

Kandungan

•	Tentang Pengarang	6
•	Penafian Risiko Kewangan	7
•	Notis Regulatori Malaysia	8
•	Penafian Maklumat Syariah	9
•	Penafian Teknologi dan Keselamatan	10
•	Pendedahan Kepentingan Pengarang	11
•	Prakata Pengarang	13
•	Cara Menggunakan Buku Ini	14
•	Prasyarat daripada Buku 01	16
•	Peta Pembelajaran	17
•	Not Your Keys, Not Your Coins — Tapi Apa Risikonya?	20

BAHAGIAN I • MEMAHAMI WEB3

01	Daripada Web2 ke Web3	25
02	Ekosistem Ethereum, Solana & Blockchain	31
03	Smart Contracts — Program yang Mengurus Aset	37
04	Layer 1, Layer 2 & Skalabiliti Blockchain	44

BAHAGIAN II • DIGITAL WALLET & SELF-CUSTODY

05	Custodial vs Non-Custodial Wallet	52
06	Panduan Lengkap MetaMask	61
07	Phantom, Solana & Hardware Wallet	68
08	Gas Fee, Transaksi & Block Explorer	74
09	Signature, Approval & Permission	82

BAHAGIAN III • MENGGUNAKAN WEB3

10	Memindahkan Aset daripada CEX ke Wallet	93
11	Connect Wallet & Memahami dApps	100
12	Decentralized Exchange (DEX) & Token Swap	106
13	Slippage, Price Impact & MEV	113
14	Blockchain Bridge & Wrapped Token	120

BAHAGIAN IV • DECENTRALIZED FINANCE

15	Liquidity Pool & Automated Market Maker	128
----	---	-----

16	Impermanent Loss – Pendapatan atau Kerugian?	136
17	DeFi Lending & Borrowing	144
18	Stablecoin, Staking & DeFi Yield	153
19	DAO, Governance, Tokenisasi & Real-World Assets	163

BAHAGIAN V • KESELAMATAN, SYARIAH & MALAYSIA

20	Web3 Scams, Wallet Drainers & Rug Pulls	170
21	Risiko Smart Contract & Due Diligence Protokol	179
22	Web3 & DeFi dari Perspektif Syariah	186
23	Peraturan Web3, Cukai & Pertimbangan Malaysia	194

BAHAGIAN VI • PENGUASAAN WEB3 PRAKTIKAL

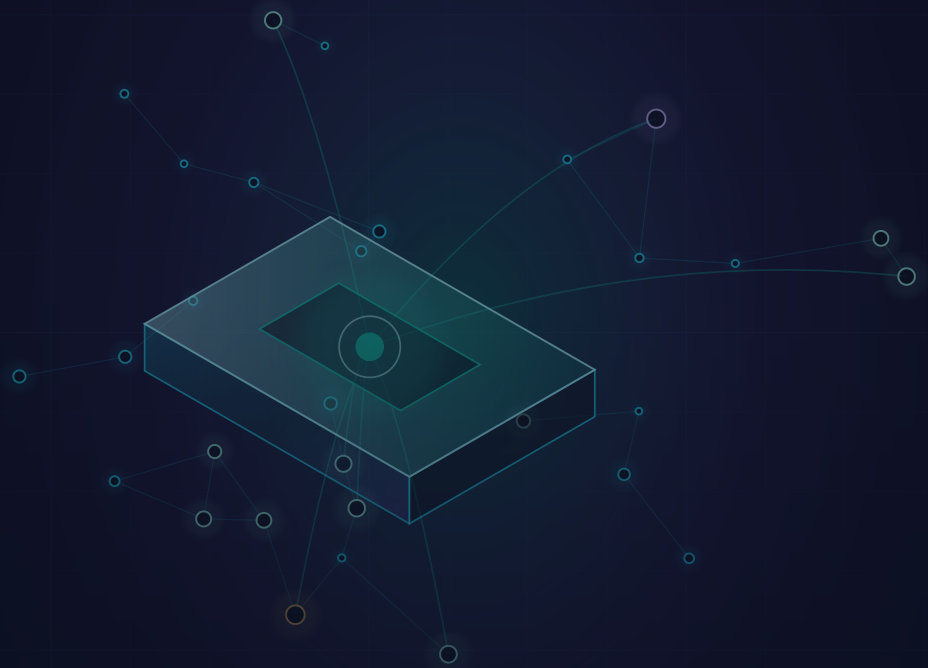
24	Makmal Web3 Hands-On	201
25	Enam Kajian Kes Web3 & DeFi	211
26	Pelan Pembelajaran Web3 30 Hari	218

