PRELIMINARY POSTMORTEM · BINANCE · 29–30 OKT 2026

~US$6,3 miliar.
~20 menit.

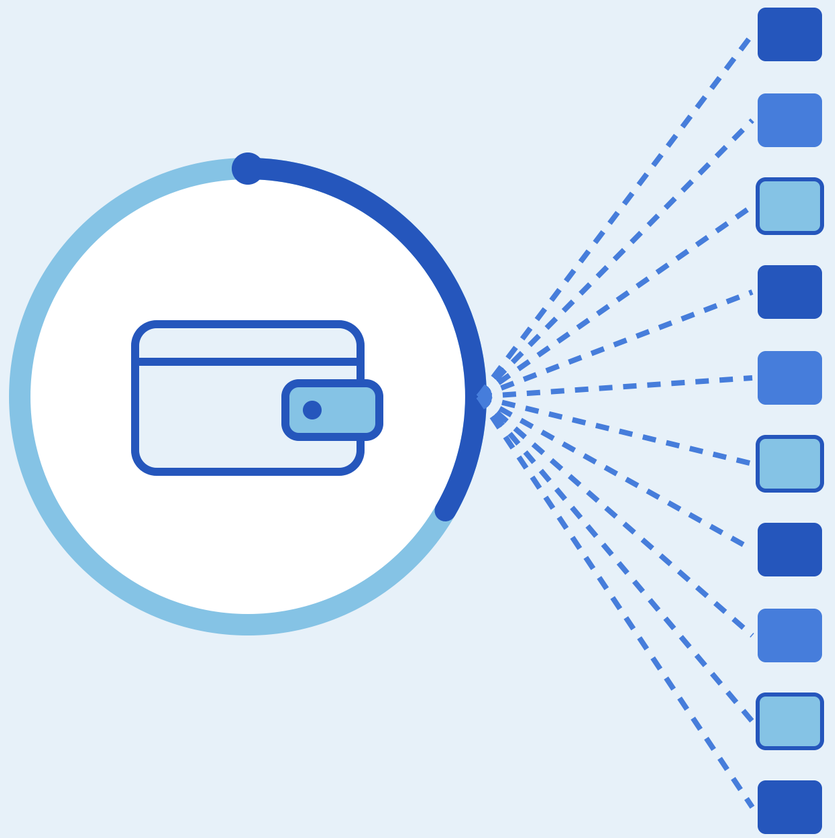
Berapa lama hot wallet kita akan bertahan?

Analisis postmortem sementara untuk direksi, CISO, CTO, tim keamanan siber, dan manajemen risiko

INVESTIGASI BERLANGSUNG · root cause belum dipublikasikan

Angka: estimasi Binance (B) dan analisis on-chain TRM Labs (C) · Batas info: 31 Okt 2026 (UTC)

~20 menit · C (TRM)



10 blockchain

Ilustrasi konseptual

A · Terkonfirmasi · B · Resmi Binance · C · Pihak ketiga · D · Belum diketahui

Insiden ~US$6,3 miliar menguji ketahanan kustodi hot wallet

B · Estimasi

~6,3 miliar US$

Estimasi dampak (Binance, 30 Okt); TRM: 6,36

B · Beku ≠ kembali

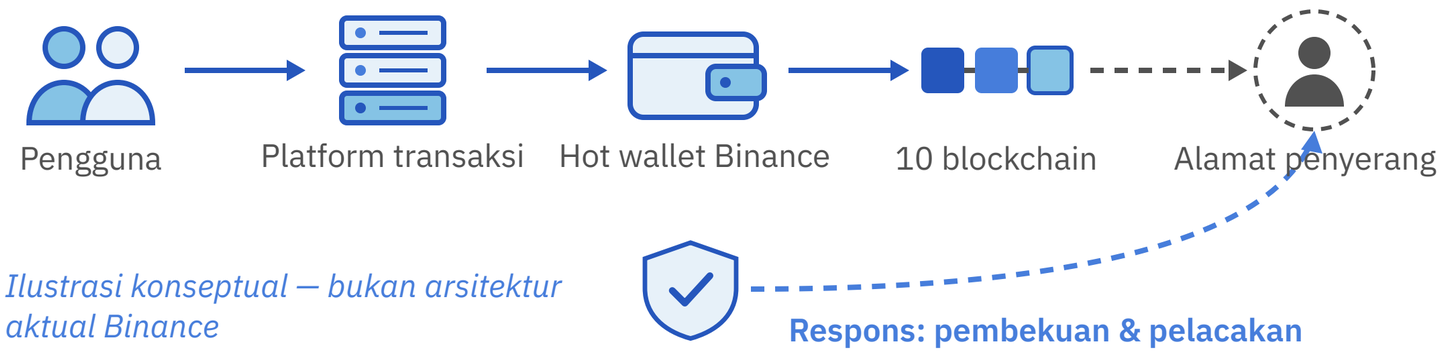
~3 miliar US$

Dibekukan on-chain (Binance); TRM: ~2,7

C · Analisis TRM

~20 menit

Sebagian besar dana keluar dari 10 blockchain



Ilustrasi konseptual — bukan arsitektur aktual Binance

STATUS INVESTIGASI

BERLANGSUNG

Root cause final belum dipublikasikan

Yang diketahui (pernyataan Binance)

