dalam sebuah transaksi. Jenis transaksi seperti ini dalam sistem Bitcoin dapat disebut transaksi *2-of-3 escrow*. Transaksi ini berarti bahwa dibutuhkan persetujuan paling sedikit 2 pihak untuk melakukan transaksi. Dua pihak ini bisa terdiri atas pembeli dan mediator, penjual dan mediator, ataupun pembeli dan penjual.

Sebagai contoh untuk kasus pertama, pembeli tidak merasa puas terhadap barang yang dibelinya karena kualitasnya lebih rendah daripada yang dijanjikan, atau bahkan mungkin barang yang telah dibayar tidak pernah diterima, maka mediator dapat berpihak pada pembeli dan dana dikembalikan kepada sang pembeli.

Contoh untuk kasus kedua adalah ketika penjual telah mengirim barang sesuai spesifikasi namun pembeli tidak mengakui pernah menerima barang tersebut, maka mediator dapat berpihak pada penjual dan mentransfer dana ke pihak penjual. Sementara untuk kasus ketiga, transaksi berjalan dengan semestinya dan pembeli maupun penjual sepa-

kat melakukan jual beli menggunakan bitcoin. Sistem mediator sama sekali berbeda dibandingkan sistem *rekber* (rekening bersama), di mana sang pengelola *rekber* memiliki peluang untuk mencuri dana yang ditransfer kepadanya.

Melalui mekanisme *escrow* dalam sistem Bitcoin, pihak mediator tidak menyimpan dana dalam dompet mereka sendiri dan tidak memiliki otoritas untuk memanfaatkan dana tersebut, sebab diperlukan persetujuan dari 2 pihak, yakni pembeli ataupun penjual untuk menggunakan dana *escrow* tersebut.

Konfirmasi Transaksi

Bagi Anda yang menerima transaksi bitcoin dalam jumlah yang besar, terdapat sebuah prinsip umum yang biasa dipakai dalam komunitas Bitcoin di dunia, yakni menunggu hingga transaksi mendapat setidaknya 6 konfirmasi baru kemudian transaksi dapat dianggap berhasil, sebab terdapat kelemahan dalam sistem Bitcoin di mana transaksi yang sudah terverifikasi dalam blok pun masih dapat diubah ataupun hilang. Oleh karena itu, menunggu hingga lebih kurang 60 menit dapat meningkatkan keamanan dari transaksi. Sementara untuk transaksi mikro biasanya tidak perlu menunggu hingga lebih dari 10 menit agar para konsumen tidak merasa terganggu dengan jeda waktu yang cukup lama tersebut.

Ajang Promosi Usaha

Bitcoin merupakan sebuah peluang yang bagus bagi para pemilik usaha. Dengan memberi dukungan pada metode pembayaran Bitcoin, maka usaha tersebut akan mendapatkan ekspos yang baik dalam komunitas Bitcoin yang semakin berkembang di seluruh dunia, termasuk Indonesia. Usaha tersebut dapat didaftarkan di berbagai situs yang menyediakan informasi toko-toko yang menerima Bitcoin, yang berarti pula sebagai ajang promosi gratis. Memberi dukungan terhadap Bitcoin juga berarti memberikan kesan bahwa usaha tersebut membuka diri terhadap perkembangan teknologi.

Status Bitcoin di Indonesia

Perkembangan Bitcoin di Indonesia masih belum didukung oleh regulasi yang memadai. Saat ini Bank Indonesia melalui siaran pers Bank Indonesia nomor 16/6/DKom tanggal 6 Februari 2014 hanya menyebutkan Bitcoin bukan sebagai alat pembayaran yang sah di Indonesia.

Demikian petikan siaran pers tersebut.

Memperhatikan Undang-undang No. 7 Tahun 2011 tentang Mata Uang serta UU No. 23 Tahun 1999 yang kemudian diubah beberapa kali, terakhir dengan Undang-Undang No. 6 Tahun 2009, Bank Indonesia menyatakan bahwa Bitcoin dan virtual currency lainnya bukan merupakan mata uang atau alat pembayaran yang sah di Indonesia.

Masyarakat dihimbau untuk berhati-hati terhadap Bitcoin dan virtual currency lainnya. Segala risiko terkait kepemilikan/penggunaan Bitcoin ditanggung sendiri oleh pemilik/pengguna Bitcoin dan virtual currency lainnya.

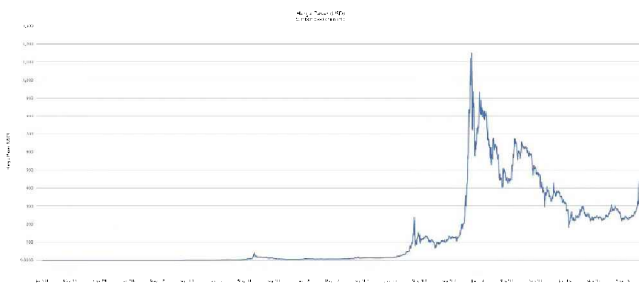
*Jakarta, 6 Februari 2014
Departemen Komunikasi*

Peter Jacobs
Direktur

Dengan demikian, seluruh pengguna Bitcoin diharapkan berhati-hati dalam melakukan transaksi dengan menggunakan Bitcoin, sebab pemerintah tidak menjamin Bitcoin atas segala risiko yang terjadi.

Bitcoin sebagai Alat Investasi dan Komoditas Perdagangan

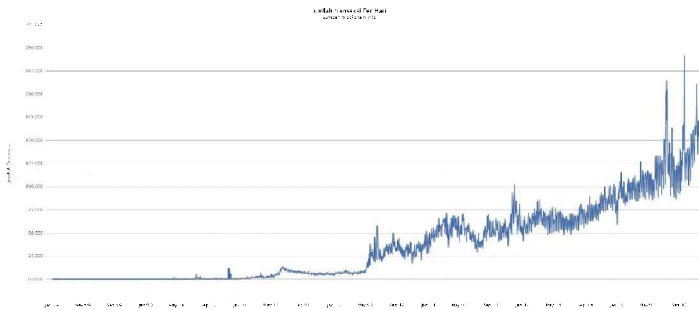
Dengan nilainya yang cenderung meningkat dalam jangka panjang, banyak orang membeli bitcoin dengan mengharapkan kenaikan harga terhadap mata uang resmi. Dalam sejarahnya, nilai bitcoin meningkat pesat selama 6 tahun ini dari tidak berharga sama sekali sampai dengan sekarang bernilai Rp 5 juta untuk setiap BTC yang diperdagangkan. Dengan jumlah pengguna Bitcoin yang makin meningkat, banyak orang yang masih berharap peningkatan harga Bitcoin akan tetap terjadi di masa yang akan datang.



Gambar 71. Grafik pergerakan harga bitcoin dalam satuan Dolar AS. Sumber: *blockchain.info*

Namun demikian, bagi Anda yang berminat untuk berinvestasi dengan membeli bitcoin, ada baiknya Anda mempelajari karakteristik harga bitcoin. Nilai Bitcoin sangatlah tidak stabil dan berubah dengan sangat cepat dari hari ke hari, bahkan jam ke jam, sebab dipengaruhi oleh permintaan dan penawaran.

Saat permintaan meningkat pesat, maka harga bitcoin ikut terkerek naik, namun saat permintaan turun tajam, misalnya karena regulasi baru tentang Bitcoin yang membatasi penggunaannya, harga bitcoin juga dapat terjun bebas. Tidak seperti investasi dalam bentuk saham maupun obligasi, investasi bitcoin tidak memiliki jaminan apapun, sehingga ketika suatu saat bitcoin menghilang dari peredaran dan tidak lagi digunakan oleh masyarakat, maka nilainya pun akan ikut menghilang. Oleh karena itu, sebagai alat investasi, Bitcoin dipandang sebagai investasi yang berisiko tinggi. Dengan Bitcoin sebagai alat investasi, Anda dapat menggunakan *paper wallet* dan menyimpan *paper wallet* tersebut di tempat yang aman, misalnya di *safe deposit box* di bank.

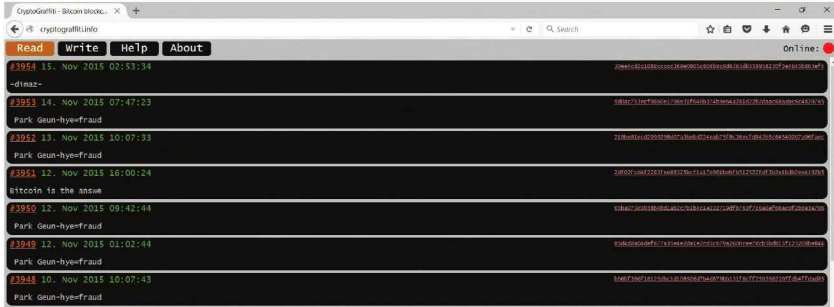


Gambar 72. Jumlah transaksi harian Bitcoin

Bitcoin dapat pula dipandang sebagai komoditas perdagangan. Keuntungan dapat diperoleh dari selisih antara harga beli dan harga jual. Di Indonesia, Anda dapat bergabung menjadi trader bitcoin melalui Bitcoin Indonesia (<https://www.bitcoin.co.id>). Namun demikian, sama halnya dengan bitcoin sebagai alat investasi, meskipun peluang untuk mendapatkan keuntungan besar, bitcoin sebagai komoditas perdagangan memiliki risiko tinggi.