LAMPIRAN & RUJUKAN

A	Glosari Web3 & DeFi A–Z	229
B	Senarai Semak Keselamatan Wallet	238
C	Senarai Semak MetaMask untuk Pemula	240
D	Senarai Semak Phantom untuk Pemula	242
E	Senarai Semak Penilaian Hardware Wallet	244
F	Perbandingan Rangkaian Blockchain	246
G	Buku Kerja Pengiraan Gas Fee	249
H	Senarai Semak Kebenaran Smart Contract	252
I	Templat Audit Token Approval	254
J	Buku Kerja Pengiraan Swap DEX	256
K	Lembaran Kerja Liquidity Pool dan Impermanent Loss	258
L	Kalkulator Health Factor Lending DeFi	261
M	Penilaian Risiko Stablecoin	265
N	Kad Skor Due Diligence Protokol	268
O	Senarai Semak Semakan Syariah DeFi	270
P	Templat Rekod Transaksi Malaysia	272
Q	Penjejak Pembelajaran 30 Hari	274
R	Soalan Lazim (FAQ) Web3	276
S	Sumber Rasmi dan Bacaan Lanjut	282
T	Pratonton Buku 04 dan Buku 05	284
•	Rujukan & Sumber Disahkan	286

Memahami Web3

Daripada Web2 ke Web3, ekosistem Ethereum dan Solana, smart contract, serta Layer 1 dan Layer 2 — di mana desentralisasi benar-benar wujud dan di mana perantara masih ada.



BAB 01 Daripada Web2 ke Web3

BAB 02 Ekosistem Ethereum, Solana & Blockchain

BAB 03 Smart Contracts — Program yang Mengurus Aset

BAB 04 Layer 1, Layer 2 & Skalabiliti Blockchain

BAB 01

BAHAGIAN I • MEMAHAMI WEB3

Daripada Web2 ke Web3

Web3 memindahkan kawalan daripada platform kepada pengguna — tetapi tidak semua perantara hilang, dan tidak semua kawalan itu percuma.

Pada pagi Isnin, Iman (watak rekaan), pereka grafik berusia 27 tahun di Kota Kinabalu, terlupa kata laluan aplikasi bank. Dalam sepuluh minit, identitinya disahkan dan kata laluan baharu ditetapkan. Petang itu, rakan sepejabat menunjukkan wallet crypto di telefonnya dan berkata, "Ini Web3. Tiada bank, tiada orang tengah. Aset kau, kawalan kau."

Iman tertanya-tanya. Jika tiada orang tengah, siapa yang menetapkan semula akses jika dia terlupa seed phrase? Siapa yang menjalankan laman web tempat dia menekan butang "swap"? Dan stablecoin yang dikatakan "sama dengan dolar" — siapa yang menjamin nilainya? Bab ini membina peta jujur: di mana desentralisasi benar-benar wujud, dan di mana perantara masih memegang peranan.

© OBJEKTIF PEMBELAJARAN

- | | |
|---|--|
| 01 Membezakan Web1, Web2 dan Web3 berdasarkan siapa yang memegang data dan kawalan. | 04 Mengenal pasti perantara yang masih wujud dalam Web3: penyedia RPC, frontend, penerbit stablecoin dan sequencer. |
| 02 Menerangkan perbezaan seni bina client-server dengan dApp. | 05 Menyenaraikan had utama Web3 sebelum anda mengambil tanggungjawab mengawal aset sendiri. |
| 03 Membandingkan aplikasi perbankan, exchange berpusat, self-custody wallet dan dApp dari segi kawalan, pemulihan dan perantara. | |

01.1 Tiga era web: baca, tulis, miliki

Rajah 1.1 meringkaskan evolusi web dalam tiga era yang bertindih. Web1 ialah era laman statik: kebanyakan pengguna hanya membaca. Web2 membawa platform interaktif — media sosial, e-dagang, perbankan dalam talian — di mana pengguna menulis dan berkongsi, tetapi akaun, data dan rekod disimpan dalam pelayan syarikat. Web3 menambah lapisan ketiga: pengguna boleh memegang aset digital dan berinteraksi dengan program awam menggunakan wallet sebagai identiti.