- Hot wallet dikompromikan ±20:05 UTC
- Withdrawal ditangguhkan; deposit normal
- Kerugian ditanggung SAFU & kas Binance
- Belum ada bukti private key bocor

Belum terkonfirmasi

- Root cause & urutan serangan penuh
- Atribusi resmi (TRM: DPRK — C)
- Pengembalian aset beku
- Pemulihan withdrawal penuh

TAKEAWAY **Dana ~US$6,3 miliar dapat keluar dalam ~20 menit: kontrol kustodi harus membatasi kerugian bahkan ketika satu jalur akses berhasil ditembus.**

Sumber: Binance Update #1 & #2 (30 Okt) · TRM Labs (29 Okt) · CNBC (30 Okt) · Batas info: 31 Okt 2026 (UTC) · 1/7

A · Terkonfirmasi · B · Resmi Binance · C · Pihak ketiga · D · Belum diketahui

Aset keluar dalam ~20 menit; pembekuan pertama menyusul <1 jam

Semua waktu: UTC

Jendela utama ~20 menit · C (TRM)



28–29 Okt

Persiapan ≥36 jam: dana via Tornado Cash, uji kode di 3 wallet

C · TRM

29 Okt 20:05

Hot wallet dikompromikan; dana mulai keluar

B · Update #2

20:20

Delegasi EIP-7702 di hot wallet ETH; BTC & Tron ikut keluar

C · TRM

21:01–21:04

Tether & Circle bekukan ~US$1,8 mld USDT/USDC

A · On-chain

~22:15

Withdrawal ditangguhkan; insiden diakui publik

B · Waktu: media

30 Okt ±02:23

Update #1: dugaan laptop DevOps; tak ada bukti kunci bocor

B · Update #1

30 Okt 19:33

Update #2: titik breach tambahan; US$6,34 mld disiapkan

B · Update #2

D · Belum diketahui dari sumber publik

Kapan akses awal terjadi · kapan alert internal pertama muncul · lokasi "titik breach tambahan" · root cause

Berikutnya · target Binance, belum terverifikasi

Withdrawal bertahap ~34 jam pasca-Update #2 (≈1 Nov) · hasil PoR 2 Nov · temuan teknis ~48 jam

TAKEAWAY **Eksekusi hanya ~20 menit, tetapi waktu akses awal dan waktu deteksi internal belum diungkap—dua data kunci untuk menilai efektivitas deteksi.**

A · Terkonfirmasi | B · Resmi Binance | C · Pihak ketiga | D · Belum diketahui

Titik masuk diakui; jalur menuju signing masih hipotesis



D · Binance mengakui “titik breach tambahan”; lokasi dan perannya dalam jalur ini belum diungkap.

B · Belum ada bukti private key bocor; Teng: delegasi EIP-7702 melewati kontrol persetujuan normal.

Titik kontrol untuk ditinjau — bukan kegagalan yang terkonfirmasi

Ilustrasi analitis · bukan diagram resmi Binance

1 Keamanan endpoint	2 IAM/PAM & kredensial	3 Workload identity	4 Segmentasi layanan	5 Proteksi signing key
6 Multi-party approval	7 Simulasi transaksi	8 Withdrawal limit	9 Deteksi anomali	10 Kill switch / pause

TAKEAWAY **Yang terkonfirmasi hanyalah ujung jalur—signature valid tereksekusi on-chain; titik masuk dan cara memperoleh otoritas signing masih dugaan.**

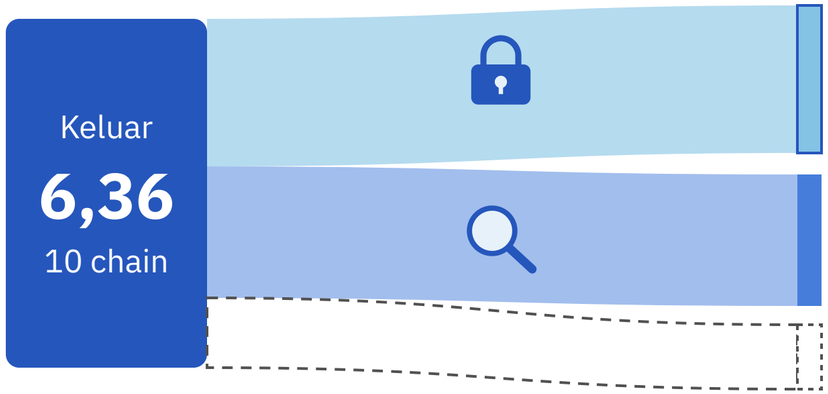
Sumber: Binance Update #1 & #2 · Decrypt & CoinDesk (30 Okt, R. Teng) · TRM Labs (29 Okt) · Batas info: 31 Okt 2026 · 3/7

