Page 79

5.0 Enigma Satoshi Nakamoto: Bitcoin dan Revolusi Privasi

Satoshi Nakamoto, seorang inovator misterius dan brilian, bermimpi tentang masa depan di mana transaksi keuangan tidak mengenal batas, transparan, dan aman—bebas dari kontrol pemerintah dan bank. Pada tahun 2008, Satoshi memicu Revolusi Kebebasan dengan makalah putih Bitcoin. Makalah ini menggambarkan implementasi praktis pertama dari teknologi blockchain. Bitcoin muncul sebagai simbol harapan dan ketahanan di dunia yang diguncang oleh krisis keuangan dan memudarnya kepercayaan pada lembaga terpusat. Transaksi Bitcoin pertama terjadi pada Januari 2009.

Didorong oleh keinginan untuk membangun sistem keuangan terdesentralisasi, Bitcoin milik Satoshi mengembalikan kekuatan kepada rakyat, memicu gerakan global yang menentang status quo dan memperjuangkan kebebasan keuangan.

5.1 Zcash dan Bitcoin

Tujuh tahun kemudian, pada tahun 2016, sekelompok ilmuwan dan peneliti meluncurkan Zcash. Tujuan mereka adalah untuk meningkatkan kekuatan game-changing dari Bitcoin milik Satoshi, yaitu dengan menambahkan fitur privasi. (Akan dibahas lebih lanjut nanti.)

Zcash sebenarnya adalah fork dari Bitcoin, yang berarti kode dari Bitcoin pada dasarnya disalin dan dimodifikasi. Ide untuk Zcash pertama kali dijelaskan dalam makalah putih yang diterbitkan pada tahun 2014 oleh profesor dan peneliti akademik dari MIT, Johns Hopkins University, Technion, dan Universitas Tel Aviv, dan dikembangkan selama beberapa tahun oleh Zooko Wilcox-O'Hearn dan timnya di Electric Coin Co. (ECC; dulunya disebut Zcash Company).

Orang-orang menggunakan Zcash untuk bertransaksi secara efisien dan aman dengan biaya rendah. Zcash ini aman, cepat, fleksibel, dan dapat diakses oleh semua orang — dibangun untuk era digital. Gunakan Zcash untuk membeli hampir apa saja, dari domain website hingga liburan ke pantai.

Anda dapat menggunakan ponsel Anda untuk membayar teman secara pribadi dengan Zcash, mengirim uang ke luar negeri, membeli kebutuhan pokok, atau mengirim donasi untuk tujuan yang baik. Gunakan aplikasi pihak ketiga seperti Flexa SPEDN untuk membayar dengan Zcash di Lowe's, Nordstrom, Baskin Robbins, dan lainnya. Layanan seperti Moon memungkinkan Anda menggunakan Zcash online di mana saja kartu Visa diterima.

5.1.1 Apa itu Bitcoin? Apa itu Zcash?

Bitcoin (BTC) adalah bentuk uang elektronik yang dapat dikirim dan diterima oleh siapa saja di jaringan Bitcoin. Bitcoin dapat disimpan dalam dompet digital, di ponsel atau komputer

desktop, yang terhubung ke sistem buku besar terdistribusi. Anggap saja ini seperti spreadsheet online raksasa, yang dapat diakses oleh semua orang, di mana semua transaksi dicatat.

Seperti Bitcoin, Zcash adalah mata uang digital yang berbasis pada buku besar berbasis blockchain yang bersifat open-source, tetapi berbeda dengan Bitcoin, Zcash memiliki sistem pembuktian zero-knowledge yang canggih yang melindungi buku besar dari penipuan sambil memungkinkan pengguna untuk menjaga informasi transaksi mereka tetap pribadi.

Page 80

5.1.2 Apa perbedaan antara Bitcoin dan Zcash?

Cara termudah untuk menggambarkan Zcash adalah bahwa ini adalah mata uang digital seperti Bitcoin tetapi melindungi privasi pengguna alih-alih mengekspos riwayat keuangan mereka. Ketika Bitcoin dirilis pada tahun 2009, itu adalah cryptocurrency terdesentralisasi pertama yang ada. Semua transaksi Bitcoin diverifikasi dan dicatat di blockchain secara publik, yang berarti siapapun di dunia dapat melihat saldo pengguna dan data transaksi. Ketiadaan privasi inilah yang menginspirasi para ilmuwan Zcash untuk membangun sesuatu yang lebih baik, dan pada tahun 2016, para ahli kriptografi ini mengambil kode sumber terbuka Bitcoin dan menambahkan bukti nol-pengetahuan (di antara perbaikan lainnya) untuk menciptakan Zcash.