Bitcoin dan Inovasi Teknologi

Bitcoin memiliki peluang pemanfaatan yang cukup luas. Selain digunakan untuk mendukung *e-commerce*, Bitcoin yang memiliki arsitektur unik dapat digunakan untuk menyimpan informasi yang akan tetap berada dalam sistem Bitcoin sampai kapanpun. Bitcoin juga dapat digunakan untuk aplikasi pengirim pesan, yang biasa disebut Bitcoin messaging. Bitcoin *messaging* bisa digunakan untuk menghindari sensor dari pemerintah terhadap aplikasi-aplikasi pesan instan biasa. Untuk menggunakan Bitcoin sebagai pengirim pesan dapat digunakan dompet Bitcoin khusus, atau layanan *online* seperti CryptoGraffiti (<http://cryptograffiti.info>), yang tidak memerlukan instalasi karena berbasis web. Setelah Anda sukses melakukan transaksi seperti yang diinstruksikan, CryptoGraffiti akan memajang pesan Anda dalam situsnya di cryptograffiti.info.



Gambar 73. CryptoGraffiti.

Anda juga bisa langsung meletakkan pesan di dalam sistem Bitcoin. Pesan tersebut akan muncul pada informasi detail transaksi seperti pada contoh yang dapat Anda akses di <http://s.id/7JW> atau <https://goo.gl/t20geX>.

Input Scripts

304502210041d7a4410ef14b5be18034dd998c182cc4074c59c1e0311dec70033a2f11402200ce9ae3a1ee4C5d099e4eac1acdd3ce3cd7b642276667e7e19bb43b67192408201
0336b5bcb26adb/Uoa58b32259e8c562749fC00e266e3baa180abe01c3228a5e1 OK

Output Scripts

OP_DUP OP_HASH160 52e57d3891885a835896c309e099e1e343616a0 OP_EQUALVERIFY OP_CHECKSIG OK
OP_RETURN 64636d517a20776173209665776521 Strange
(decoded: dimaz was here!)

Gambar 74. Memasukkan pesan dalam transaksi Bitcoin

Untuk membuat pesan seperti gambar di atas, Anda dapat menggunakan aplikasi gratis dari Setfive yang beralamat di <http://code.setfive.com/btcscript>. Aplikasi tersebut akan membuat alamat Bitcoin baru yang terlebih dahulu harus Anda isi dengan sejumlah bitcoin (tidak harus banyak, misalnya 50.000 satoshi agar bisa membuat beberapa pesan berantai). Untuk setiap transaksi akan dikenai biaya sekitar 1.000 satoshi. Biaya ini merupakan ongkos transaksi bitcoin dan Setfive tidak mengutip biaya apapun dalam penggunaan layanan ini, artinya dengan 50.000 satoshi Anda dapat mengirim 50 pesan pendek.

Get Keys

Private Key

Public Address

Send To Address

Import Key

Generate keys

Check Address

You'll need to make sure you a high enough balance to actually send anything (plus fees). Click "Refresh" below to grab the info for the keys above.

Refresh

Type	Balance	Received	Sent	Amount
Confirmed				
Total (Confirmed+Unconfirmed)				
Unspent (Click to use in TX)				

Gambar 75. Mengirim pesan dalam Bitcoin. Sumber: Setfive.com

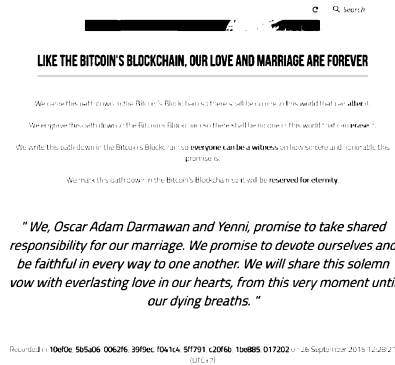
Apabila sukses, pesan tersebut akan terbaca di situs Coin Secrets (<http://coinsecrets.org>).

Transaction ID	Amount	Address
385578	0.00000000	1A1zP1eP5QGefi2DMPTfQN5YaZv39ASu
385578	0.00000000	1A1zP1eP5QGefi2DMPTfQN5YaZv39ASu
385578	0.00000000	1A1zP1eP5QGefi2DMPTfQN5YaZv39ASu
385577	0.00000000	1A1zP1eP5QGefi2DMPTfQN5YaZv39ASu
383077	0.00000000	1A1zP1eP5QGefi2DMPTfQN5YaZv39ASu

Gambar 76. Pesan yang dikirim melalui Bitcoin. Sumber: coinsecrets.org

Pembuktian Eksistensi Dokumen

Pesan yang tertera dalam sistem Bitcoin ini dapat digunakan untuk bermacam-macam fungsi, misalnya untuk menyimpan janji nikah seperti pada pernikahan CEO Bitcoin Indonesia, Oscar Darmawan, yang dapat Anda lihat di <http://bitcoinwedding.com>. Anda juga bisa memanfaatkan layanan dari Eternity Wall (<http://eternitywall.it>) yang dapat membantu Anda menyimpan pesan dalam blockchain dengan mudah. Layanan ini juga menggratiskan 1 pesan tiap jam.



Gambar 77. Janji Nikah disimpan dalam Bitcoin. Sumber: bitcoinwedding.com

Selain pesan instan, Bitcoin juga dapat dimanfaatkan untuk memberikan validasi atas eksistensi sebuah dokumen elektronik. Misalnya Anda menulis sebuah artikel pada tanggal 1 Desember 2015 dan mengirimkannya pada sebuah koran elektronik, namun ternyata pada tanggal 1 Januari 2016, artikel tersebut terbit atas nama orang lain. Untuk berjaga-jaga atas hal ini, Anda dapat membuat sebuah bukti bahwa Anda adalah pemilik artikel tersebut dengan menggunakan layanan yang dibangun memanfaatkan sistem Bitcoin. Contoh situs yang menyediakan layanan seperti ini adalah Proof of Existence (<https://proofofexistence.com>). Validasi atas dokumen elektronik tersebut akan disimpan dalam sistem Bitcoin dan siapapun bisa memeriksa informasi yang tersedia di dalamnya dan mencocokkannya dengan dokumen yang tervalidasi.

Bitcoin dapat juga digunakan dalam pengelolaan aset atau yang biasa disebut *colored coin*. Contoh layanan seperti ini disediakan oleh Coinprism (<https://coinprism.com>). Aset tersebut dibuatkan tanda bukti dan disimpan dalam sistem Bitcoin dan menjadi bukti kepemilikan aset Anda yang dibuat dalam bentuk transaksi Bitcoin.

Kontrak

Kontrak juga dapat dibuat dalam sistem Bitcoin. Contohnya ketika Anda menyewa rumah, pemilik rumah meminta Anda untuk membayar suatu jaminan uang sebesar 1 bulan nilai sewa di mana uang jaminan tersebut akan dikembalikan pada waktu yang telah ditentukan. Dalam kasus ini, Bitcoin dapat digunakan sebab dalam sistem Bitcoin dapat dibuat transaksi pengembalian pembayaran uang jaminan tersebut pada waktu tertentu di masa depan. Demikian juga untuk kebutuhan penyediaan jaminan, Bitcoin dapat digunakan untuk membuat sebuah kontrak yang menahan sejumlah uang dalam rentang waktu tertentu sebelum dikembalikan kepada pemiliknya.

E-voting

Bitcoin juga memungkinkan untuk digunakan dalam *e-voting* di masa depan. *E-voting* merupakan suatu teknik untuk menjalankan prinsip demokrasi pemilihan berdasarkan suara terbanyak yang didukung oleh teknologi informasi. Dengan menggunakan Bitcoin untuk *e-voting*, pemerintah tidak perlu membangun infrastruktur apapun untuk menjalankan sistem *e-voting*, sebab sistem Bitcoin sendiri telah ada dan berjalan dengan baik. Adanya perlindungan berbasis kriptografi dan terdesentralisasi, membuatnya lebih sulit bagi siapapun untuk mencurangi sistem demi mengubah hasil *e-voting*, sebab informasi tidak hanya disimpan dalam 1 atau 2 server saja, melainkan dalam seluruh *node* Bitcoin di seluruh dunia. Beberapa *startup* telah memulai riset untuk memanfaatkan Bitcoin dalam kegiatan *e-voting*, di antaranya BitCongress (<http://bitcongress.org>) dan LiquidFeedback (<http://liquidfeedback.com>) yang masih dalam tahap pengembangan. •



Foto: AP via voanews.com

“...There are other technologies, like blockchain, which is used for bitcoin, but can also be used for many other applications... and our banks must keep up to date with these developments.”

