**TUGAS**

**BLOCKCHAIN**

**“Blockchain Transaction”  
**

**Dosen Pengampu:**

**Ade Kurniawan. S.Pd.M.Pd.T**

**Oleh Kelompok 10:**

**Mauliza Aprilia (22346014)**

**Natha Fahrezi Azra. A (22346017)**

**PROGRAM STUDI INFORMATIKA**

**DEPARTEMEN TEKNIK ELEKTRONIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS NEGERI PADANG**

**2025**

1. **Blok dalam Blockchain**

**1.5.1 Arti Blok**

Blok adalah catatan yang berisi detail data transaksi. Ini terdiri dari rincian berikut:

1) Hash blok – Nomor alfanumerik untuk mengidentifikasi blok

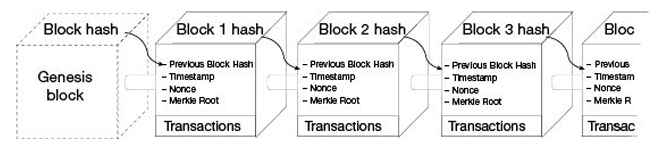
2) Hash blok sebelumnya

3) Stempel waktu

4) Nonce – angka acak yang digunakan untuk memvariasikan nilai hash

5) Akar Merkle – hash semua hash dari semua transaksi di blok

6) Data transaksi. Ini berisi rincian beberapa transaksi



Gambar 1.10: Representasi blok

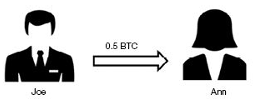
Blok genesis adalah blok pertama. Ini adalah satu-satunya blok tanpa hash data dari blok sebelumnya karena tidak ada blok yang mendahuluinya. Blok genesis berisi transaksi yang digabungkan dan divalidasi untuk menghasilkan hash yang unik.

Hash blok genesis, bersama dengan semua transaksi baru, diproses dan digunakan sebagai input untuk membuat hash baru yang digunakan di blok berikutnya, yaitu, katakanlah Blok 1 (lihat Gambar 1.10). Hash Blok 2 dibuat dengan hash Blok 1 dan serangkaian transaksi baru lainnya. Ini berlanjut dengan setiap blok yang menghubungkan kembali ke blok sebelumnya melalui hash-nya, sehingga membentuk rantai yang mengarah kembali ke blok genesis. Oleh karena itu namanya, blockchain.

Keterkaitan berkelanjutan ini membuat tidak mungkin bagi aktor jahat untuk mengubah informasi atau menyisipkan blok di antara dua blok yang ada. Untuk melakukannya, semua blok yang terhubung juga perlu diubah. Akibatnya, setiap blok memperkuat blok sebelumnya, termasuk keamanan seluruh blockchain, karena rantai yang lebih besar berarti lebih banyak blok perlu diubah jika seseorang ingin merusak informasi apa pun.

**1.5.2 Transaksi Blockchain dalam Nutshell**

Mari kita lihat semua langkah tingkat tinggi yang terlibat dalam transaksi blockchain. Ingat: Blockchain adalah buku besar digital atau database digital Buku besar blockchain didistribusikan ke semua node dalam jaringan, yaitu, semua node memiliki salinan buku besar yang sama Blockchain terdesentralisasi, yaitu, tidak ada kontrol pusat. Semua node dalam jaringan dapat berpartisipasi dalam pemrosesan dan pembuatan blok Kunci kriptografi unik mengamankan setiap catatan di blockchain Mari kita ambil contoh rencana Joe untuk mengirim 0,5 BTC ke Ann melalui blockchain.



Tabel berikut memberikan representasi langkah demi langkah dari transaksi antara Joe dan Ann di blockchain.

