

Bab #9:

Pengantar Sisi Teknis Bitcoin



Tentang Uang



Penyimpan Nilai

Durable (Tahan lama)

Scarce (Langka)

Alat Tukar

Acceptable (Bisa diterima)

Divisible (Bisa dibagi-bagi)

Permissionless (Tidak perlu izin untuk dipakai)

Portable (Mudah dibawa dan dipindahkan)

Verifiable (Keasliannya mudah diperiksa)

Satuan Hitung

Fungible (Kesetaraan unit)

Evolusi Uang



Dari Barter ke Uang Logam

Terciptalah suatu barang yang berperan sebagai alat tukar standar universal

Dari Uang Logam ke Uang Kertas

Uang kertas lebih mudah dibawa dan dipindahkan dibandingkan uang logam

Dari Uang Kertas ke Uang Digital

Uang digital memungkinkan transaksi jarak jauh secara instan

Dari Uang Digital ke Uang Terdesentralisasi

Sistem keuangan menjadi tidak bergantung pada pihak ketiga seperti bank

Apa itu Bitcoin?

Diciptakan oleh **Satoshi Nakamoto**, Bitcoin adalah jaringan moneter **terdesentralisasi, peer-to-peer** yang memungkinkan transaksi ***trustless*** dan ***permissionless*** dengan uang yang bisa **menyimpan nilainya seiring waktu.**



In a Nutshell



Apa itu Bitcoin?

Sebuah catatan riwayat transaksi dari semua bitcoin yang ada sejak 3 Januari 2009.

Siapa yang menyimpan catatan ini?

Semua orang yang menjalankan aplikasi atau software tertentu memiliki salinan dari catatan ini.

Siapa yang bisa meng-update catatan ini?

Siapapun bisa, asalkan mereka berhasil menebak angka yang benar (**dari 1 hingga 4.294.967.295**)

Blockchain

Node

Miner

The Problem with Trust

Sistem **terdesentralisasi**,
siapa yang kita percaya?

Ada **Aturan Konsensus Nakamoto** yang ditegakkan oleh setiap **node**.

Node adalah wasit di dalam jaringan Bitcoin.



Selamanya hanya akan ada 21 juta Bitcoin.

Blockchain yang paling panjang adalah yang valid.

Bitcoin yang sama tidak boleh dipakai lebih dari satu kali.

Ukuran maksimum blok adalah ~1 MB.

Kriptografi di Bitcoin



Kriptografi Kunci Bitcoin



Bitcoin adalah catatan riwayat transaksi, sehingga tidak ada bentuk fisiknya.

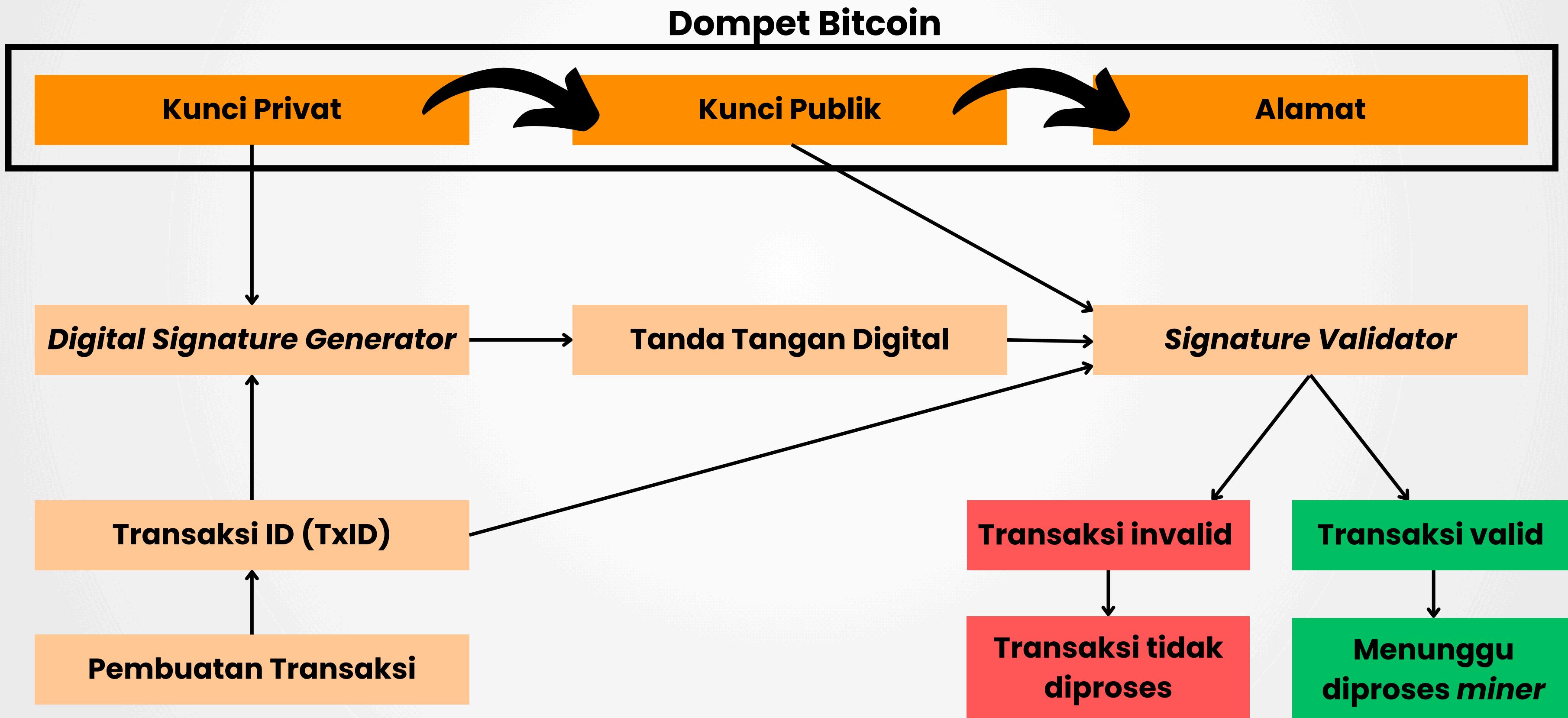
Oleh karena itu, tiap orang perlu **sertifikat kepemilikan** atas Bitcoin Anda (**Kunci**).

Kunci ini disimpan di dalam **dompet Bitcoin** Anda.