Perdana Menteri Singapura, Lee Hsien Loong November 2015

KONTROVERSI BITCOIN

SEBAGAI SEBUAH SISTEM YANG MASIH BERUSIA MUDA NAMUN MENDOBRAK NILAI-NILAI TRADISIONAL DALAM DUNIA FINANSIAL KHUSUSNYA SISTEM PEMBAYARAN, TIDAK DIPUNGKIRI TERDAPAT BEBERAPA KONTROVERSI SEPUTAR SISTEM BITCOIN INI, YANG MEMBUAT ORANG BERTANYA-TANYA ATAU BAHKAN BERDEBAT SATU SAMA LAIN. KITA AKAN MEMBAHAS BEBERAPA KONTROVERSI BITCOIN DI BAWAH INI.

Satoshi Nakamoto

Hingga kini, tidak ada yang tahu pasti siapa di balik akun Satoshi Nakamoto. Faktanya, Bitcoin diluncurkan tanpa adanya pertemuan fisik. Semua tahap pengembangan aplikasi dan pembicaraan antarsesama ahli kriptografi dilakukan melalui *mailing list* (milis). Milis adalah grup/kelompok yang terdiri atas banyak e-mail, dan ketika seseorang mengirimkan e-mail ke grup, maka semua orang dalam grup akan menerima email yang sama. Konsep milis dapat diibaratkan seperti grup *chatting* (pesan singkat).

Ada yang menyangka Bitcoin dikembangkan bersama-sama sebagai sebuah grup, CIA misalnya, namun ada juga yang memperkirakan beberapa ahli kriptografi dunia sebagai aktor di belakang nama Satoshi Nakamoto, seperti Nick Szabo dan Hal Finney (Wikipedia, 2015e). Ada pula yang menyangkutpautkan seseorang bernama Dorian Satoshi Nakamoto, warga negara Amerika Serikat keturunan Jepang yang tinggal di California. Na-

mun sampai sekarang tidak ada yang mengklaim dirinya sebagai Satoshi Nakamoto sang pencipta Bitcoin. Padahal, di dalam dompet Bitcoin miliknya terdapat 1 juta BTC yang bila dirupiahkan akan bernilai Rp 5 triliun (dengan asumsi 1 BTC = Rp 5 juta). Seluruh pengembangan sistem Bitcoin kini diserahkan pada Gavin Andresen dan timnya.

Ketiadaan Inflasi

Sistem Bitcoin tidak mengenal inflasi, bahkan nilainya terus meningkat dari tahun ke tahun. Hal ini sekilas terlihat bagus, namun para ahli keuangan menentang pendapat ini. Tanpa adanya inflasi, maka ekonomi akan melambat, karena semua orang memilih untuk tidak membelanjakan uangnya dan menunda sampai nilainya meningkat. Hal ini cukup berbeda bila dibandingkan dengan sistem keuangan tradisional di mana inflasi dalam batas tertentu akan membuat orang lebih memilih membelanjakan uangnya ke-timbang menunda belanja, sebab inflasi akan membuat nilai uang hari ini lebih tinggi dibandingkan nilai uang besok atau setahun kemudian. Tidak adanya inflasi membuat orang ragu-ragu dengan kemampuan Bitcoin menyaingi sistem keuangan tradisional seperti rupiah atau dolar AS.

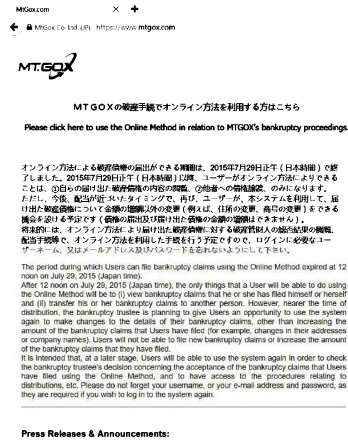
Deflasi, sebagai lawan kata inflasi, merupakan salah satu karakteristik Bitcoin dengan melakukan pembatasan jumlah total bitcoin yang dapat beredar yaitu sejumlah 21 juta bitcoin. Satu-satunya cara untuk mencetak bitcoin baru adalah melalui proses penambangan (*mining*). Bitcoin baru tersebut akan dihadiahkan pada penambang yang berhasil menciptakan sebuah blok baru yang dapat ditambahkan ke dalam *blockchain*.

Hadiah bitcoin baru tersebut berjumlah 50 BTC yang berlaku sejak tahun 2009, dan kebijakan pemotongan hadiah (*reward halving*) tersebut berlaku setiap sekitar 4 tahun sekali atau setiap 210.000 blok yang ditambang. Pada tanggal 28 November 2012, hadiah tersebut dipotong separuhnya, hingga berjumlah 25 BTC (Bitcoin Wiki, 2011a), karena jumlah blok telah mencapai lebih dari 210.000. Berdasarkan perkiraan, pemotongan hadiah bitcoin berikutnya akan terjadi antara tahun 2016 atau 2017 ketika jumlah blok telah mencapai 420.000 yang akan mengubah hadiah dari 25 BTC menjadi 12,5 BTC. Pemotongan tersebut akan terus terjadi hingga nanti tahun 2140 tidak akan ada lagi hadiah bitcoin yang diberikan pada penambang (Bitcoin Wiki, 2011a).

Mt. Gox

Mt. Gox dulu merupakan perusahaan perdagangan Bitcoin terbesar di dunia sebelum bangkrut. Mt. Gox di masa jayanya melayani 70% dari total transaksi Bitcoin di seluruh dunia. Perusahaan yang berbasis di Jepang ini pada akhirnya mengajukan kebangkrutan karena menyatakan diri telah “kecurian” sebanyak 850 ribu bitcoin yang saat ini bernilai Rp. 4,2 triliun (asumsi 1 BTC = Rp 5 juta) oleh *hacker*. Mark Karpeles, sebagai CEO Mt. Gox tidak mengetahui bagaimana serangan ini terjadi, dan menyalahkan sebuah kelemahan dalam sistem Bitcoin yang disebut *transaction malleability* (Franco, 2015). Kasus Mt. Gox merupakan contoh bagaimana aplikasi Bitcoin yang tidak memperhatikan

keamanan akan menyebabkan kerugian yang sangat besar. Kasus Mt. Gox juga menjadi pelajaran bahwa dompet panas bisa dicuri oleh hacker bila tidak diamankan dengan baik.



Gambar 78. Kebangkrutan yang dialami Mt. Gox

Silk Road

Di dunia Internet, selain dari situs-situs yang kita kenal selama ini, terdapat sebuah area yang tidak banyak diketahui keberadaannya, yang disebut *deep web* atau kadang-kadang juga disebut *dark web*, bisa diartikan sebagai situs yang berada di kedalaman atau kegelapan.

Andaikanlah selama ini Anda berselancar di permukaan lautan Internet, maka *deep web* berada ratusan meter di bawah permukaan laut yang tidak terindeks oleh mesin pencari biasa, bahkan oleh Google, sekalipun. Untuk mulai berselancar dalam *deep web*, pengguna cukup menggunakan peramban (*browser*) yang disebut dengan Tor untuk masuk ke dalam jaringan anonim (Dingledine, Mathewson, & Syverson, 2004).

Deep web digunakan untuk menyembunyikan privasi para penggunanya, yaitu pengunjung dan pemilik situs (Bartlett, 2014). Banyak layanan yang ada dalam *deep web* merupakan layanan ilegal dan melawan hukum. *Deep web* menjadi terkenal saat terjadi penangkapan atas pemilik Silk Road, sebuah toko *online* yang menjual berbagai jenis narkoba. Bitcoin disangkutpautkan dengan Silk Road, sebab transaksi jual beli banyak dilakukan menggunakan bitcoin. Cap buruk melekat pada Bitcoin, karena potensi penggunaannya dalam kegiatan-kegiatan ilegal. Padahal jika ditelisik lebih jauh, uang fisik sudah jauh terlebih dahulu dipakai dalam transaksi ilegal (Bartlett, 2014). Bitcoin di-

gunakan dalam *deep web* karena dianggap anonim dan identitas pengguna tidak dapat terlacak, padahal sebenarnya alur transaksi dalam sistem Bitcoin masih dapat dilacak, jauh lebih mudah ketimbang melacak alur transaksi uang fisik (Bartlett, 2014).