Tabel 1.2 Representasi langkah demi langkah dari transaksi blockchain

|  |  |
| --- | --- |
| **Langkah 1: Joe meminta transaksi yang diusulkan**  Joe dikirimkan Joe 0,5 BTC dari aplikasi Dompetnya |  |
| **Langkah 2: Transaksi yang diusulkan disiarkan ke jaringan** |  |
| **Langkah 3: Penambang memverifikasi transaksi dan menggabungkannya ke dalam blok bersama dengan transaksi lainnya.**  – Penambang akan memvalidasi keaslian transaksi, yaitu, status Joe, saldonya, dll. **Catatan:** Penambang memvalidasi semua transaksi yang ingin mereka sertakan dalam blok yang mereka rencanakan untuk ditambang. |  |
| **Langkah 4: Penambang bersaing untuk memecahkan teka-teki matematika yang kompleks.**  – Teka-teki membutuhkan banyak daya komputasi untuk dipecahkan.  – Ini melindungi blockchain dari peretas karena akan sulit dan mahal untuk menyerang jaringan. |  |
| **Langkah 5: Node memverifikasi pekerjaan penambang.**  – Penambang yang menemukan hash yang benar menyiarkan blok ke jaringan  – Mayoritas node/penambang perlu menyetujui/memverifikasi blok agar dapat diterima ke dalam blockchain  – Setelah disetujui, penambang yang menang dapat mengumpulkan hadiahnya. |  |
| **Langkah 6: Blok ditambahkan ke blockchain.**  – Setelah blok diverifikasi, penambang yang menang menambahkan bloknya ke blockchain yang ada. **Catatan:** Transaksi Joe ditambahkan ke blockchain bersama dengan transaksi lainnya |  |
| **Langkah 7: Salinan blockchain yang diperbarui diedarkan ke seluruh jaringan.** |  |
| **Langkah 8: Penyelesaian transaksi**  Ann menerima 0,5 BTC di dompetnya. Transaksi selesai. |  |

Jadi singkatnya, proses transaksi blockchain terdiri dari:

– Sebuah node di blockchain (jaringan P2P) meminta transaksi melalui dompet.

– Transaksi disiarkan ke semua node dalam jaringan.

– Transaksi divalidasi/diverifikasi oleh jaringan menggunakan algoritma konsensus, yaitu, aturan preset yang ditetapkan oleh blockchain tertentu.

– Transaksi diterima atau ditolak. Jika diterima, transaksi ditambahkan dalam urutan kronologis bersama dengan transaksi lain untuk membuat blok data baru yang disegel (hash).

– Transaksi sekarang menjadi bagian dari blockchain dan permanen dan tidak dapat diubah.

**1.5.3 Pengeluaran Ganda**

Dengan popularitas blockchain yang terus meningkat, semakin banyak orang bergerak menuju transaksi dalam mata uang digital. Hal ini membawa masalah pengeluaran ganda, kelemahan yang unik untuk mata uang digital. Pengeluaran ganda, seperti namanya, adalah menghabiskan uang lebih dari sekali. Sama seperti seseorang dapat menyalin file digital dan mengirimkannya ke beberapa orang, dimungkinkan untuk menduplikasi koin atau token kripto dan menggunakannya kembali. Jika ini terjadi di jaringan blockchain, itu tidak hanya dapat merusak konsep buku besar terdistribusi tepercaya tetapi juga menyebabkan inflasi dengan mata uang duplikat yang curang di jaringan. Ingat, tidak ada pihak ketiga tepercaya untuk memvalidasi bahwa transaksi tersebut bukan pembelanjaan ganda.

Masalah pengeluaran ganda dihindari dalam blockchain melalui mekanisme konsensusnya dan struktur kronologis dasar tentang bagaimana blok dirantai bersama.

Transaksi diverifikasi dan ditambahkan ke blok melalui mekanisme konsensus setelah sejumlah besar daya komputasi dan sumber daya dihabiskan. Kembali dan mencoba untuk menggandakan transaksi itu akan membutuhkan daya komputasi yang sama jika tidak lebih banyak, terutama dengan lebih banyak blok yang ditambahkan ke rantai untuk sementara; praktis tidak mungkin untuk memodifikasi semua blok. Tidak ada yang akan menghabiskan sejumlah besar sumber daya jika pengembalian tidak sepadan dengan usahanya.

Selain itu, transaksi pertama akan diberi stempel waktu dan ditautkan secara kriptografis ke blok sebelumnya dan disiarkan ke semua node dalam jaringan. Ketika transaksi kedua (penipuan) diusulkan, itu akan gagal pada proses verifikasi dan ditolak.

Setelah transaksi dikonfirmasi, hampir tidak mungkin untuk membelanjakannya dua kali. Semakin banyak blok yang dikonfirmasi dalam rantai, semakin sulit untuk membelanjakan kripto secara ganda.

Namun, secara teoritis dimungkinkan untuk membelanjakan mata uang kripto dua kali lipat. Meskipun jarang, ini dapat dilakukan dengan serangan 51% (di mana ada kendali lebih dari setengah hash rate jaringan), serangan Finney, atau serangan Race. Lebih lanjut tentang serangan blockchain dijelaskan di Bab 11.