Dompet Bitcoin



Validasi Transaksi



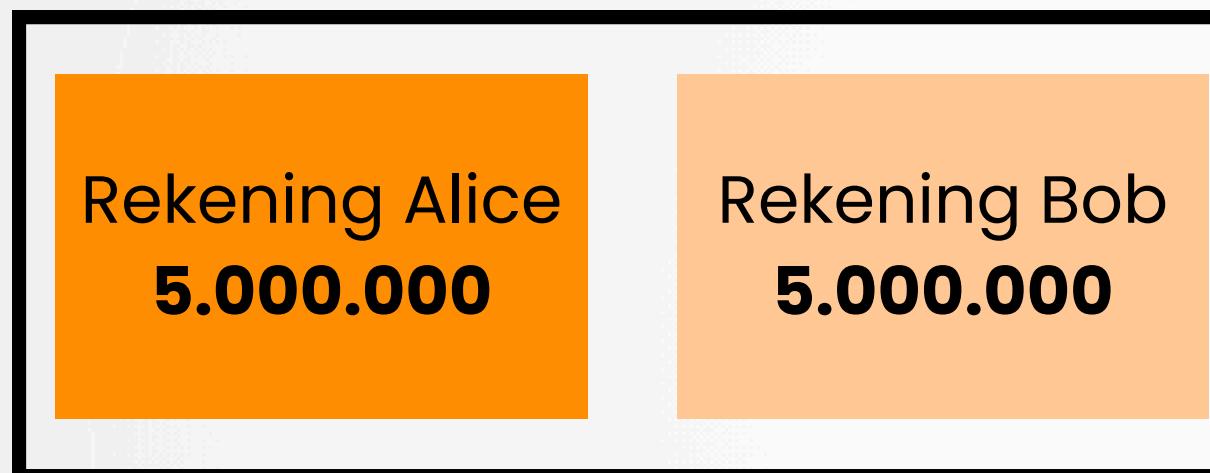
UTXO Model **di Bitcoin**



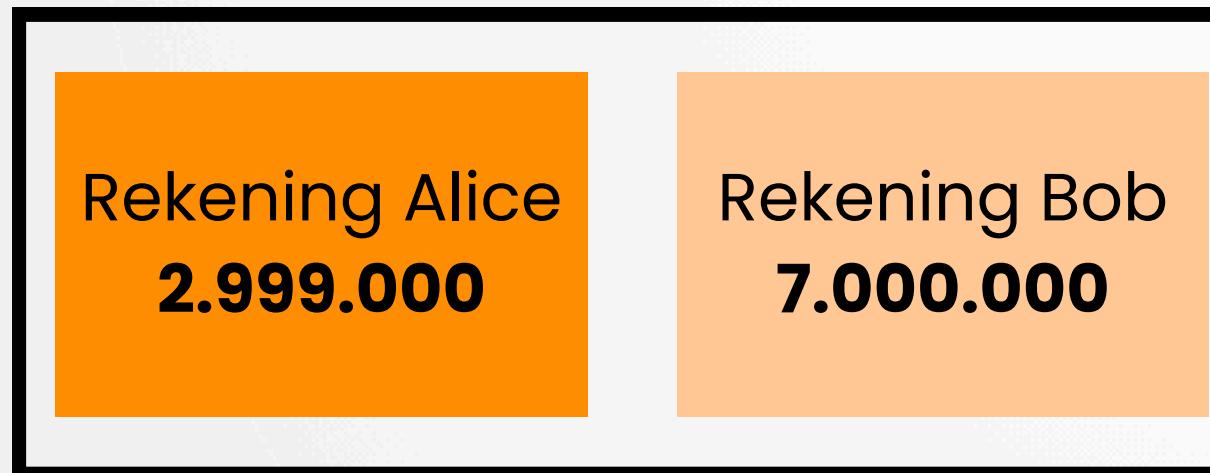
Account-Based vs UTXO Model

Account-Based Model

Sebelum transaksi



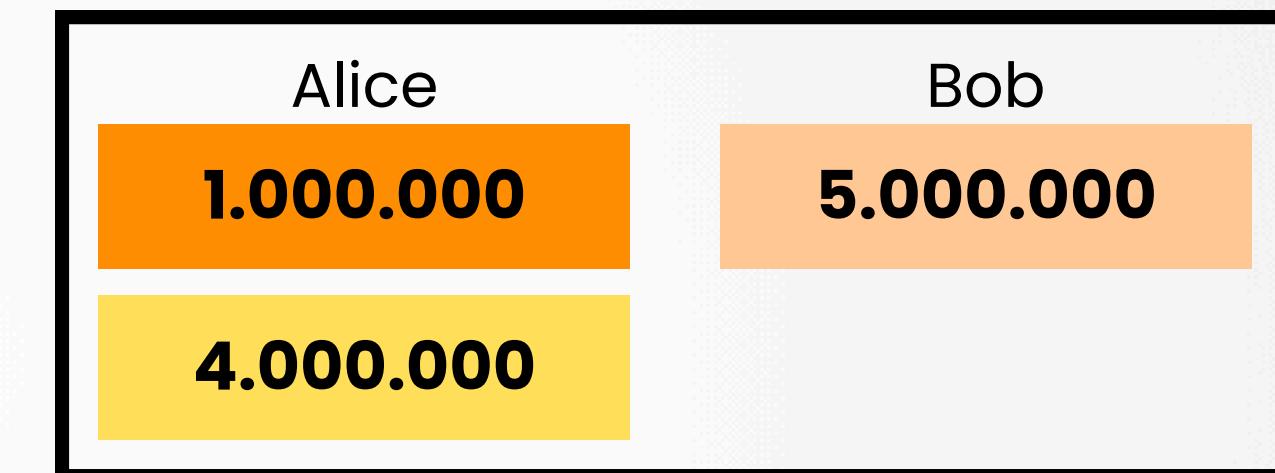
Setelah transaksi (Alice bayar Bob 2 juta)



Biaya transaksi untuk bank **1.000**

UTXO Model

Sebelum transaksi



Setelah transaksi (Alice bayar Bob 2 juta)