A · Terkonfirmasi | B · Resmi Binance | C · Pihak ketiga | D · Belum diketahui

Hampir separuh dana dibekukan, tetapi beku belum berarti kembali

Arus dana menurut TRM · miliar US$ · 30 Okt 00:30 UTC

C · Data berkembang

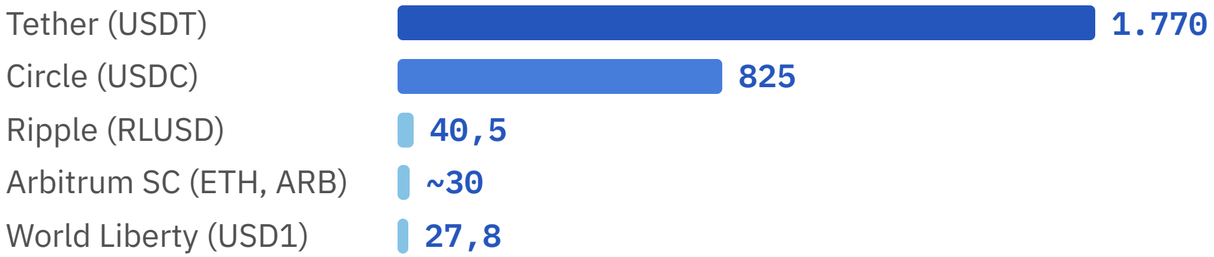


~2,7 dibekukan
Tether, Circle, Ripple, WLFI & Arbitrum SC

~2,4 masih dikuasai
>420 rb ETH & 18.270 BTC; tak bisa dibekukan issuer

Selisih: tidak dirinci (D)

Pembekuan per pihak · juta US$ (TRM, 30 Okt)



Dibekukan ≠ dikembalikan
Pengembalian butuh proses hukum & issuer (TRM)

Cakupan dampak

Finansial · ~US$6,3 mld; Binance siapkan >US$6,34 mld	Estimasi
Pelanggan · withdrawal tertunda; deposit normal	Terkonfirmasi
Operasional · layanan withdrawal dibangun ulang	Terkonfirmasi
Pasar & reputasi · BTC sempat –2%; risiko arus keluar	Potensi
Ekosistem · issuer, Aave, 1inch ikut bekukan/blokir	Terkonfirmasi
Lainnya · dampak per akun, biaya total, sikap regulator	Belum tersedia

TAKEAWAY **Pelanggan menanggung jeda withdrawal; kepercayaan kini bergantung pada PoR & pemulihan aset.**

Sumber: TRM Labs (data 30 Okt 00:30 UTC) · Binance Update #2 · Fox Business/Reuters (30 Okt) · Batas info: 31 Okt 2026 · 4/7

A · Terkonfirmasi | B · Resmi Binance | C · Pihak ketiga | D · Belum diketahui

Respons cepat lintas pihak; pemulihan penuh belum terbukti

Status tindakan: Diumumkan | Sedang berlangsung | Selesai | Belum diketahui *Selesai = tindakan terlaksana, bukan aset kembali*

Pihak	29 Okt · malam (UTC)	30 Okt	31 Okt – 2 Nov · target
Binance	Selidiki insiden; tangguhkan withdrawal di berbagai jaringan Diumumkan	Cabut otorisasi alamat; kontainmen; bangun ulang layanan withdrawal Sedang berlangsung	Target withdrawal bertahap ≈1 Nov; hasil PoR 2 Nov; laporan teknis Belum diketahui
Issuer & mitra blockchain	Tether, Circle, Ripple, WLFI bekukan stablecoin, 21:01–22:26 UTC Selesai	Arbitrum SC amankan ~US$30 jt; Aave bekukan pasar; pelacakan dana Sedang berlangsung	Pengembalian aset beku ke Binance—butuh proses hukum Belum diketahui
Penegak hukum / regulator	Circle bekukan USDC berkoordinasi dengan penegak hukum Diumumkan	Binance bekerja dengan penegak hukum untuk identifikasi pelaku Sedang berlangsung	Atribusi resmi pemerintah & langkah regulator Belum diketahui
Pengguna	Binance: dana pengguna aman; seluruh kerugian ditanggung Diumumkan	Deposit normal; >US$6,34 mld disiapkan, ~80% dalam token sama Sedang berlangsung	Withdrawal pulih penuh & saldo terverifikasi lewat PoR Belum diketahui