Inefisiensi Energi

Bitcoin dikenal memiliki sistem yang tidak ramah lingkungan, karena konsumsi energi yang sangat besar oleh instalasi pertambangan Bitcoin di seluruh dunia. Inefisiensi ini menyebabkan timbulnya banyak kritik dari berbagai pihak, salah satunya oleh Ben Laurie (Laurie, 2011) yang merupakan direktur Apache Software Foundation. Walau demikian, besarnya infrastruktur pertambangan Bitcoin diperlukan untuk menghindari serangan dari pihak-pihak yang tidak bertanggungjawab. Sebab, untuk melakukan perubahan data pada sistem Bitcoin, seseorang harus memiliki kekuatan komputasi yang sangat besar menandingi total semua kekuatan komputasi dalam sistem Bitcoin. Dengan besarnya kekuatan komputasi di dalam jaringan Bitcoin, maka dibutuhkan investasi yang sangat besar untuk menyerang sistem Bitcoin dan mengubah informasi di dalamnya.

Ukuran Blok

Ukuran blok Bitcoin menjadi topik perdebatan yang hingga kini tak kunjung usai. Sebagaimana telah dibahas, bahwa transaksi-transaksi Bitcoin yang telah dikonfirmasi akan dimasukkan ke dalam blok-blok sebagai bagian dari *blockchain*. Nah, dengan semakin popularnya Bitcoin, jumlah transaksi juga semakin meningkat hari demi hari. Sementara ukuran sebuah blok saat ini tidak boleh melebihi 1MB, oleh karena itu antrean transaksi yang harus dikonfirmasi juga semakin panjang. Hal ini memicu beberapa orang pengembang untuk menambah ukuran blok menjadi lebih besar (Bitcoin Wiki, 2015b). Namun demikian, usul ini mendapat penolakan dari beberapa pihak. Beberapa alasan penolakan tersebut adalah untuk menghindari lalu lintas jaringan komputer yang terlalu padat dan menghindari peningkatan ukuran *blockchain* yang terlalu signifikan, sehingga meningkatkan ongkos yang harus ditanggung oleh pihak-pihak yang menyediakan node Bitcoin maupun para penambang.

Meskipun masih menjadi perdebatan, pengembang Bitcoin, Gavin Andresen dan Mike Hearn mengembangkan versi lain dari Bitcoin *core* yang disebut dengan Bitcoin XT yang mengimplementasikan ukuran blok Bitcoin yang lebih besar dibandingkan standar ukuran blok seperti yang ditentukan pada Bitcoin *core* (Bitcoin Wiki, 2015a). Bitcoin XT ini mengimplementasikan peningkatan ukuran blok sebesar 8 MB dan akan diperbesar dua kali lipat setiap 2 tahun. Namun demikian, proposal yang diajukan oleh Bitcoin XT untuk memperbesar ukuran blok dianggap telah gagal, sebab mayoritas tidak menginginkan peningkatan blok ini. Persoalan yang tidak kunjung usai ini akhirnya menyebabkan Mike Hearn mengundurkan diri dari posisinya sebagai *core developer* Bitcoin (Bitcoin Wiki, 2015a).

Jumlah Node Semakin Berkurang

Node Bitcoin merupakan salah satu komponen penting dalam sistem Bitcoin selain penambangan (Cawrey, 2014). *Node* Bitcoin adalah komputer yang menjalankan aplikasi Bitcoin *core* dan dengan demikian memelihara salinan lengkap seluruh transaksi Bitcoin di seluruh dunia yang disimpan dalam basis data yang disebut *blockchain* (Bitcoin Wiki, 2014a). *Node* Bitcoin inilah yang membuat sistem Bitcoin tidak memerlukan pengendali sentral seperti pada uang tradisional pada umumnya, sebab semakin banyak *node*, maka akan semakin sulit bagi orang untuk memanipulasi transaksi yang sudah terekam dalam *blockchain*. Meskipun memegang peranan penting dalam sistem Bitcoin, jumlah *node* Bitcoin semakin berkurang dengan sangat drastis (Yeow, 2016). Hal ini disebabkan karena tidak adanya insentif atau bayaran atas jasa-jasa mereka yang menyediakan *node* Bitcoin, berbanding terbalik dengan penambang Bitcoin yang mendapatkan keuntungan atas setiap blok yang dihasilkan. Permasalahan ini coba dipecahkan dengan mengusulkan beberapa skema, di antaranya pemberian insentif atau balas jasa atas fasilitas yang disediakan oleh *node* Bitcoin (Zsales et al., 2015). •

ALTCOIN

MESKIPUN BITCOIN MERUPAKAN PIONIR DALAM DUNIA CRYPTOCURRENCY, BITCOIN BUKANLAH SATU-SATUNYA UANG DIGITAL YANG BERBASIS KRIPTOGRAFI. SEJAK KESUKSESAN BITCOIN, ORANG-ORANG MULAI MELAKUKAN IMPROVISASI DAN MEMBUAT CRYPTOCURRENCY VERSI MEREKA SENDIRI.

Cryptocurrency yang muncul setelah Bitcoin, biasa disebut AltCoin, atau *alternative coin* (Franco, 2015). Beberapa AltCoin mulai dikenal sebagai alternatif Bitcoin karena karakteristik khusus, konsep yang berbeda, dan harganya yang masih rendah. Beberapa AltCoin akan dibahas di sini di antaranya Ripple, Litecoin, Dogecoin, Peercoin, dan Ethereum. Meskipun masih banyak AltCoin yang tersedia di pasaran, beberapa AltCoin yang disebutkan tadi memiliki pangsa pasar dan potensi pengaruh yang besar dibandingkan yang lainnya.

AltCoin, seperti halnya Bitcoin, memiliki beberapa karakteristik yang sama dengan Bitcoin. Mereka memiliki infrastruktur yang sama, yakni penambang, layanan pertukaran uang, dan konsumen pengguna. Namun masing-masing memiliki perbedaan satu dengan yang lainnya dan menerapkan teknologi yang berbeda.

Ripple

Ripple (XRP) memiliki pangsa pasar kedua terbesar setelah Bitcoin. Saat ini, Ripple memiliki investor besar seperti Seagate, Bank Santander (Spanyol), dan Bank Fidor (Jerman). Ripple diciptakan pertama kali oleh Ryan Fugger untuk

mendukung transaksi perbankan melalui Internet (Wikipedia, 2015d). Ripple digunakan utamanya untuk keperluan RTGS (*real time gross settlement*), karena kecepatan transaksinya, yaitu sekitar 3 sampai 5 detik hingga terverifikasi dalam sistem.

Saat ini Ripple berfokus untuk melayani transaksi internasional yang melibatkan mata uang yang berbeda. Untuk layanan itu, Ripple mengombinasikan teknologi terdesentralisasi dengan layanan perbankan. Ripple menggunakan konsep yang berbeda dengan Bitcoin dalam hal mengamankan transaksi yang dilakukan di dalam sistem. Ripple memilih untuk menggunakan metode konsensus dibandingkan dengan Bitcoin yang menggunakan komputasi matematis. Sebagai akibatnya, Ripple memiliki tingkat efisiensi yang lebih tinggi. Namun sayangnya dalam sistem Ripple, kita tidak bisa ikut menambang untuk mendapatkan koin, sebab semua koin telah ditambang oleh pengelola Ripple, sehingga pengguna hanya bisa membeli Ripplecoin.

Untuk menggunakan Ripple, pengguna harus mendaftar melalui *gateway*. *Gateway* merupakan penghubung antara pihak perbankan dengan sistem Ripple. Terdapat beberapa *gateway* yang dapat digunakan, salah satunya adalah Ripple Singapore yang beralamat di alamat website <https://www.ripplesingapore.com>. Untuk mulai mendaftar di Ripple Singapore sebagai *gateway* Ripple Anda, Anda dapat mengunjungi alamat <https://www.ripplesingapore.com/Account/Register>.

The image shows the registration page of Ripple Singapore. At the top, there's a header with the Ripple logo and the tagline "Gold & Silver in your wallet". Below the header, there's a navigation bar with links: Home, Our Services, Get started, About us, and F.A.Q. The main content area has a heading "Register" and a subtext "Create a new account." Below this, there are input fields for Firstname, Middlename, Lastname, E-mail address, Password, and Confirm password. At the bottom, there's a "Register" button. On the right side, there's a "Live transaction feed" showing "0.33 BTC" and a "Wallet" section.

Gambar 79. Ripple Singapore

Setelah melakukan pendaftaran dan verifikasi alamat email, Anda dapat mulai login dalam sistem Ripple.