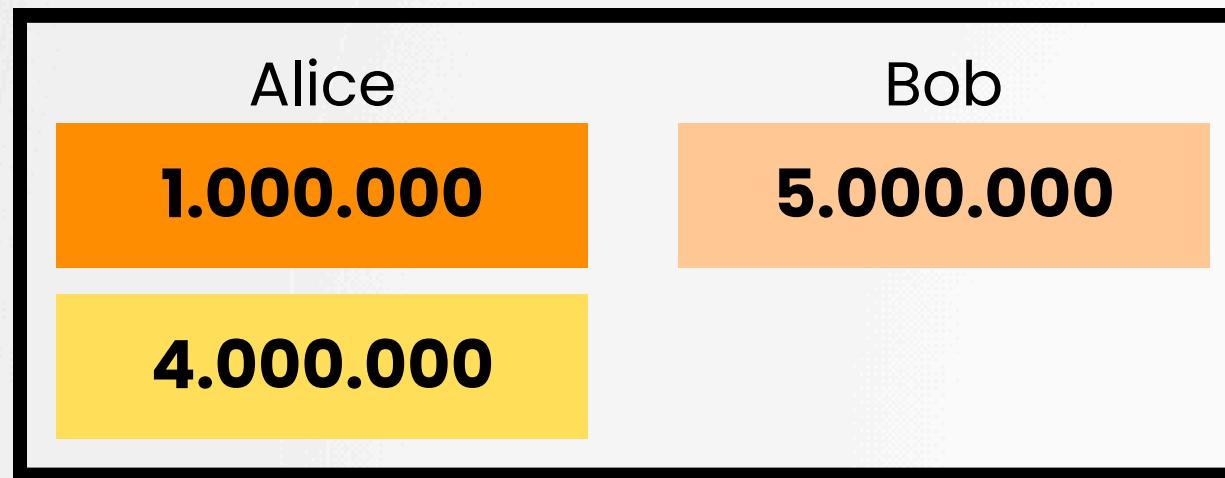


Biaya transaksi untuk miner **1.000**

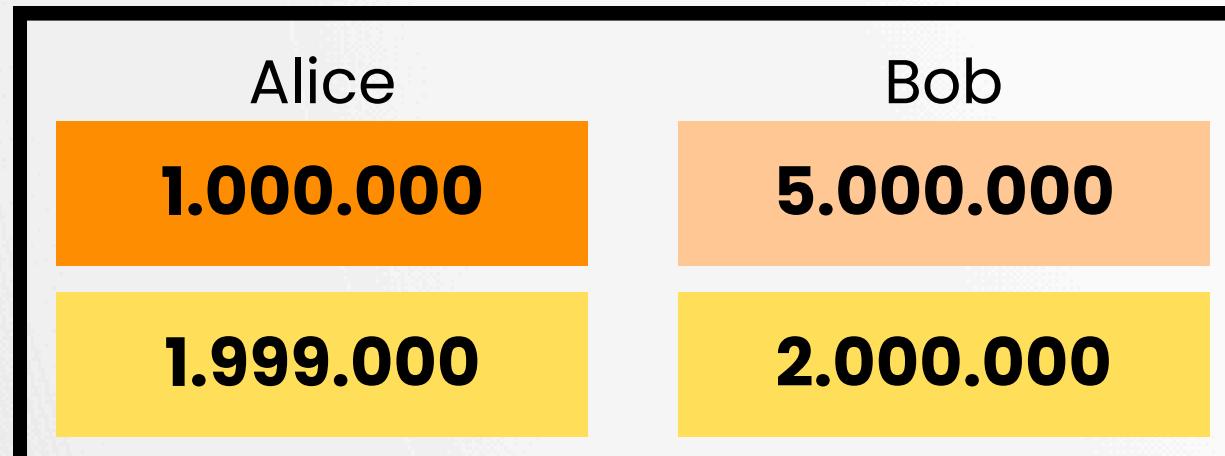
UTXO: Bongkahan Bitcoin



Sebelum transaksi



Setelah transaksi (Alice bayar Bob 2 juta)



Biaya transaksi untuk miner 1.000

UTXO = Unspent Transaction Output.

UTXO adalah **bongkahan Bitcoin** yang ada di dompet Anda.

Saldo yang tampil di dompet Bitcoin adalah **total nominal dari semua UTXO**.

Tiap UTXO harus digunakan secara penuh, **tidak bisa “dicuil-cuil”**. Contoh: pembayaran 13.000.000:



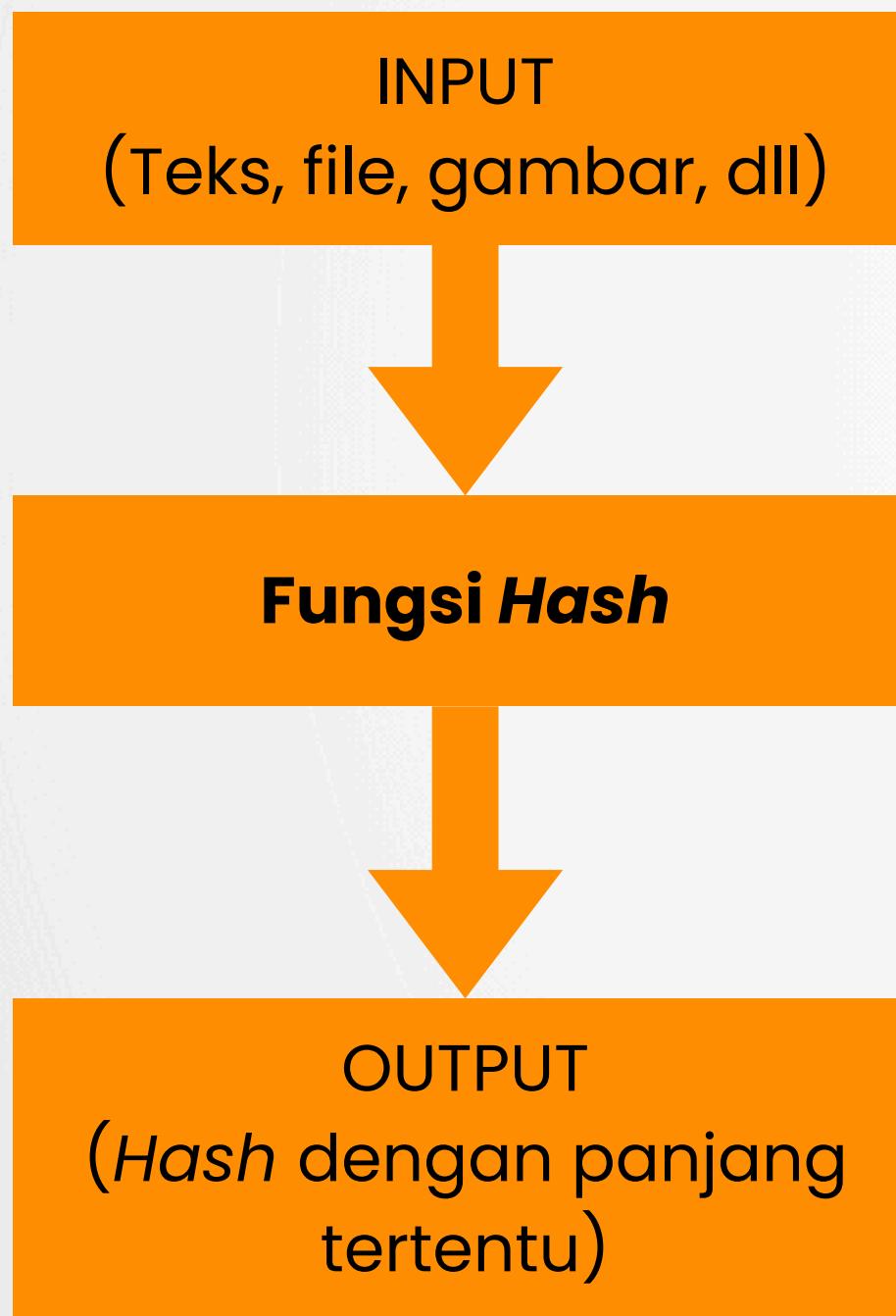
Blockchain Bitcoin



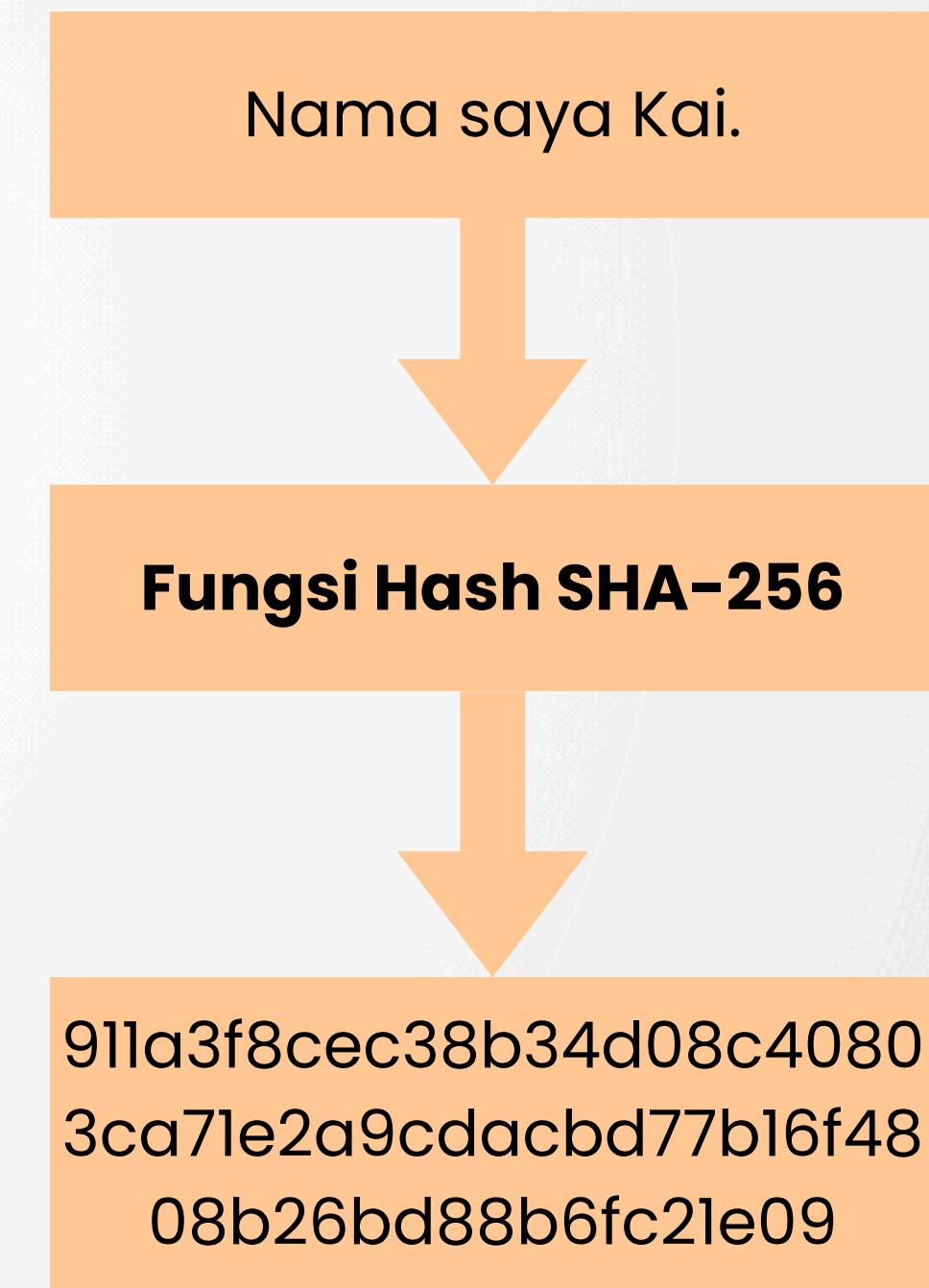
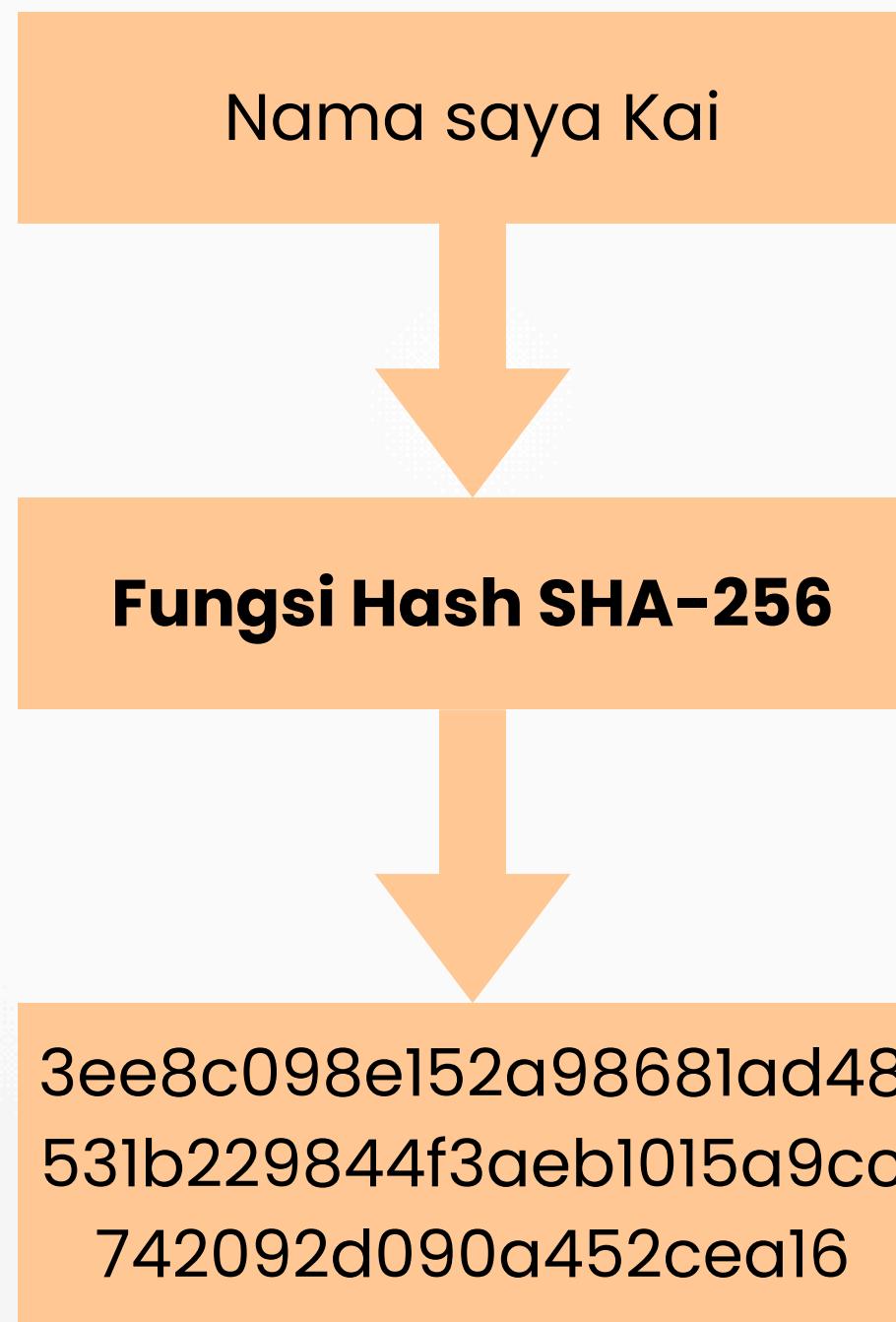
Hash Function