Zcash menawarkan semua kenyamanan Bitcoin, tetapi dengan enkripsi penuh untuk melindungi informasi keuangan pengguna. Ada juga perbedaan penting lainnya, misalnya, mekanisme pendanaan mandiri untuk pengembangan Zcash, waktu konfirmasi yang lebih pendek, bidang memo pribadi, transaksi yang lebih cepat, dan banyak lagi.

5.1.3 Mengapa belajar tentang Zcash?

Zcash memberikan kesempatan kepada orang-orang untuk mentransfer uang digital dan data lainnya secara pribadi dan tanpa izin, tanpa perantara seperti bank atau lembaga pemerintah. Memiliki sistem uang yang pribadi, peer-to-peer, dan tanpa izin memberi orang kemampuan untuk menyimpan uang mereka dan bertransaksi dengan orang lain, terlepas dari entitas terpusat yang sering memberlakukan kontrol atau biaya. Zcash memberikan kebebasan kepada orang-orang untuk memilih apakah dan kapan mereka ingin mengungkapkan informasi tentang keuangan mereka kepada orang lain.

Zcash menyelesaikan kelemahan terbesar Bitcoin: kepemilikan pribadi dan transfer data. Di dunia di mana aplikasi blockchain dan cryptocurrency semakin diterima secara luas, transaksi pseudonim, seperti yang ada di Bitcoin, tidak lagi menjadi opsi yang layak untuk melindungi privasi pengguna. Aplikasi pengawasan semakin canggih dari hari ke hari dan banyak digunakan oleh orang-orang dan institusi untuk menganalisis dan melacak transaksi blockchain.

Page 81

5.1.4 Apa yang memberikan nilai pada Zcash?

Orang-orang dapat menggunakan ZEC untuk menyimpan kekayaan dalam aset yang keras dan melindungi privasi pengguna. Akan ada hanya 21 juta unit ZEC, yang berarti bahwa aset ini memiliki pasokan tetap. Setelah ZEC ke-21 juta ditambang dan beredar, aset ini akan menjadi anti-inflasi. Aset anti-inflasi merupakan lindung nilai yang baik terhadap inflasi jika para penjaga gerbang terpusat menggelembungkan pasokan uang nasional.

Zcash telah berkembang pesat sejak peluncuran jaringan aslinya pada akhir 2016, dan terus menawarkan kontrol atas privasi bagi pengguna blockchain dan kripto. Bukti kriptografi zk-SNARK telah membantu menetapkan standar privasi untuk kasus penggunaan berbasis blockchain di pasar global. Berbagai pengguna dan klien perusahaan sama-sama menuntut jenis privasi, fleksibilitas, dan kinerja yang disediakan oleh protokol Zcash.

5.1.5 Mengapa saya harus peduli?

Zcash memberikan pilihan kepada orang-orang untuk bertransaksi di luar sistem terpusat yang dapat menyensor dan/atau mengeksploitasi individu, serta untuk mengungkapkan informasi tentang keuangan mereka kepada orang lain atau menjaga informasi tersebut tetap pribadi. Mekanisme pembayaran digital yang tahan sensor ini melindungi kebebasan berbicara dan kebebasan berkumpul — serta kebebasan untuk menjadi manusia, bersikap konyol, atau menjadi apapun yang mereka inginkan!

Pengguna Zcash dapat mendonasikan uang kepada organisasi, mengirim uang ke luar negeri, atau hanya mengirimnya kepada teman, tanpa mengungkapkan identitas mereka dan tanpa rasa takut akan konsekuensi. Dan karena Zcash memiliki pasokan tetap sebanyak 21 juta, sama seperti Bitcoin, pengguna dapat merasa yakin bahwa ZEC mereka tidak akan terdevaluasi oleh pihak terpusat yang mencetak lebih banyak sesuai keinginan.

5.2 Zcash terdiri dari apa saja?

Zcash memberikan pengguna opsi untuk dua jenis transaksi: **transparent** (yang dapat dilihat oleh siapa saja) dan **shielded** (pribadi). Keduanya dieksekusi di blockchain Zcash yang sama, tetapi jumlah dan bukti untuk transaksi ditangani dengan cara yang berbeda. Untuk menjaga agar transaksi terlindungi tetap pribadi, Zcash memanfaatkan apa yang dikenal sebagai **zero-knowledge proof**.