Settings

Security
Verification
Activity Log
Support

Account details

Firstname *
Middlename
Lastname *
Date of birth * Date of birth *
MM DD YYYY

Mobile phone number *
Address 1 *
Address 2 (optional)
City *

Government ID number *
Zip code *
State
Country *
Select country

* These extra fields are required

Bank details

Ripple name/address *
IBAN/Bank account
Bank code *
Branch code *

Silver/Billion Account Number *
Bank BIC/SWIFT
San code/PSORouting Code/ABA number *

Your Unique Account Identifier id *
12092

Bank name
Bank country
Select country

Bank address & number
Bank city

Bank building & unit number
Bank zip code

Gambar 80. Melengkapi Data Akun Ripple Singapore

Karena Ripple sangat terhubung dengan sistem perbankan, maka untuk membuat akun yang valid, semua informasi yang tertera pada akun tersebut harus divalidasi menggunakan kartu identitas yang resmi.

rippleSingapore
Gold & Silver in your wallet

Live transaction feed
1,543,183 XRP (worth \$0.09 USD)
wallet

Home Our Services Get started Deposit Withdrawal Buy/Sell Counter

Account Verification

Please enter your personal data in settings
Enter your personal data on the settings page first to be able to verify your account.
GO TO SETTINGS

To verify your account please submit (300dpi scan)
Government issued ID, such as: passport, national ID card or driver's license.
Proof of residency (max. 3 months old), such as: bank statement, rent contract, utility bill.

More details about Government issued ID & Proof of residency

After you are verified you can also verify yourself with SATS. To do this click the button below:
GO TO VERIFICATION

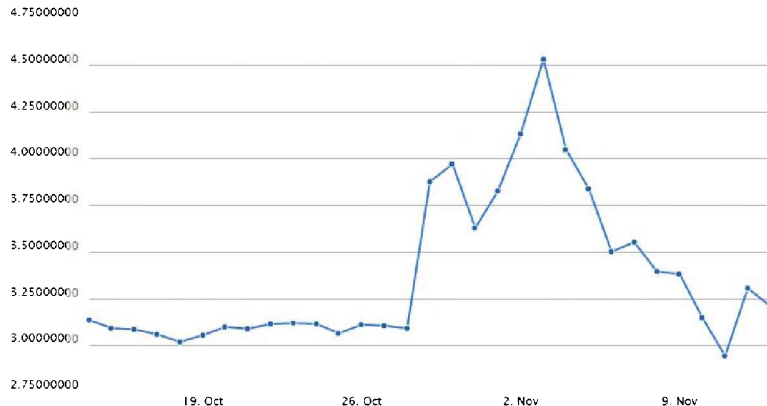
Gambar 81. Verifikasi Akun Ripple

Setelah melakukan pendaftaran dan verifikasi, maka transaksi internasional melalui Ripple dapat mulai dilakukan.

Litecoin

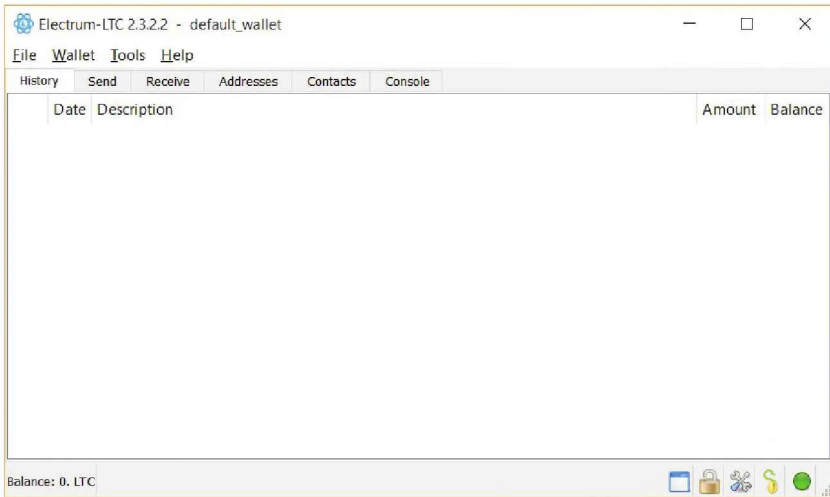
Litecoin (LTC) merupakan salah satu *cryptocurrency* yang dikembangkan dari Bitcoin. Litecoin diciptakan oleh Charles Lee, mantan pegawai Google (Wikipedia, 2015c). Pengembangan itu termasuk dengan peningkatan kecepatan transaksi, yaitu setiap 2,5 menit, jumlah koin, dan beberapa hal teknis lainnya. Oleh karena itu, dibandingkan dengan Bitcoin, Litecoin memiliki tingkat kecepatan yang 4 kali lebih tinggi, karena hanya membutuhkan 2,5 menit untuk verifikasi transaksi dibandingkan dengan sistem Bitcoin saat ini. Litecoin juga merupakan *cryptocurrency* yang terbesar ketiga setelah Bitcoin dalam hal total nilai pasar. Tidak seperti Ripple, Litecoin dapat ditambang sebagaimana halnya dengan Bitcoin. Meski demikian, penambangan Litecoin memiliki mekanisme yang berbeda dibandingkan dengan penambangan Bitcoin, oleh karena itu membutuhkan perangkat yang berbeda pula. Dahulu, Litecoin hanya bisa ditambang menggunakan kartu grafis (*graphic card*) berspesifikasi tinggi yang harganya jutaan rupiah, namun belakangan telah muncul mesin-mesin ASIC yang harganya lebih terjangkau.

Litecoin (LTC/USD) 30 Days Price Chart



Gambar 82. Pergerakan Harga Litecoin

Untuk memulai petualangan dalam sistem Litecoin, pertama-tama yang dibutuhkan adalah dompet Litecoin. Electrum memiliki versi Litecoin yang dapat diunduh melalui alamat <http://electrum-ltc.com>. Terdapat beberapa versi sistem operasi yang dapat digunakan, di antaranya Windows, Linux, dan OSX.



Gambar 83. Electrum LTC

Litecoin dapat diperoleh dengan membelinya dari bursa *cryptocurrency*, yang biasanya selain memperdagangkan Bitcoin juga menjual Litecoin, di antaranya Bitcoin Indonesia yang menyediakan Litecoin. Namun sayangnya, penggunaan Litecoin masih sangat terbatas pada jual beli di bursa *cryptocurrency* dan sangat jarang toko yang menerima Litecoin sebagai alat pembayaran. Perdagangan Litecoin yang dilakukan di Bitcoin Indonesia pun juga terbatas pada pertukaran LTC dengan BTC atau sebaliknya, artinya tidak bisa membeli LTC langsung dari rupiah melainkan harus ditukar dahulu dengan BTC baru kemudian dikonversi ke dalam LTC. LTC juga tidak dapat dibeli dengan harga market secara langsung seperti halnya transaksi BTC, namun harus masuk pada fitur jual beli di bursa.

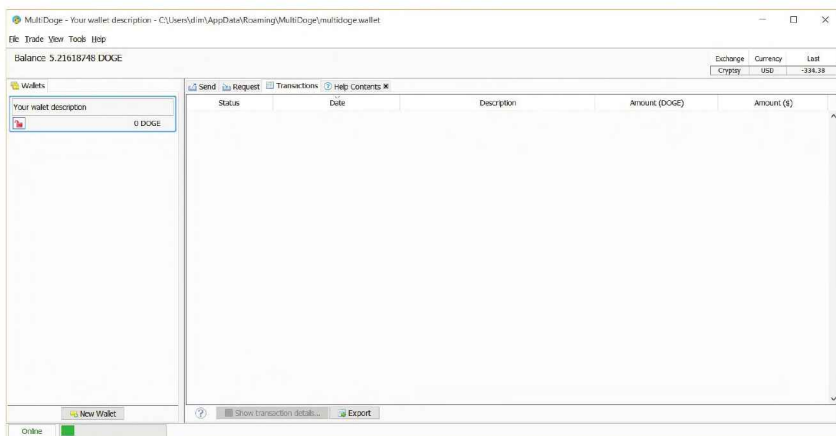
Dogecoin

Tidak semua *cryptocurrency* dibangun atas dasar keseriusan. Buktinya adalah munculnya Dogecoin (DOGE) yang semula ditujukan untuk lelucon, kini menempati peringkat keempat dari daftar *cryptocurrency* yang memiliki kapitalisasi pasar terbesar. *Cryptocurrency* ini unik sebab logonya berupa *meme* (gambar lelucon) anjing ras khas Jepang yang menggemaskan, Shiba Inu (Wikipedia, 2015a). Dogecoin kini banyak digunakan untuk pengumpulan bantuan untuk kegiatan-kegiatan sosial. Untuk membedakan dengan alamat Bitcoin, alamat Dogecoin dimulai dengan huruf D.



