Nama : Diah Aisyah

NIM : 1103184023

**Bitcoin: A Peer-to-Peer Electronic Cash System**

Meskipun sistem bekerja dengan cukup baik untuk sebagian besar transaksi, sistem ini masih memiliki kelemahan yang melekat pada model berbasis kepercayaan. kemungkinan untuk transaksi kasual kecil, dan ada biaya yang lebih besar dalam hilangnya kemampuan untuk mengganggu mereka untuk mendapatkan lebih banyak informasi daripada yang mereka butuhkan.

Penipuan tertentu diterima sebagai hal yang tidak dapat dihindari. dihindari secara langsung dengan menggunakan mata uang fisik, tetapi tidak ada mekanisme untuk melakukan Yang dibutuhkan adalah sistem pembayaran elektronik berdasarkan bukti kriptografi dan bukan kepercayaan, yang memungkinkan dua pihak yang bersedia untuk bertransaksi secara langsung satu sama lain. Transaksi yang secara komputasi tidak praktis untuk dibalik akan melindungi penjual dari penipuan, dan mekanisme escrow rutin dapat dengan mudah diterapkan untuk Dalam makalah ini, kami mengusulkan solusi untuk masalah pengeluaran ganda menggunakan server cap waktu terdistribusi peer-to-peer untuk menghasilkan bukti komputasi urutan Sistem aman selama node yang jujur secara kolektif mengontrol lebih banyak daya CPU daripada kelompok node penyerang yang bekerja sama.

Dapat di definisikan koin elektronik sebagai rantai tanda tangan digital. Setiap pemilik mentransfer koin ke yang berikutnya dengan menandatangani secara digital hash dari transaksi sebelumnya dan kunci publik dari pemilik berikutnya dan Penerima pembayaran dapat memverifikasi tanda tangan untuk memverifikasi rantai Masalahnya tentu saja adalah penerima pembayaran tidak dapat memverifikasi bahwa salah satu pemilik tidak memeriksa setiap transaksi untuk pengeluaran ganda. Setelah setiap transaksi, koin harus dikembalikan ke mint untuk mengeluarkan koin baru, dan hanya koin yang dikeluarkan langsung dari mint yang dipercaya untuk tidak dibelanjakan Masalah dengan solusi ini adalah bahwa nasib seluruh sistem uang tergantung pada perusahaan yang menjalankan mint, dengan setiap transaksi harus melalui mereka, seperti bank. Kami membutuhkan cara bagi penerima pembayaran untuk mengetahui bahwa pemilik sebelumnya tidak Untuk tujuan kami, transaksi paling awal adalah yang diperhitungkan, jadi kami tidak peduli dengan upaya selanjutnya untuk membelanjakan dua kali lipat.

Tidak adanya transaksi adalah dengan mengetahui semua transaksi dan memutuskan mana yang datang lebih dulu. Untuk mencapai hal ini tanpa pihak yang dapat dipercaya, transaksi harus diumumkan secara publik diperlukan sistem bagi peserta untuk menyetujui Penerima pembayaran membutuhkan bukti bahwa pada saat setiap transaksi, mayoritas node setuju bahwa itu adalah yang pertama diterima. Solusi yang kami usulkan dimulai dengan server cap waktu.

Hash dari blok item yang akan diberi stempel waktu dan mempublikasikan hash tersebut secara luas, seperti di Stempel waktu membuktikan bahwa data harus ada pada saat itu, jelas, untuk rantai, dengan setiap stempel waktu tambahan memperkuat yang sebelumnya. sistem proofof-work yang mirip dengan Hashcash Adam Back , daripada posting koran atau Usenet.

Pekerjaan rata-rata yang diperlukan adalah eksponensial dalam jumlah bit nol yang diperlukan dan Untuk jaringan timestamp kami, kami mengimplementasikan proof-of-work dengan menambahkan nonce di dikeluarkan untuk membuatnya memenuhi proof-of-work, blok tidak dapat diubah tanpa mengulang pekerjaan. Karena blok selanjutnya dirantai setelahnya, pekerjaan untuk mengubah blok akan mencakup mengulang Jika mayoritas didasarkan pada satu-alamat-satu-suara, itu bisa ditumbangkan oleh siapa saja yang bisa sebagian besar daya CPU dikendalikan oleh node yang jujur, rantai yang jujur akan tumbuh paling cepat dan Untuk memodifikasi blok sebelumnya, penyerang harus mengulang proof-of-work blok dan semua blok setelahnya dan kemudian mengejar dan melampaui pekerjaan node yang jujur.

Untuk mengimbangi peningkatan kecepatan perangkat keras dan minat yang bervariasi dalam menjalankan node dari waktu ke waktu, kesulitan proof-of-work ditentukan oleh rata-rata bergerak yang menargetkan jumlah rata-rata

Langkah-langkah untuk menjalankan jaringan adalah sebagai berikut:

1. Transaksi baru disiarkan ke semua node.
2. Setiap node mengumpulkan transaksi baru ke dalam satu blok.
3. Setiap node bekerja untuk menemukan proof-of-work yang sulit untuk bloknya.
4. Ketika sebuah node menemukan proof-of-work, blok tersebut akan disiarkan ke semua node.
5. Node menerima blok hanya jika semua transaksi di dalamnya valid dan belum dibelanjakan.
6. Node mengekspresikan penerimaan mereka terhadap blok dengan bekerja membuat blok berikutnya dalam rantai, menggunakan hash dari blok yang diterima sebagai hash sebelumnya.

Node selalu menganggap rantai terpanjang sebagai yang benar dan akan terus bekerja untuk Jika dua node menyiarkan versi berbeda dari blok berikutnya secara bersamaan, beberapa node mungkin menerima satu atau yang lain terlebih dahulu. Dalam hal ini, mereka mengerjakan yang pertama .