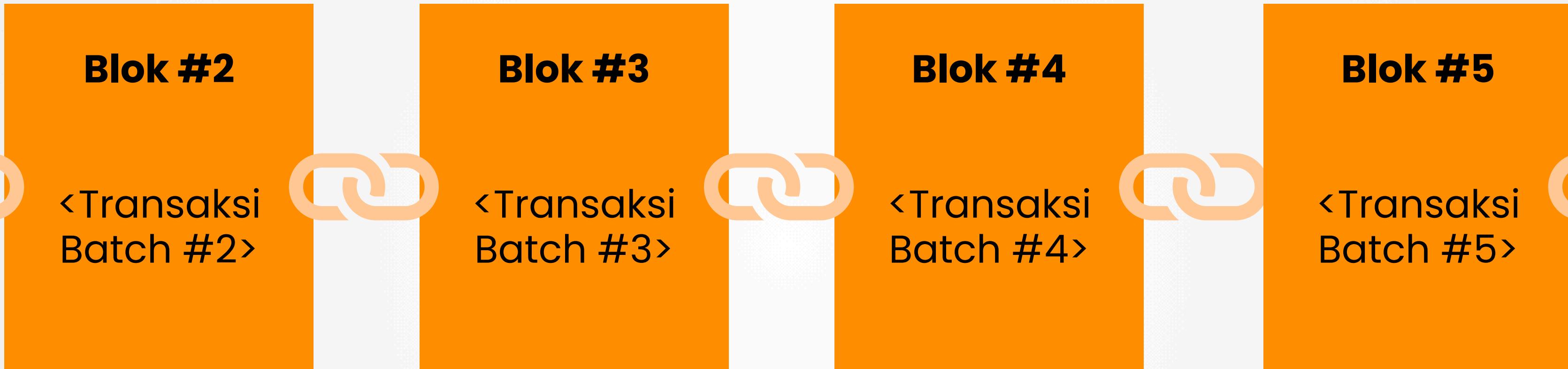
Prinsip Kerja



Contoh Hash Function: SHA-256



Blockchain Bitcoin



Bagaimana rantai blok Bitcoin bekerja:

1. Transaksi-transaksi **dicatat dalam blok**.
2. Total data transaksi tiap blok **tidak lebih dari ~1 MB**.
3. Blok-blok ini **disambung** menjadi satu, urut secara waktu.

Struktur Blok Bitcoin

Block Header

1. **Hash dari Blok sebelumnya**, penghubung blok dengan blok sebelumnya.
2. **Nonce**, angka yang harus ditebak untuk memproses transaksi dalam blok ini.
3. **Komponen-komponen lainnya**.

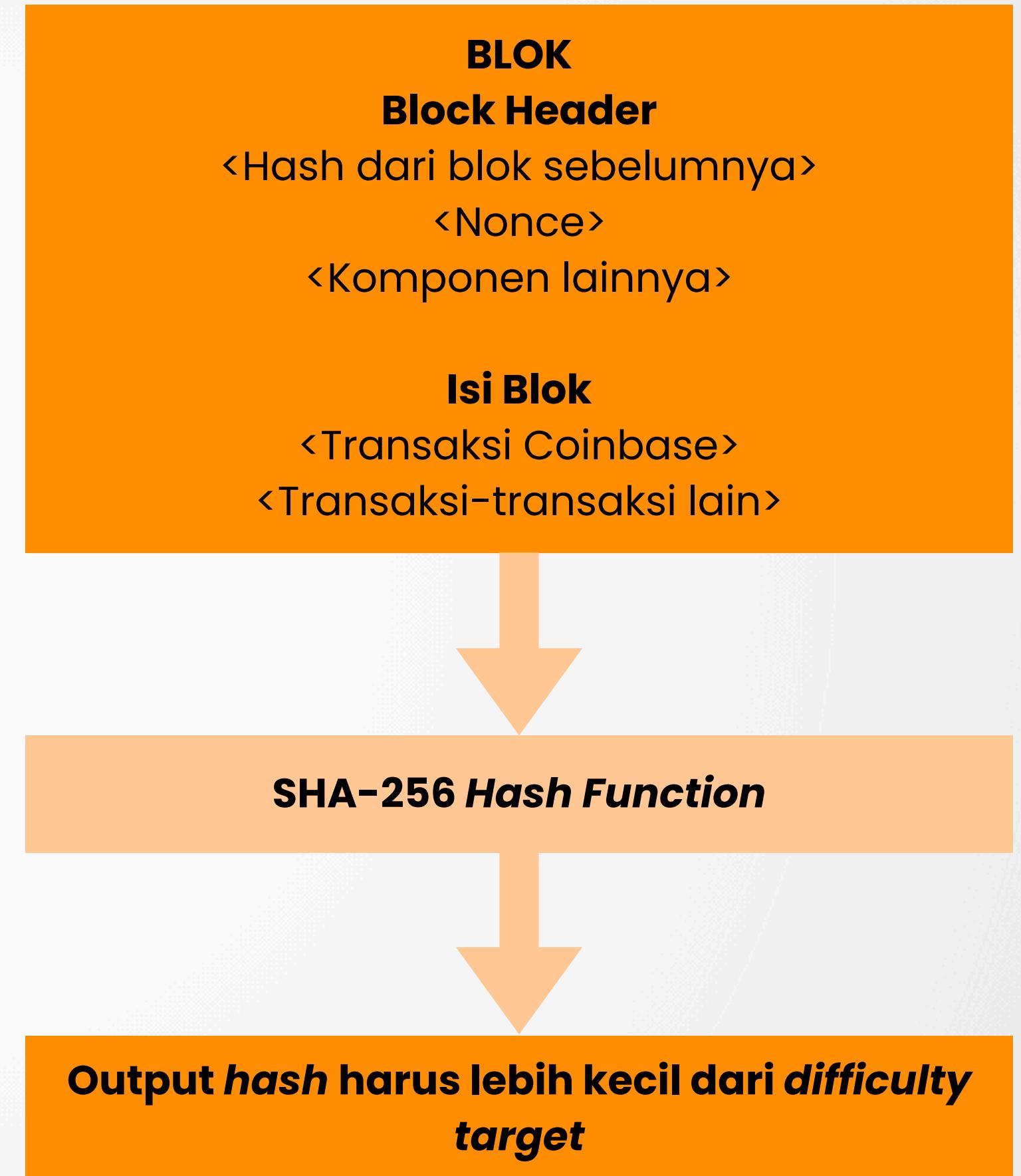
Isi Blok

1. **Coinbase transaction**, transaksi yang memberikan reward untuk *miner* yang berhasil memproses transaksi dalam blok.
2. **Transaksi-transaksi** yang diproses dalam blok ini.

Mining di Bitcoin

Minning adalah “perlombaan” pemrosesan transaksi yang membutuhkan energi listrik yang besar.