TAKEAWAY **Kontainmen cepat lintas pihak; keberhasilan baru terbukti saat withdrawal, PoR & aset pulih.**

Sumber: Binance Update #1 & #2 · TRM Labs (29 Okt) · Cryptopolitan & NBC News (30 Okt) · Batas info: 31 Okt 2026 · 5/7

A · Terkonfirmasi · B · Resmi Binance · C · Pihak ketiga · D · Belum diketahui

Kaji kontrol, bukan orang: 10 area bukti untuk postmortem

L1 · Akses & identitas
Lemah → pijakan internal

→ **L2 · Layanan & workload**
Lemah → jalur ke withdrawal

→ **L3 · Otorisasi transaksi**
Lemah → transaksi tak sah diteken

→ **L4 · Deteksi & respons**
Lemah → kerugian tak terbendung

Lapis	Area kontrol	Pertanyaan postmortem	Bukti yang dibutuhkan	Status bukti publik
L1	Endpoint engineer	Bagaimana laptop dikompromikan; EDR terpicu?	Forensik endpoint, log EDR	Perlu diverifikasi
L1	IAM/PAM & kredensial	Kredensial apa dipakai; ada JIT & MFA kuat?	Log IdP/PAM, sesi istimewa	Belum ada bukti publik
L2	Segmentasi container	Mengapa endpoint bisa menjangkau container?	Peta jaringan, aturan akses	Perlu diverifikasi
L2	Workload identity	Bolehkah container meminta signing bebas?	Kebijakan S2S, token layanan	Belum ada bukti publik
L3	Signing & kunci	Bagaimana signature valid terbit di 10 chain?	Log HSM/MPC & signing policy	Perlu diverifikasi
L3	Multi-party approval	Mengapa delegasi EIP-7702 lolos approval?	Alur kuorum, log approval	Diketahui · B
L3	Batas withdrawal	Mengapa tak ada limit yang menahan arus?	Konfigurasi limit hot wallet	Belum ada bukti publik
L4	Deteksi anomali	Kapan alert pertama vs. transfer 20:05 UTC?	Timeline SIEM/SOC	Belum ada bukti publik
L4	Penghentian darurat	Berapa lama dari deteksi ke penangguhan?	Log keputusan, runbook	Perlu diverifikasi
L4	Tata kelola IR	Pernahkah skenario kompromi signing dilatih?	Laporan tabletop, RACI	Belum ada bukti publik

TAKEAWAY **Fokus review: bukti kontrol sistemik di setiap lapis—bukan mencari individu yang disalahkan.**

A · Terkonfirmasi | B · Resmi Binance | C · Pihak ketiga | D · Belum diketahui

Roadmap 90 hari: batasi dampak meski satu kontrol ditembus

Workstream · owner ** bersyarat investigasi*	0–30 hari Contain & validate	31–60 hari Harden & redesign	61–90 hari Assure & communicate	Indikator · bukti audit
1 Endpoint & identitas CISO · P1	Rotasi kredensial; cabut sesi admin aktif	Admin JIT, MFA phishing-resistant, PAW	Red team jalur endpoint → produksi	0 akses admin permanen · log PAM/IdP
2 Signing & approval Head of Custody · P1	Tolak & pantau delegasi EIP-7702 tak terduga	Signer per chain/tier + kuorum multi-pihak*	Audit independen HSM/MPC & signing policy	100% transaksi > ambang via kuorum · log signer
3 Monitoring & deteksi Head of SOC · P1	Alert real-time arus keluar & delegasi	Velocity limit + simulasi pra-signing*	Uji deteksi berkala; ukur MTTD/MTTC	Target MTTD < 5 menit · laporan uji SIEM
4 IR lintas pihak CISO + Legal · P2	Uji kill switch per wallet; kontak issuer	Playbook freeze bersama issuer & aparat	Tabletop kompromi signing lintas fungsi	Target jeda ke pause < 15 mnt · hasil tabletop
5 Transparansi aset CFO + Comms · P2	Update status berkala ke pelanggan	PoR pasca-insiden + atestasi pihak ketiga	Publikasi postmortem & rencana perbaikan*	PoR terverifikasi · laporan atestasi

3 keputusan direksi

1. Batas kerugian per jam dari hot wallet yang kita terima?
2. Danai signer per chain & kuorum multi-pihak tahun ini?
3. Siapa berwenang menekan kill switch, dalam berapa menit?

TAKEAWAY **Prioritas utama: signing tahan kompromi—signer terpisah, kuorum multi-pihak, limit otomatis.**

Rekomendasi analitis, diturunkan dari slide 2–6 · rujukan: TRM Labs (rekomendasi signing policy) · Batas info: 31 Okt 2026 · 7/7