Gambar 84. Logo Dogecoin. Sumber: Wikipedia

Untuk menggunakan Dogecoin, yang dibutuhkan adalah sebuah dompet Dogecoin. Dompet Dogecoin dapat diunduh dari <http://dogecoin.com>. Tentu saja untuk versi Android dapat diunduh dari Google Play, dan versi iOS melalui App Store. Selain versi *desktop* dan *smartphone*, Dogecoin juga memiliki dompet versi *online* yang bisa jadi pilihan ketika Anda menginginkan kepraktisan.



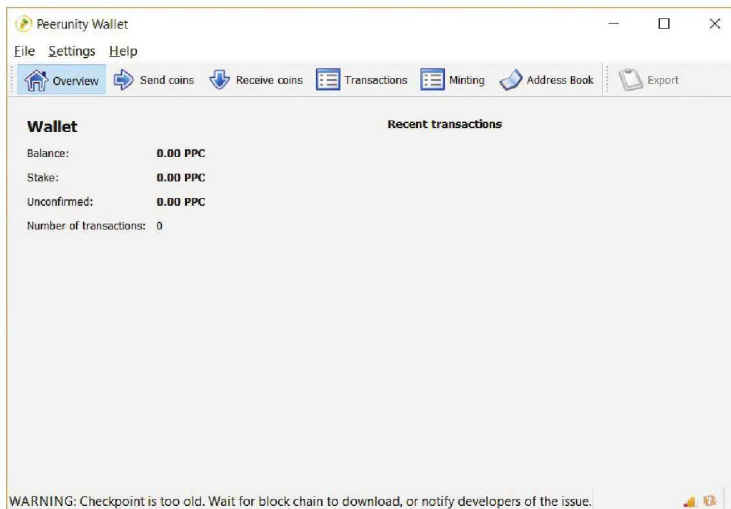
Gambar 85. Multidoge, Dompet Dogecoin versi desktop

Untuk mendapatkan dogecoin pertama Anda, ada baiknya Anda coba dahulu dogecoin faucet yang tersedia. Anda dapat mencoba <http://indogewetrust.com> dan [88](http://doge-</p>
</div>
<div data-bbox=)

faucet.com. Dogecoin harganya tidak setinggi Bitcoin dan sekarang ini masih dalam tahap pengembangan dari sisi teknis maupun komunitas, sehingga banyak orang yang mendonasikan dogecoin supaya lebih banyak orang terlibat dalam sistem ini. Mereka juga membuat sebuah game menarik bertema pertambangan Dogecoin yang bisa Anda coba di <http://dogeminer.se>. Dogecoin dikembangkan berdasarkan arsitektur Litecoin, dan karenanya dapat ditambang menggunakan perangkat yang sama dengan perangkat penambangan Litecoin. Bahkan beberapa *mining pool* seperti GHASH.IO (<http://ghash.io>) menambang Dogecoin dan Litecoin dalam waktu yang bersamaan sehingga pengguna memperoleh keuntungan ganda.

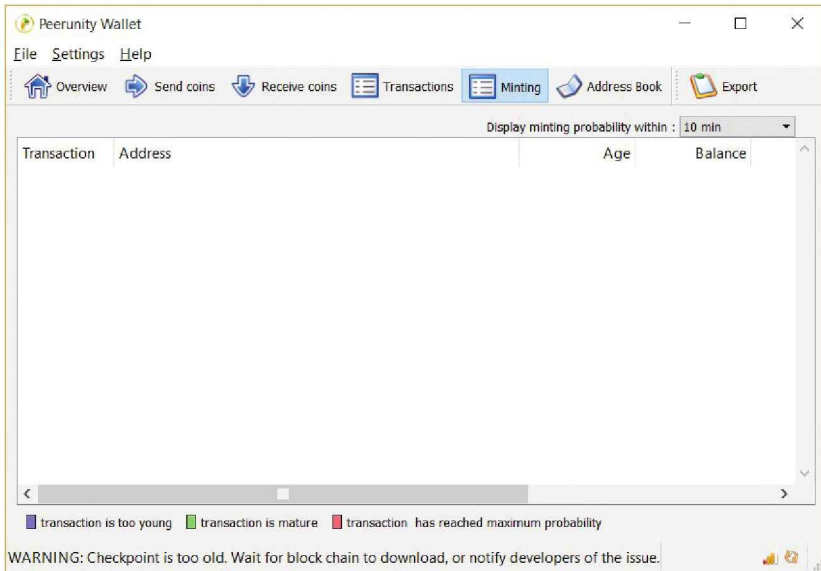
Peercoin

Urutan berikutnya setelah Dogecoin, dengan kapitalisasi pasar kelima terbesar di dunia *cryptocurrency*, adalah Peercoin yang didesain oleh seorang pengembang *software* bernama Sunny King (King & Nadal, 2012). Peercoin dikembangkan dari kode Bitcoin dengan penambahan beberapa konsep baru seperti inflasi yang tidak dikenal di dunia Bitcoin (Wikipedia, 2014). Peercoin dapat ditambang sebagaimana halnya dengan Bitcoin. Pilihan dompet Peercoin dapat dilihat melalui situs resmi mereka di <https://www.peercoin.net/wallet>. Salah satu pilihan dompet Peercoin yang tersedia adalah Peerunity, dompet berbasis *desktop* yang mendukung beberapa sistem operasi seperti Windows, Linux, dan OSX.



Gambar 86. Peerunity, Dompet Peercoin

Salah satu perbedaan yang terdapat pada Peercoin bila dibandingkan dengan Bitcoin adalah adanya konsep *minting*. *Minting* akan memberi hadiah pada pengguna Peercoin sesuai dengan jumlah peercoin dan umur peercoin yang dimilikinya dalam dompet Peercoin. Umur peercoin merupakan istilah yang menunjukkan berapa hari sejak *peercoin* tersebut diterima di dalam alamat Peercoin. Semakin lama umur peercoin yang dimiliki, maka semakin besar peluang seseorang untuk mendapatkan hadiah tersebut (dengan jumlah sekitar 1% dari total peercoin yang dimiliki).



Gambar 87. Informasi tentang minting peercoin yang dimiliki dalam dompet Peercoin

Meskipun terdapat proses *minting*, dalam Peercoin tetap mengenal adanya *mining* atau penambangan Peercoin. *Minting* dikenalkan untuk mengurangi dampak pemborosan energi seperti yang terjadi pada penambangan Bitcoin.

Ethereum

Ethereum (<https://ethereum.org>) merupakan AltCoin yang memiliki konsep yang berbeda jika dibandingkan dengan AltCoin-AltCoin yang lain. Koin pada Ethereum disebut ether. Ide pembuatan Ethereum pertama kali dipaparkan oleh Vitalik Buterin (Wikipedia, 2015b) untuk menyediakan fitur *smart contract* dalam lingkungan *cryptocurrency* (Wood, 2015). *Smart contract* adalah tipe kontrak yang memiliki klausul aktivasi di dalamnya. Ethereum dibangun dengan tujuan agar siapapun dapat membangun aplikasi desentralisasi (*decentralized application* atau DAPP) di atasnya, termasuk di antaranya membuat *cryptocurrency* sendiri.

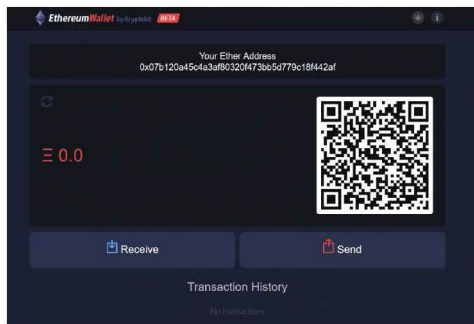
Contoh-contoh aplikasi yang dibangun di atas Ethereum dapat dilihat di situs State of the Dapps (<http://dapps.ethercasts.com/>), di mana kita bisa menemukan aplikasi asuransi penerbangan, *voting*, berbagai jenis *cryptocurrency* baru, *chatting*, sampai *social network* juga ada.

Seperti halnya *cryptocurrency* yang lain, untuk memulai penggunaan Ethereum, Anda memerlukan sebuah aplikasi dompet. Salah satu aplikasi dompet Ethereum yang disebut Mist, memiliki GUI atau antarmuka yang mudah digunakan oleh orang awam. Mist dapat diunduh melalui alamat <https://github.com/ethereum/mist/releases/>. Anda dapat juga menggunakan dompet berbasis Javascript yang disediakan oleh Ethereum Wallet yang dapat diakses melalui peramban di alamat <https://ethereumwallet.com>.



Gambar 88. Dompet Online Ethereum

Ethereumwallet tidak memerlukan instalasi maupun registrasi. Password juga tidak diperlukan karena akan dipilihkan secara random sesuai gerakan *mouse* pada saat pembuatan dompet pertama kali.