TIGA ERA WEB • ERA BERTINDIH



RAJAH 1.1 — Evolusi Web1 ke Web3. Web3 menambah lapisan pemilikan dan kawalan aset, tetapi tidak menggantikan sepenuhnya infrastruktur Web2. [EZX3-001]

Perkataan "bertindih" penting. Web3 tidak menggantikan Web2; ia dibina di atasnya. Anda masih menggunakan pelayar, sambungan internet, kedai aplikasi dan laman web yang dihoskan syarikat untuk sampai ke blockchain. Yang berubah ialah lapisan rekod dan kawalan aset.

► DALAM SIRI EZYKRIPTO

Buku 01, Bab 03 (Blockchain Tanpa Pening Kepala) dan Bab 05 (Wallet, Private Key dan Pemilikan Aset) memberi asas blockchain dan kunci yang diandaikan dalam bab ini.

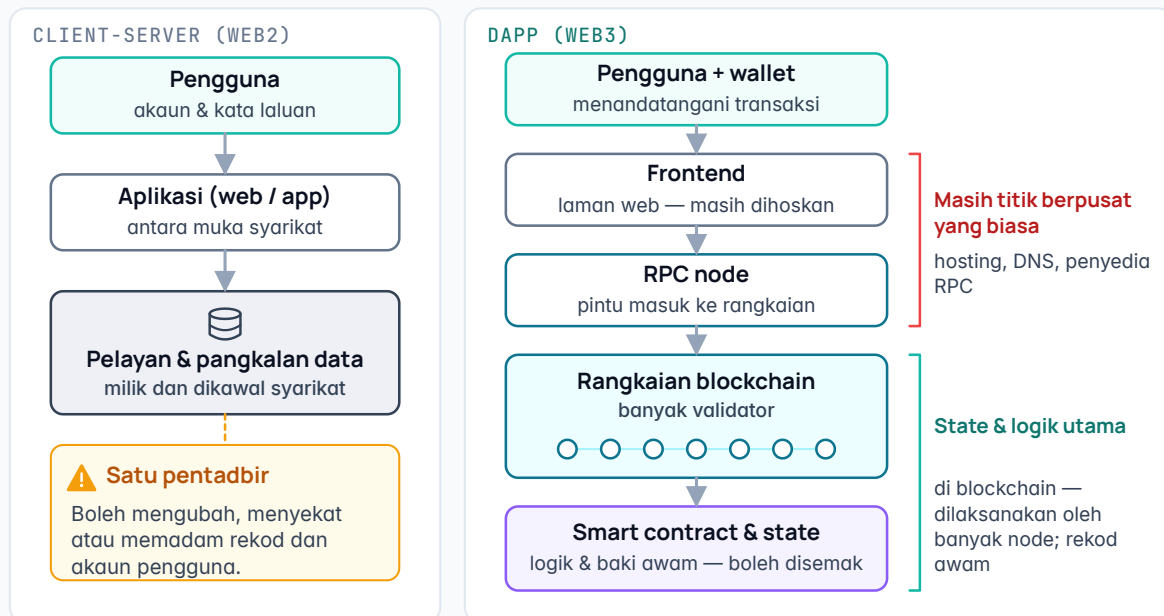
◆ DEFINISI TEKNIKAL

Istilah Asas Web3

Web1 — era laman web statik yang kebanyakannya untuk dibaca. **Web2** — model internet berasaskan platform, di mana syarikat menyimpan akaun dan data pengguna dalam pelayan sendiri. **Web3** — model di mana rekod aset dan logik aplikasi berada di blockchain awam, dan pengguna mengawalinya melalui wallet. **Client-server** — seni bina di mana aplikasi pengguna (client) meminta data daripada pelayan yang dikawal satu pentadbir. **dApp** — aplikasi yang logik dan state utamanya berada dalam smart contract di blockchain, biasanya diakses melalui laman web. **Permissionless** — sesiapa boleh menggunakan atau membina tanpa meminta kebenaran pihak pusat. **Censorship resistance** — sukar bagi satu pihak untuk menyekat transaksi yang sah. **Intermediary (perantara)** — pihak ketiga yang memegang, memproses atau mengesahkan sesuatu bagi pihak anda. **Composability** — keupayaan smart contract memanggil dan menggabungkan contract lain seperti blok binaan.

01.2 Client-server lawan dApp

Dalam aplikasi Web2, seperti dalam **Rajah 1.2** (kiri), telefon anda menghantar permintaan kepada pelayan syarikat. Pelayan menyemak pangkalan data, mengemas kini baki, dan membalas. Satu pentadbir boleh membetulkan kesilapan, membekukan akaun atau mengubah rekod. Ini bukan semestinya buruk — kebolehan membetulkan kesilapan ialah perlindungan pengguna yang bernilai.