Secara khusus, Zcash menggunakan **zk-SNARKs**, sebuah protokol zero-knowledge proof. Akronim zk-SNARK berarti **Zero-Knowledge Succinct Non-Interactive Argument of Knowledge**, dan merujuk pada konstruksi bukti di mana seseorang dapat membuktikan kepemilikan informasi tertentu, misalnya, kunci rahasia, tanpa mengungkapkan informasi tersebut dan tanpa interaksi antara pemberi bukti dan verifikator.

Sederhananya, zero-knowledge proof adalah metode kriptografi yang dapat membuktikan bahwa sesuatu itu benar tanpa mengungkapkan informasi yang membuatnya benar. Misalnya, dalam Zcash, ketika sebuah transaksi dilakukan antara dua pihak, zero-knowledge proof digunakan untuk memverifikasi bahwa pengirim memiliki cukup uang di dompet mereka untuk membayar total yang dikirim tanpa mengungkapkan kepada penerima, blockchain, atau orang lain informasi tentang saldo dompet pengirim.

Page 82

Bayangkan sejenak mata Anda ditutup, dan Anda memegang dua bidak catur di belakang punggung Anda. Anda tidak tahu apakah keduanya memiliki warna yang sama atau berbeda. Anda mengeluarkan satu dan menunjukkannya kepada pihak lawan Anda, yang tidak dibutakan. Dia memberi tahu Anda warna bidak tersebut — tetapi Anda tidak tahu apakah dia berbohong. Kemudian, Anda membawa bidak itu kembali ke belakang punggung Anda — mengganti bidak tersebut atau tidak — dan mengulangi prosesnya. Dengan melakukan ini berkali-kali, Anda dapat mulai merasa yakin tentang apakah orang lain berbohong.

Sebagai contoh, jika Anda mengeluarkan bidak yang sama dua kali dan dia memberi tahu Anda “hitam” pada kali pertama, dan “merah” pada kali kedua, Anda tahu dia berbohong. Jika jawabannya konsisten dengan pengetahuan Anda tentang bidak mana yang Anda tunjukkan, Anda dapat menjadi cukup yakin tentang apakah orang lain memberikan informasi yang jujur kepada Anda.

Proses semacam ini dapat digunakan untuk melindungi sejumlah besar informasi dengan kompleksitas yang tidak terbatas (seperti penggunaan SNARK rekursif untuk menyimpan akar Merkle dari keadaan global blockchain; tetapi itu di luar ruang lingkup buku ini).

5.2.1 Bagaimana koin Zcash baru masuk ke jaringan?

Basis moneter Zcash adalah pasokan tetap sebanyak 21 juta unit mata uang ZEC. Setiap 75 detik, sebuah blok baru ditambang ke dalam blockchain Zcash dan hadiah blok sebesar 3,125 ZEC masuk ke dalam peredaran. Hadiah blok ini didistribusikan kepada para penambang dan dana pengembangan Zcash.

Jumlah hadiah blok berkurang setengahnya sekitar setiap empat tahun hingga semua 21 juta ZEC berada dalam peredaran. Inflasi Zcash hampir secara tepat meniru inflasi Bitcoin. Penting untuk dicatat bahwa seiring dengan penciptaan koin baru, inflasi akan menurun, dan pada setiap peristiwa "halvening," laju inflasi turun secara signifikan.

5.2.2 Pengenalan ke Privasi Zcash

Alamat Zcash yang terlindungi menjaga informasi keuangan Anda tetap pribadi. Sebaliknya, alamat transparan membuat informasi tersebut menjadi publik. Sebagian besar blockchain mengekspos semua informasi transaksi dan saldo secara publik. Itu bukanlah rahasia yang memalukan, melainkan cara mereka dirancang. Menyimpan dan bertransaksi dengan Zcash yang terlindungi memberikan pengguna lebih banyak kontrol atas aset mereka dan dapat melindungi mereka dari penipu dan aktor berniat jahat lainnya.

Ketika Anda mengirim Zcash dari dompet digital Anda, Anda akan melihat bahwa alamat Anda adalah rangkaian panjang angka dan huruf. Penerima Anda juga akan memiliki alamat yang terdiri dari rangkaian panjang angka dan huruf. Jika alamat Anda dimulai dengan "z" dan Anda mengirim ke alamat penerima yang juga dimulai dengan "z," Anda dapat yakin bahwa informasi transaksi sepenuhnya pribadi. Jumlah pertukaran dan alamat masing-masing dompet terlindungi di blockchain publik. Ini biasanya merupakan cara terbaik untuk mengirim dan menerima ZEC ketika privasi diperlukan.