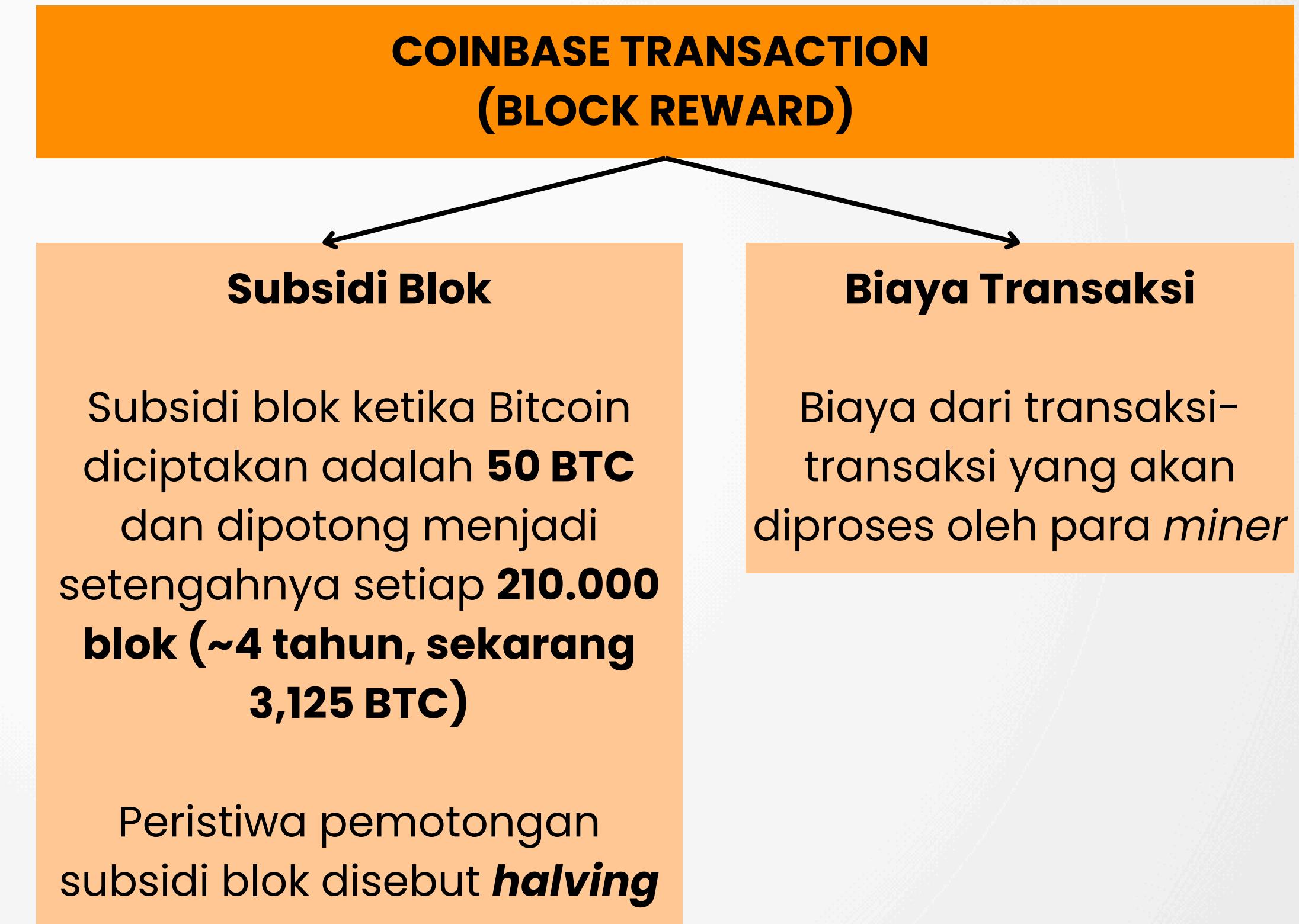
Miner berusaha menebak **nonce** sehingga **output SHA-256** dari blok tersebut lebih kecil dari batas yang ditentukan (**difficulty target**)



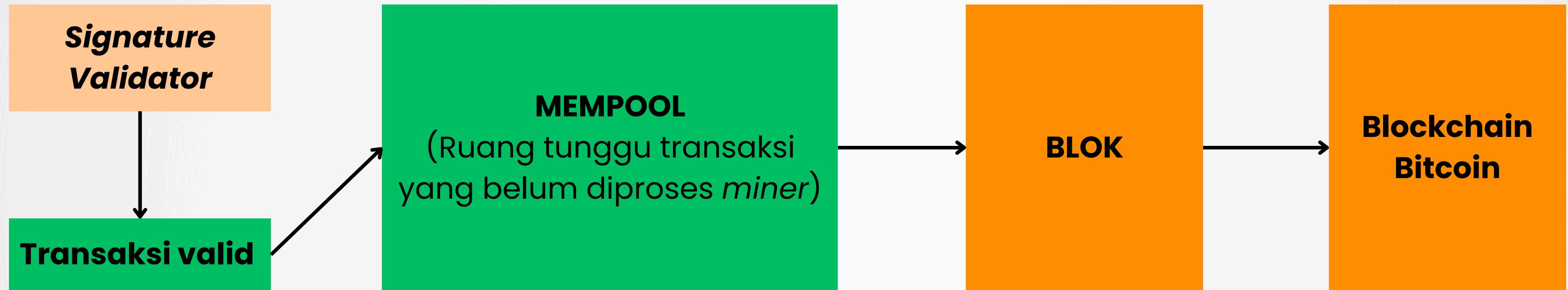
Transaksi Coinbase: Incentif Miner

Mengapa orang-orang mau **mining**? Karena ada **block reward** berupa **bitcoin**.

Transaksi *coinbase* adalah transaksi yang ditujukan untuk memberi *reward* Bitcoin kepada *miner*.



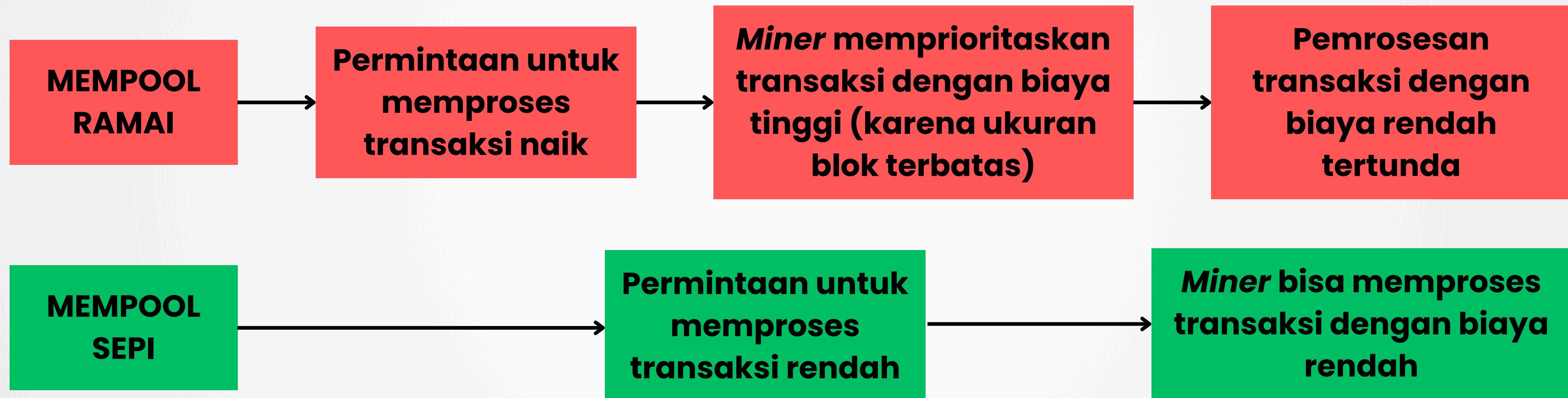
Mempool: Ruang Tunggu Transaksi



Catatan: Ukuran Blok Bitcoin **terbatas** (~1 MB), sehingga *miner* akan cenderung memilih memproses transaksi dengan **biaya yang lebih tinggi** duluan.

Biaya Transaksi: Incentif Miner

Dalam setiap transaksi Bitcoin, penentuan nominal biaya transaksi adalah kebebasan pengguna.