RAJAH 1.2 — Seni Bina Berpusat vs Terdesentralisasi. Dalam dApp, state dan logik utama berada di blockchain, tetapi frontend dan RPC sering masih berpusat. [EZK3-002]

Dalam dApp (kanan), wallet anda menandatangani transaksi, sebuah node RPC menyiarkannya ke rangkaian, dan validator memasukkannya ke dalam blok. Logik dijalankan oleh smart contract yang sama untuk semua pengguna. Sesiapa boleh menerbitkan contract tanpa kebenaran [ETH-024], dan contract lain boleh memanggilnya — inilah composability. Kelebihan ini juga risiko: jika satu contract yang dipanggil gagal, kesannya boleh merebak kepada protokol lain yang bergantung padanya.

Perhatikan anotasi merah dalam **Rajah 1.2**: state dan logik berada di blockchain, tetapi pintunya — laman web dan node RPC — selalunya masih dikendalikan syarikat.

01.3 Empat cara memegang dan menggunakan aset

Perbezaan utama antara empat model dalam jadual berikut bukan teknologi, tetapi siapa yang mengawal kebenaran transaksi dan siapa yang boleh membetulkan kesilapan.

ASPEK	APLIKASI BANK	EXCHANGE BERPUSAT (CEX)	SELF-CUSTODY WALLET	DAPP
Siapa mengawal kebenaran	Bank	Exchange (custody)	Anda, melalui private key	Anda menandatangani; contract melaksanakan
Rekod baki	Pangkalan data bank	Lejar dalaman exchange	Blockchain	State contract di blockchain
Lupa akses	Bank tetapkan semula	Exchange pulihkan selepas pengesahan	Bergantung sepenuhnya pada sandaran anda	Bergantung pada wallet anda
Salah hantar	Ada saluran aduan	Pengeluaran on-chain muktamad	Muktamad	Muktamad, ikut logik contract
Perantara kekal	Bank, rangkaian pembayaran	Exchange, bank untuk RM	Pembuat wallet, penyedia RPC	Frontend, RPC, penerbit stablecoin, admin contract

Dalam self-custody, pembuat wallet tidak memegang aset anda, dan anda bertanggungjawab sepenuhnya menjaga kunci [ETH-058]. Transaksi di blockchain tidak boleh diterbalikkan, dan tiada perkhidmatan sah akan

meminta seed phrase anda [ETH-059]. Itulah harga kawalan langsung.