Ketika Anda mengirim dari atau menerima ke alamat yang dimulai dengan "t," yaitu, transaksi z-to-t atau t-to-z, tingkat privasi tidak selalu tinggi, karena beberapa informasi akan terlihat di blockchain. Transaksi t-to-t sepenuhnya publik, sama seperti transaksi Bitcoin.

Pengguna Zcash juga akan menemui alamat dompet yang dimulai dengan "u." Ini disebut sebagai **unified address**, dan berfungsi seperti adaptor perjalanan universal. Dengan alamat terpadu, dompet dapat secara otomatis memindahkan koin ke kolam terlindungi terbaru. Jadi, misalnya, katakanlah seorang pengguna membeli beberapa Zcash di bursa. Bursa tersebut mungkin mengirimkan Zcash transparan dari alamat t ke alamat terpadu Anda. Namun, jika dompet Anda mendukung autoshielding, dana tersebut akan secara otomatis dipindahkan ke penyimpanan pribadi.

Page 83

Jenis-jenis alamat Zcash

Saat ini, ada tiga jenis alamat utama yang digunakan hingga saat ini. Jenis-jenis ini meliputi:

Images Here

UNTUK PRIVASI MAKSIMUM, SELALU GUNAKAN ALAMAT Z- ATAU U-.

5.2.3 Bagaimana blockchain melacak siapa yang menggunakan Zcash?

Sebuah pohon hash atau **Merkle tree** terdiri dari cabang dan simpul daun yang diberi label dengan hash kriptografi dari sebuah blok data. Merkle tree adalah contoh dari skema komitmen kriptografi. Akar pohon dianggap sebagai komitmen, dan simpul daun dibuktikan sebagai bagian dari komitmen asli.

Mereka memverifikasi data yang disimpan atau di transfer di jaringan P2P, memastikan bahwa data yang diterima dari rekan tidak diubah. Dalam kolam terlindungi Zcash Sapling & Orchard, **Note Commitment Tree** digunakan untuk memverifikasi bahwa transaksi valid terhadap konsensus sambil sepenuhnya menyembunyikan pengirim, penerima, dan jumlah yang digunakan.

Page 84

5.2.4 Apakah transaksi Zcash aman?

Ya. Protokol Zcash dapat dianggap sangat aman karena merupakan salah satu protokol pembayaran nol-pengetahuan yang paling terdokumentasi dengan baik di dunia. Protokol ini telah direplikasi oleh sejumlah proyek kripto besar lainnya seperti Namada dan Penumbra. Selain itu, telah dilakukan banyak audit keamanan terhadap dompet dan komponen kriptografi yang digunakan dalam produk yang dipakai oleh pengguna Zcash.
5.2.5 Ikuti langkah-langkah berikut untuk melakukan transaksi Zcash:

- Konfirmasikan bahwa dompet Anda sudah tersinkronisasi dengan ketinggian blok terbaru.
- Jika sudah tersinkronisasi sepenuhnya, Anda dapat memastikan bahwa saldo Anda diperbarui dengan jumlah yang dapat dibelanjakan sepenuhnya.
- Masukkan alamat terpadu penerima Anda ke dalam kolom "alamat." Anda dapat menyalin alamat dari clipboard atau memindai kode QR dari pihak lawan.
- Isi jumlah yang ingin Anda kirim; biaya akan dihitung secara otomatis.
- Masukkan memo terlindungi untuk transaksi Anda. Ingat: Alamat transparan tidak dapat menerima memo.
- Konfirmasikan rincian transaksi dan kemudian klik kirim.

Waktu blok Zcash adalah 75 detik, dan mungkin memerlukan waktu 1-2 menit bagi penerima untuk diberi tahu tentang dana yang masuk. Tergantung pada jumlah konfirmasi yang diperlukan oleh dompet penerima Anda, mereka mungkin harus menunggu sebelum dapat membelanjakan Zcash tersebut.

5.2.6 Latihan: Transaksi Zcash dalam Aksi

Untuk mencoba menukar Zcash dengan teman, ikuti langkah-langkah berikut:

1. Keduanya siapkan dompet Zcash.
2. Di opsi "Kirim," pindai kode QR alamat teman Anda atau masukkan alamat U atau Z mereka.
3. Kirim memo yang mengatakan: "Hai, selamat datang di Zcash!"