Gambar 89. Ethereumwallet

Hal penting yang perlu diperhatikan saat menggunakan *ethereum wallet* adalah Anda tidak boleh lupa mem-*bookmark* URL dompet Anda agar Anda tidak kehilangan kontrol atas isi dompet tersebut.

Dalam Ethereum juga dikenal istilah penambangan (*mining*) yang dilakukan dengan menggunakan CPU dan GPU (*Graphic Processing Unit* atau kartu grafis). Penambangan tersebut dapat dilakukan dengan menggunakan aplikasi Geth yang tersedia dalam situs Ethereum.

Seperti halnya dalam Bitcoin, Ethereum juga memiliki pecahan nilai yang lebih kecil dari Eth. Terdapat beberapa pecahan nilai setara 1 ETH yang dapat dilihat dalam tabel berikut (sumber : <http://ether.fund/tool/converter>).

1.000.000.000.000.000.000	wei
1.000.000.000.000.000	Kwei
1.000.000.000.000	Mwei
1.000.000.000	Gwei
1.000.000	szabo
1.000	finney
1	ether

Terdapat pula istilah Gas yang memiliki nilai setara dengan 10 szabo. Gas merupakan satuan yang digunakan dalam menentukan biaya transaksi sesuai dengan tingkat kerumitan skrip yang dipakai. Untuk transaksi standar, biayanya adalah 1 Gas. Biaya transaksi ini akan dikutip oleh para penambang Ether bersamaan dengan upah penambangan setidaknya sebesar 5 ether.

Berspekulasi Dengan AltCoin

Dalam sejarahnya, AltCoin banyak bermunculan namun banyak pula yang tenggelam, tergantung pada bagaimana komunitas *cryptocurrency* merespons keberadaan AltCoin tersebut. Banyak orang tertarik menjadi investor AltCoin-AltCoin baru, karena peluang mencetak keuntungan besar, saat harga AltCoin tersebut melambung tinggi di kemudian hari. Namun faktanya, banyak AltCoin tersebut dibangun dengan sembarangan. Teknologi yang ditanamkan dalam AltCoin tersebut seringkali tidak mampu bertahan dari serangan *hacker*, sehingga para pengguna terancam kehilangan koin yang mereka miliki.

Cryptocurrency merupakan sebuah bidang yang sangat mengandalkan kepercayaan. Begitu kepercayaan itu hilang, maka orang berbondong-bondong menjual AltCoin mereka dan harga pun akan turun drastis sesuai dengan mekanisme pasar. Saat harga mendekati nol, maka kebanyakan AltCoin ini akan ditinggalkan begitu saja oleh si pembuatnya yang barangkali telah menghasilkan cukup uang untuknya sendiri.

Berspekulasi pada AltCoin baru dengan membelinya pada saat harga masih rendah merupakan hal yang sangat berisiko tinggi, meskipun ada pula peluangnya untuk mencetak keuntungan besar jika Altcoin tersebut sukses di pasaran. Sebab sama seperti Bitcoin, AltCoin juga tidak memiliki aset yang dapat dijual untuk menutup kerugian saat harga jatuh.

Cross Chain Trading

Cross chain trading merupakan konsep berdagang lintas *cryptocurrency*. Konsep *cross chain trading* muncul, karena faktanya setiap *cryptocurrency* memiliki fluktuasi harga naik turun yang tidak terkait satu sama lain. Sebagai contoh misalnya antara Bitcoin dan Litecoin. Ketika harga Bitcoin turun, belum tentu harga Litecoin turun, atau bahkan pada saat yang sama harga Litecoin naik. Nah, di saat inilah *trader cross chain trading* menjual Litecoin dan membeli Bitcoin. Di saat harga Bitcoin meningkat dan harga Litecoin turun, maka *trader* menjual Bitcoin dan membeli Litecoin.

Dengan menggunakan 2 atau lebih *cryptocurrency*, maka kemungkinan mendapatkan profit akan lebih besar atau bahkan mendapatkan keuntungan ganda, meskipun risiko akan kehilangan uang juga tidak kecil, apabila terjadi kesalahan perhitungan atau perkiraan. *Cross chain trading* sendiri dapat dilakukan melalui perantara *cryptocurrency exchanger* seperti Bitcoin Indonesia (<https://bitcoin.co.id>). Sementara itu terdapat juga mekanisme jual beli *antarcryptocurrency* tanpa melalui *exchanger* yang disebut dengan istilah *cross chain transfer*.

Cross chain transfer merupakan teknik tukar menukar antar *cryptocurrency* (termasuk AltCoin dan Bitcoin) menggunakan mekanisme kontrak dan kunci rahasia (Tiernan, 2013). Contoh *cryptocurrency* yang mendukung teknologi *cross chain transfer* adalah Burst (<http://burstcoin.info/>) dan Qora (<http://www.qora.org/>). Dengan menggunakan Burst atau Qora, pengguna dapat melakukan aktivitas jual beli antara Burst, Qora, dan Bitcoin langsung antarpengguna secara aman. •

PERKEMBANGAN TERKINI

PENGUNAAN BITCOIN DAN CRYPTOCURRENCY TERUS BERKEMBANG DARI WAKTU KE WAKTU. BERAGAM PELUANG AKAN POTENSI KEUNTUNGAN BESAR YANG DAPAT DIRAIH DALAM KEGIATAN MINING.

Sebuah perusahaan yang berbasis di Melbourne Australia bernama Bitcoin Group (<http://www.bitcoingroup.com.au>) berencana untuk masuk ke bursa efek Australia (Australia Stock Exchange atau ASX). Bitcoin Group mengklaim diri menguasai 1% kekuatan komputasi di jaringan Bitcoin. Mereka membangun fasilitas penambangan Bitcoin di Tiongkok dan Islandia.

Masuk Bursa Saham

Dana yang diperoleh dari penjualan saham Bitcoin Group akan digunakan untuk berinvestasi pada mesin-mesin ASIC baru yang tentunya mereka berharap akan adanya peningkatan profit dari hasil investasi tersebut. Hal ini menandakan bahwa proses *mining* dengan modal besar dapat menghasilkan keuntungan yang cukup menggiurkan. Perusahaan ini juga rutin mengadakan acara kampanye sosialisasi Bitcoin setiap hari Rabu malam bertajuk “Talk and Trade Bitcoin”.

Perbankan

Barclays Bank yang merupakan salah satu bank besar di Inggris mulai melirik Bitcoin untuk mengumpulkan donasi (Macfarlan, 2015), karena melihat keuntungan yang dapat diperoleh dari transaksi berbasis Bitcoin yang tidak memerlukan infrastruktur yang mahal. Lebih lanjut lagi, 11 bank besar seperti HSBC, UBS, dan Commonwealth Bank Australia bergabung dalam perusahaan R3 dalam sebuah konsorsium yang terdiri atas 43 perusahaan mengembangkan sistem berbasis teknologi *blockchain* untuk menghemat biaya transaksi yang selama ini dibebankan kepada pengguna saat mengirim dan menerima uang pada sistem perbankan tradisional (Kelly, 2016). R3 sendiri merupakan perusahaan yang berfokus pada pengembangan *blockchain* untuk penggunaan yang lebih luas pada sistem perbankan.

Startup

Sementara itu, *startup* berbasis Bitcoin juga semakin berkembang, salah satunya Coinbase yang merupakan salah satu perusahaan besar dalam dunia Bitcoin, berekspansi di Asia Tenggara dengan membuka cabang di Singapura (Cosseboom, 2015). Demikian pula dengan CoinJar, perusahaan berbasis Australia yang melayani jual beli Bitcoin, mulai merambah Eropa dengan memasuki pasar Inggris (Swan, 2014). Hal ini menunjukkan bahwa penggunaan Bitcoin semakin meluas di seluruh dunia dan bukan tidak mungkin Bitcoin dan teknologi *blockchain* menjadi teknologi yang mengubah wajah perbankan di masa depan sebagaimana disampaikan oleh Coffrini (2015).