Biaya Transaksi

$$\text{Biaya Transaksi} = \text{Fee rate} \times \text{Ukuran Transaksi}$$

↓
Biaya total
transaksi

↓
Tergantung
lalu lintas
transaksi di
mempool

↓
Tergantung pada
jumlah UTXO yang
dipakai dalam
transaksi

Mining Game



Mekanisme Game



- 1** Peserta memindai QR code dan masuk ke website SHA-256. Permainan ini akan terdiri dari 1 ronde uji coba dan 3 ronde mining.
- 2** Di setiap ronde, akan ada suatu kalimat transaksi di layar presentasi. Peserta wajib mengetikkan kalimat transaksi secara sama persis ke bagian input di website SHA-256. Apabila terdapat perbedaan (huruf kapital, tanda baca, typo), maka hasil kerja peserta tidak akan dianggap valid.
- 3** Tekan Enter, lalu peserta berusaha untuk menambah sebuah komponen yang merupakan kombinasi angka/huruf/simbol atau karakter lainnya (proof of work) yang membuat output dari SHA-256 diawali oleh **dua angka nol atau lebih**. Apabila tidak di-enter, maka proof of work tidak akan dianggap valid.
- 4** Setelah berhasil menemukan proof of work, peserta wajib menscreenshot layar dan mengirimkan hasilnya ke grup BPA. Screenshot harus dengan jelas menunjukkan **KALIMAT TRANSAKSI** dan **OUTPUT** dari SHA-256.
- 5** Hasil screenshot memenuhi syarat-syarat berikut:
 - 1. Kalimat transaksi dan output ter-screenshot,**
 - 2. Tidak ada typo pada kalimat transaksi,**
 - 3. Ada jarak enter,**
 - 4. Output diawali minimal dua angka 0.**Apabila terdapat komponen yang tidak valid, maka game berlanjut. Apabila screenshot sudah sesuai syarat, maka peserta tersebut dinyatakan menang. Peserta yang sama bisa memenangkan lebih dari satu ronde. (1 pemenang saja per ronde).

Contoh Salah:

1. Arale membayar 3000 sats ke Kai.

Input

```
Ofj1bi91efbf1xxi01x0i1sbi0e1b0befw  
ocievidviqvodvivovozqsdqlhofotoksakaqql111isjrjwk  
ajehri3o29wiakqhejwksjrjfbfuekakqowiejsjakaksuejek  
sjwueiskjiri3jehshsjejekwiwi2i2283uujejshshahahah  
hsshsjsjslwvdqlvqdlv1rv1lv1rklqdvqlvl1rvr1ov  
1ovqovo1vro1r39393983388f8ec18vjsjsjshzsbbzejwjw  
jwjwjjqjjsjjwhwjajjjsjhjsjsjajwjajajajjhshshs  
hshshqvqr1g1e1rshshhshhs818193858s9ajzy2o
```

Output

```
8a0c7595f249999840ed4cff6567fddf60b37ce047628d023c  
c5edee8fd6ea14
```

Kalimat transaksi tidak ter-screenshot

Input

```
1 Arale membayar 3000 sats ke Kai  
Ofj1bi91efbf1xxi01x0i1sbi0e1b0befw  
ocievidviqvodvivovozqsdqlhofotoksakaqql111isjrjwk  
ajehri3o29wiakqhbuekakqowiejsjakaksuejeksjwuwi2  
i2283uujejshshahahahhsshsjsjslwvdqlvqdlv1rv1  
1v1rklv1rvr1ov1ovqovo1vro1r39393983388f8ec18vjsj  
sjshzsbbzejwjwjwjqjjsjjwhwjajjjsjhjsjsjajwj  
jajajajajjhshshhshqvqr1g1e1rshshhshhs818193858
```

Output

```
34e8b177976eb361c7a64c383d54fdd8b330e5d719474acaef  
bedc2a7bcb3ba8
```

Kalimat transaksi ada typo
Output tidak diawali oleh setidaknya dua angka nol

Contoh Benar:

1. Arale membayar 3000 sats ke Kai.

```
Input
1. Arale membayar 3000 sats ke Kai.
0fj1bi91efbf1xxi01x0x0i1sbi0e1b0befw
ocievidviqvodvivovozqqsdqlhofotoksakaqq111isjrjwk
ajehri3o29wiakqhejwksjrjfbfuekakqowiejsjakaksuejek
sjwueiskjiri3jehshsjejekwiwi2i2283uejejshshahahah
hsshsjsjsjsjsjshzsbbbejewjwjwjjqjjsjwhwjajjjs
jhjsjsjsjajwjajajajahshshshshhhshhs818193
858s9ajzy2d

Output
00bdbf3793f553222b93e7e11eacb69386a52adcd7e5740693
3b5336e8d6b453
```

Kalimat transaksi dan output terlihat jelas

Kalimat transaksi tidak ada typo

Ada jarak Enter

Output diawali setidaknya dua angka nol

Ronde Uji Coba



**1. Greg Notorito membayar 1 Bitcoin ke
Nisa**

Reminder:

- 1. Kalimat transaksi dan output ter-screenshot,**
- 2. Tidak ada typo pada kalimat transaksi,**
- 3. Ada jarak enter,**
- 4. Output diawali minimal dua angka 0.**

Ronde 1



2. Greg Notorito membayar 1 Bitcoin ke Nisa

Reminder:

1. Kalimat transaksi dan output ter-screenshot,
2. Tidak ada typo pada kalimat transaksi,
3. Ada jarak enter,
4. Output diawali minimal dua angka 0.

Ronde 2



**3. user#444 membayar 4 BTC ke
user#333**

Reminder:

- 1. Kalimat transaksi dan output ter-screenshot,**
- 2. Tidak ada typo pada kalimat transaksi,**
- 3. Ada jarak enter,**
- 4. Output diawali minimal dua angka 0.**

Ronde 3



4. ABCDEF membayar 600 satoshi ke KLM

Reminder:

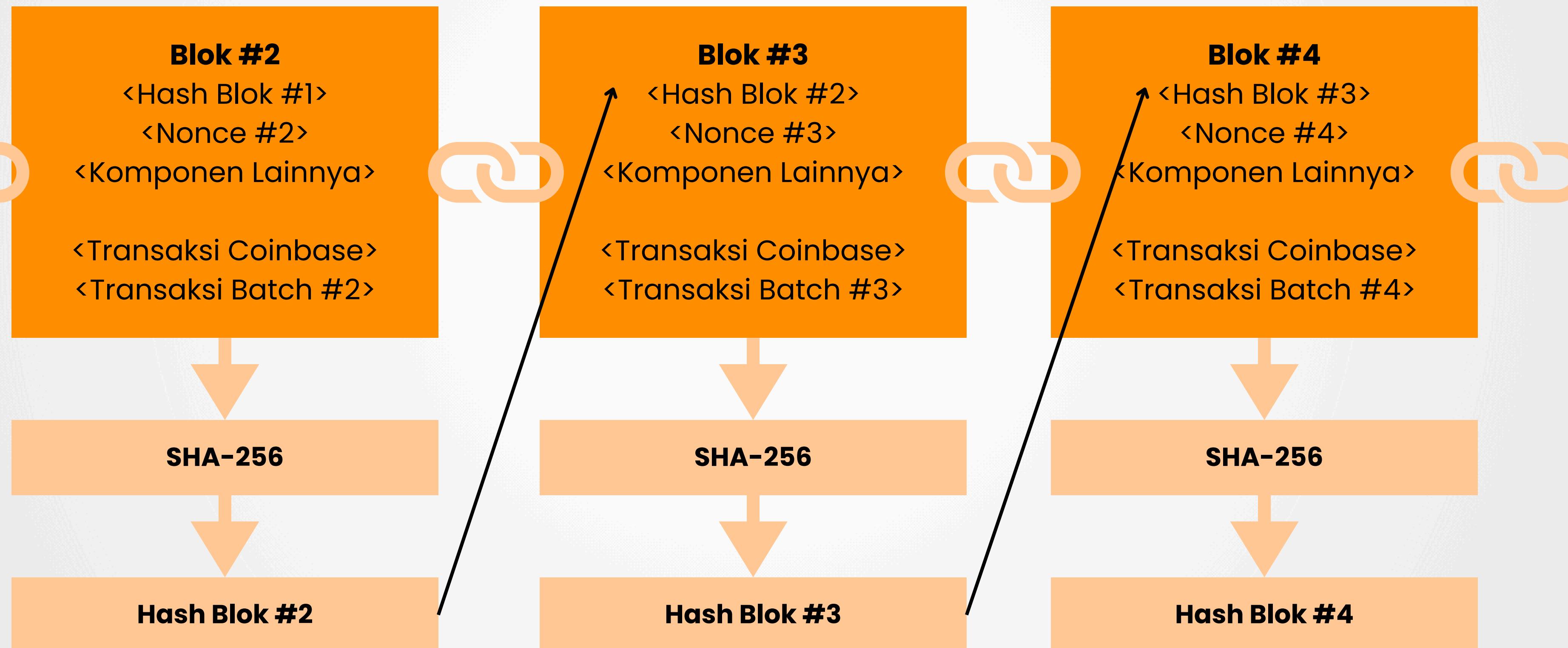
1. Kalimat transaksi dan output ter-screenshot,
2. Tidak ada typo pada kalimat transaksi,
3. Ada jarak enter,
4. Output diawali minimal dua angka 0.



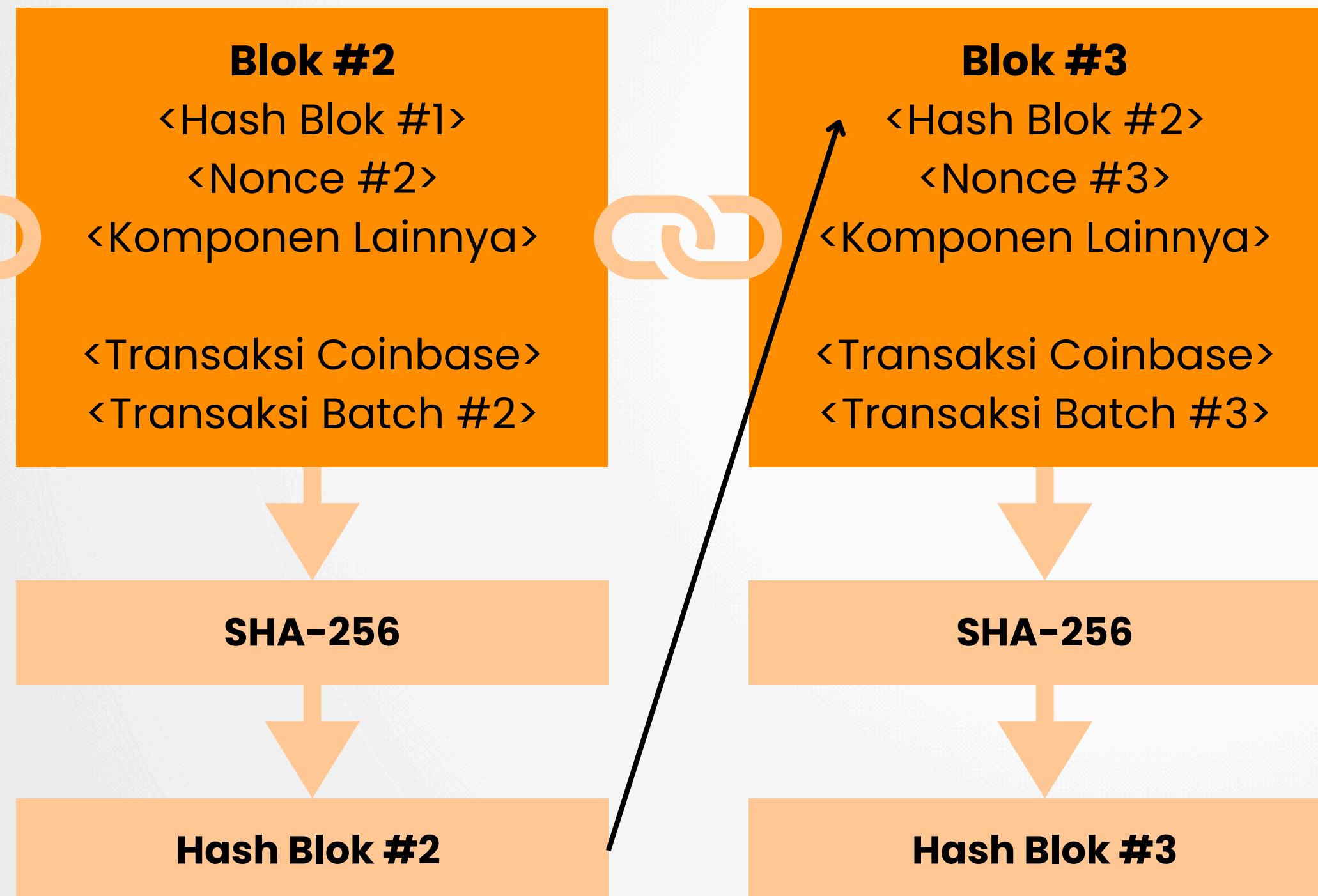
Proof of Work dan Timechain



Struktur Blockchain Bitcoin



Timechain: Riwayat Transaksi yang Hampir Mustahil diubah



Alur Manipulasi:

1. Ada transaksi di **Batch #2** yang dimanipulasi.
2. Output SHA-256 dari **Blok #2** berubah, tidak lagi di bawah *difficulty target*
3. <**Nonce**> **blok #2** harus dicari ulang
4. <**Hash Blok #2**> berubah
5. Output SHA-256 dari Blok #3 karena <**Hash Blok #2**> adalah bagian dari **header blok #3**
6. <**Nonce**> **blok #3** harus dicari ulang
7. Hal ini terus terjadi untuk blok-blok selanjutnya.



Untuk mengubah **Bitcoin**, kita membutuhkan energi yang setara dengan energi yang sudah dikonsumsi para *miner* hingga hari ini sejak **Bitcoin** diciptakan.



Penyesuaian Kesulitan

Bitcoin didesain sedemikian rupa sehingga blok ditambahkan ke *blockchain* tiap rata-rata **10 menit sekali.**

Penyesuaian kesulitan adalah penyesuaian *difficulty target* yang **terjadi setiap 2016 blok (~2 minggu).**



Terima Kasih