5.2.7 Bisakah Zcash dihentikan?

Tidak. Zcash adalah protokol pembayaran internet terdesentralisasi yang tidak memerlukan izin, dijalankan oleh individu di seluruh dunia. Perangkat lunak node bersifat gratis dan sumber terbuka. Tidak ada otoritas pusat yang terlibat dalam validasi transaksi Zcash. Faktanya, karena privasi yang ditingkatkan oleh Zcash, jaringan ini sebenarnya lebih tahan terhadap upaya untuk mematikan jaringan.

Page 85

5.3 Siapa dan apa saja yang ada di Zcash?

Ada banyak tim dan developer independen yang mengerjakan Zcash, tetapi berikut adalah beberapa pemain kunci:

Electric Coin Co. (ECC)

Electric Coin Co. (ECC) menciptakan dan meluncurkan mata uang digital Zcash pada tahun 2016. Saat ini — bersama dengan tim dan pengembang independen lainnya — ECC terus mendukung komunitas Zcash melalui pengembangan produk, kesadaran dan adopsi, serta berbagai jenis penelitian. ECC dikenal luas sebagai salah satu tim kriptografi terkuat di dunia. Pada tahun 2016, mereka menjadi yang pertama berhasil menerapkan kriptografi nol-pengetahuan dalam aplikasi dunia nyata (Zcash), dan pada tahun 2022, insinyur ECC menemukan Halo, sebuah mekanisme pembuktian nol-pengetahuan rekursif yang baru, yang untuk pertama kalinya memberikan enkripsi blockchain yang benar-benar tanpa kepercayaan dan meningkatkan skalabilitas. Ada puluhan tim di berbagai proyek independen yang bekerja untuk menerapkan Halo dalam rilis mereka sendiri.

The Zcash Foundation (ZF)

The Zcash Foundation (ZF) adalah organisasi amal publik 501(c)(3) yang membangun infrastruktur privasi keuangan untuk kepentingan publik, terutama melayani pengguna protokol dan blockchain Zcash. Mereka, bersama dengan pihak lain, bekerja untuk memastikan bahwa protokol Zcash dan jaringan terbuka yang didukungnya tetap terdesentralisasi dan beragam. Beberapa kontribusi teknis ZF yang signifikan untuk ekosistem adalah pengembangan Zebra, sebuah node Zcash independen yang modern, dan FROST, sebuah skema tanda tangan ambang. Yayasan juga menyelenggarakan Zcon, sebuah konferensi tahunan yang berfokus pada teknologi privasi dan ekosistem Zcash, serta mendukung inisiatif komunitas akar rumput seperti Zcon Vozes, A/V Club, dan berbagai panggilan komunitas terbuka serta AMAs. Selain itu, Yayasan memajukan Zcash dengan membiayai berbagai proyek dalam program Minor Grants-nya, proyek penelitian internal dan eksternal, serta memberikan dukungan administratif untuk Zcash Community Grants (ZCG).

Zcash Community Grants (ZCG)

Zcash Community Grants (ZCG) membiayai proyek-proyek yang meningkatkan kegunaan, keamanan, privasi, dan adopsi Zcash. ZCG adalah dewan penasihat teknologi yang merupakan komite dari The Zcash Foundation sesuai dengan anggaran dasarnya. Hibah dipilih oleh komite yang terdiri dari lima anggota yang dipilih oleh Zcash Community Advisory Panel.

Proyek-proyek terbaru yang telah disetujui oleh ZCG termasuk:
- **Zcash Shielded Assets (ZSA)** yang dipimpin oleh tim QEDIT, membawa DeFi ke Zcash dengan protokol pembayaran baru yang menambahkan fitur tambahan ke mainnet.
- **Dokumenter pendek Zcash Media** yang menampilkan Zcasher terkenal seperti Edward Snowden, Zooko Wilcox, dan Deirdre Connolly.
- Sistem pembayaran terlindungi satu klik dan sistem Point-of-sale untuk toko fisik SDK yang sedang dikerjakan oleh **ZGo**.
- Program **Global Ambassador**, yang membantu Zcash mendapatkan representasi yang lebih luas secara internasional.

ZecHub

ZecHub adalah pusat pendidikan sumber terbuka yang berfokus pada Zcash, menampilkan komunitas global kontributor yang menerbitkan fitur-fitur, buletin, blog, tutorial, podcast, dan banyak lagi.