Blockchain-as-a-service

Perusahaan teknologi raksasa Microsoft mulai memperkenalkan *blockchain-as-a-service* pada layanan *cloud* mereka, Microsoft Azure. Layanan ini dapat digunakan bagi pengembangan yang tidak memiliki infrastruktur *blockchain* sendiri untuk menyewa infrastruktur milik Microsoft dalam mengembangkan teknologi *blockchain*. Hal ini menunjukkan teknologi *blockchain* menjadi salah satu teknologi utama di masa depan. *Blockchain* dianggap mampu menjadi solusi atas berbagai permasalahan, di antaranya transparansi transaksi dan keamanan sistem. •

REFERENSI

- Alstyne, M. V. (2014). Why Bitcoin has value. *Commun. ACM*, 57(5), 30-32.
doi:10.1145/2594288
- Andresen, G. (2011). M-of-N Standard Transactions. Retrieved from <https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki>
- Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*: "O'Reilly Media, Inc."
- Back, A. (2002). Hashcash-a denial of service counter-measure.
- Bangsaid. (2015). Pilih Kartu Uang Elektronik yang Mana? Flazz, e-Money, atau JakCard? Retrieved from <http://bangsaid.com/2015/10/pilih-kartu-uang-elektronik-yang-mana-flazz-e-money-atau-jakcard.html>
- Bartlett, J. (2014). *The Dark Net*: The Random House.
- Bitcoin Wiki. (2011a, 16 January 2016). Controlled supply. Retrieved from https://en.bitcoin.it/wiki/Controlled_supply
- Bitcoin Wiki. (2011b, August 17, 2015). Technical background of version 1 Bitcoin addresses. Retrieved from https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses
- Bitcoin Wiki. (2011c, 11 December 2015). Transaction fees. Retrieved from https://en.bitcoin.it/wiki/Transaction_fees
- Bitcoin Wiki. (2012, July 8, 2015). Contract. Retrieved from <https://en.bitcoin.it/wiki/Contract>
- Bitcoin Wiki. (2013a). Elliptic Curve Digital Signature Algorithm. Retrieved from https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
- Bitcoin Wiki. (2013b, September 25, 2015). Script. Retrieved from <https://en.bitcoin.it/wiki/Script>
- Bitcoin Wiki. (2013c, 28 May 2015). Transaction. Retrieved from <https://en.bitcoin.it/wiki/Transaction>
- Bitcoin Wiki. (2014a, 30 December 2015). Full node. Retrieved from https://en.bitcoin.it/wiki/Full_node

- Bitcoin Wiki. (2014b, June 30, 2014). RIPEMD-160. Retrieved from <https://en.bitcoin.it/wiki/RIPEMD-160>
- Bitcoin Wiki. (2015a, 26 January 2016). Bitcoin XT. Retrieved from https://en.bitcoin.it/wiki/Bitcoin_XT
- Bitcoin Wiki. (2015b, 20 January 2016). Block size limit controversy. Retrieved from https://en.bitcoin.it/wiki/Block_size_limit_controversy
- Brown, D. R. (2010). Recommended Elliptic Curve Domain Parameters. *Certicom Corp.*
- Cawrey, D. (2014). What Are Bitcoin Nodes and Why Do We Need Them? Retrieved from <http://www.coindesk.com/bitcoin-nodes-need/>
- Coffrini, F. (2015). Bitcoin's 'blockchain' tech may transform banking. Retrieved from <http://www.dailymail.co.uk/wires/afp/article-3366709/Bit-coins-blockchain-tech-transform-banking.html>
- Cosseboom, L. (2015, 3 September 2015). Top bitcoin company Coinbase launches in Singapore. *Techinasia*. Retrieved from <https://www.techinasia.com/singapore-bitcoin-coinbase-cryptocurrency-news>
- Dai, W. (1998). B-money. Retrieved from <http://www.weidai.com/bmoney.txt>
- Darmawan, O. (2014). *Bitcoin Mata Uang Digital Dunia*: Jakom.
- Diffie, W., & Hellman, M. E. (1976). *Multiuser cryptographic techniques*. Paper presented at the Proceedings of the June 7-10, 1976, national computer conference and exposition.
- Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*. Retrieved from
- ElGamal, T. (1985). *A public key cryptosystem and a signature scheme based on discrete logarithms*. Paper presented at the Advances in cryptology.
- Franco, P. (2015). *Understanding Bitcoin: Cryptography, engineering, and economics*.: John Wiley & Sons Ltd.
- Harding, D. A. (2015). Bitcoin Developer Guide. Retrieved from <https://bitcoin.org/en/developer-guide>
- Kelly, J. (2016, 21 January 2016). Eleven big banks test blockchain-based trading system. *Daily Mail*. Retrieved from <http://www.dailymail.co.uk/wires/reuters/article-3408332/Eleven-big-banks-test-blockchain-based-trading-system.html>
- King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake.

- Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(177), 203-209.
- Laurie, B. (2011). Decentralised currencies are probably impossible (but let's at least make them efficient). *Practice*, 1-10.
- Macfarlan, T. (2015). Barclays set to become first UK high street bank to accept bitcoin as it starts taking charity donations in the virtual currency. Retrieved from <http://www.dailymail.co.uk/news/article-3216246/Barclays-UK-high-street-bank-accept-bitcoin.html>
- Mankiw, N. G. (2014). *Principles of macroeconomics*: Cengage Learning.
- Miller, V. S. (1985). *Use of elliptic curves in cryptography*. Paper presented at the Advances in Cryptology—CRYPTO'85 Proceedings.
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from <http://bitcoin.org/bitcoin.pdf>
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.
- Swan, D. (2014). Aussie Bitcoin start-up CoinJar moves to the UK. Retrieved from [http://www.theaustralian.com.au/business/latest/aussie-bitcoin-start-up-coinjar-moves-to-the-uk/news-story/2444c29cc30717a6ad1557e444071401?=-](http://www.theaustralian.com.au/business/latest/aussie-bitcoin-start-up-coinjar-moves-to-the-uk/news-story/2444c29cc30717a6ad1557e444071401?)
- Tesauro, M. (2015). Cryptography in Practice. Retrieved from https://github.com/mtesauro/ut-cs-361/blob/master/2015-fall/lectures/Lect-05_Cryptography-in-Practice.md
- Tiernan, N. (2013, May 7, 2013). Alt Chains and Atomic Transfers. Retrieved from <https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949>
- Wikipedia. (2014, 29 October 2015). Peercoin. Retrieved from <https://en.wikipedia.org/wiki/Peercoin>
- Wikipedia. (2015a, 13 January 2016). Dogecoin. Retrieved from <https://en.wikipedia.org/wiki/Dogecoin>
- Wikipedia. (2015b). Ethereum. Retrieved from <https://en.wikipedia.org/wiki/Ethereum>
- Wikipedia. (2015c, 16 January 2016). Litecoin. Retrieved from <https://en.wikipedia.org/wiki/Litecoin>
- Wikipedia. (2015d, 27 October 2015). Ripple (payment protocol). Retrieved from [https://en.wikipedia.org/wiki/Ripple_\(payment_protocol\)](https://en.wikipedia.org/wiki/Ripple_(payment_protocol))

- Wikipedia. (2015e, 19 January 2016). Satoshi Nakamoto. Retrieved from https://en.wikipedia.org/wiki/Satoshi_Nakamoto
- Wikipedia. (2015f). SHA-2. Retrieved from <https://en.wikipedia.org/wiki/SHA-2>
- Wood, G. (2014). Less-techy: What is Web 3.0? Retrieved from <http://gavwood.com/web3lt.html>
- Wood, G. (2015). ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. Retrieved from <http://gavwood.com/Paper.pdf>
- Yeow, A. (2016). Bitnodes. Retrieved from <https://bitnodes.21.co/>
- Zsales, A., Ames, D., Georgem, Chaositech, WoodenBush, & Coins101. (2015). Proof of Bitcoin Node. Retrieved from <http://spreadcoin.info/news/wp-content/uploads/2015/10/Proof-of-Bitcoin-Node-DRAFTv1-1.pdf>



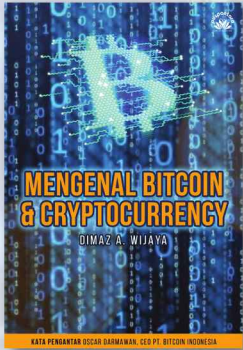
TENTANG PENULIS

DIMAZ ANKAA WIJAYA

Penulis menyelesaikan pendidikan Sarjana Komputer di Universitas Gadjah mada pada tahun 2007, kemudian memulai karir sebagai pengembang perangkat lunak. Dimaz lalu melanjutkan studi melalui beasiswa LPDP dalam program Master of Networks and Security di Monash University dan kini sedang melakukan penelitian tentang Bitcoin dan *cryptocurrency*. Dimaz dapat dihubungi melalui e-mail: dimaz@kriptologi.com.



PUSPANTARA.ORG



Bitcoin merupakan terobosan baru penggunaan kriptografi dalam sistem pembayaran berbasis teknologi. Sebagai pionir dalam teknologi cryptocurrency, Bitcoin menawarkan sebuah sistem pembayaran yang tidak memerlukan bank sentral untuk mengatur sistem tersebut dan mengandalkan kalkulasi matematis dalam melakukan verifikasi atas transaksi yang dilakukan. Buku ini akan membantu Anda mengenal Bitcoin, dasar-dasar teknologi yang digunakan, cara mendapatkan dan menggunakan bitcoin. Buku ini juga mengulas beberapa jenis AltCoin, uang digital yang muncul setelah Bitcoin.