RM MYR EXAMPLE

Kesilapan yang sama, akibat berbeza

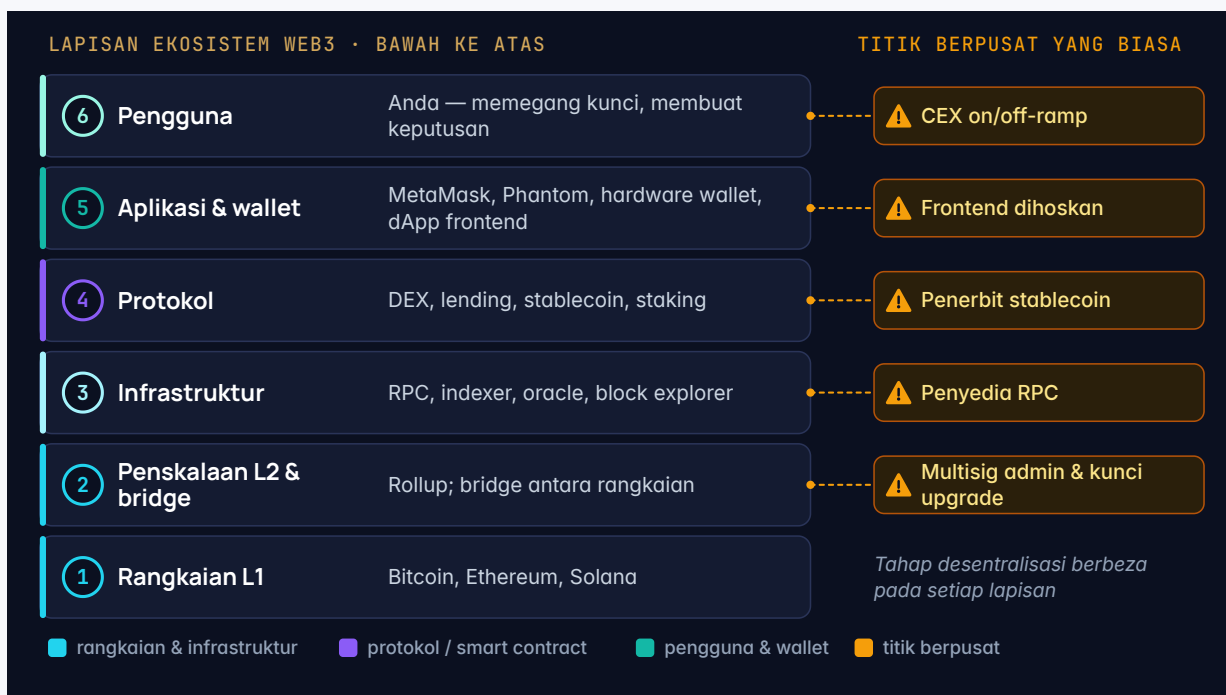
Andaian (hipotetikal): ETH = RM12,600; gas pindahan ringkas $21,000 \times 10$ gwei.

- **Bank:** Iman tersalah taip nombor akaun dan menghantar RM504. Dia boleh membuat aduan kepada bank; pemulihan tidak dijamin, tetapi ada pihak yang boleh menyiasat.
- **Self-custody:** Iman menghantar 0.04 ETH ($\approx$ RM504) ke alamat yang salah dan membayar gas 0.00021 ETH ($\approx$ RM2.65). Selepas transaksi muktamad, tiada pihak yang boleh membatalkannya. Jumlah terdedah $\approx$ RM506.65.

Pengajaran: Jumlah yang sama, tetapi dalam self-custody, tanggungjawab menyemak alamat dan rangkaian terletak sepenuhnya pada anda. Gas juga dibayar walaupun transaksi itu satu kesilapan.

01.4 Di mana desentralisasi wujud, di mana perantara kekal

Rajah 1.3 melihat Web3 sebagai timbunan lapisan. Desentralisasi paling kukuh biasanya berada di lapisan bawah: konsensus blockchain yang dijalankan oleh ramai validator, dan smart contract yang kodnya terbuka dan berkelakuan sama untuk semua. Semakin ke atas, semakin banyak pihak berpusat yang muncul.



RAJAH 1.3 — Peta Ekosistem Web3. Web3 ialah timbunan lapisan; tahap desentralisasi berbeza pada setiap lapisan. [EZX3-003]

Penyedia RPC. Wallet perlu bercakap dengan blockchain melalui node RPC, dan kebanyakan pengguna bergantung pada penyedia lalai yang dikendalikan syarikat. Penyedia boleh mengalami gangguan, mengehadkan permintaan atau melihat alamat IP anda. Solana sendiri menyatakan endpoint RPC awamnya dihadkan kadar dan tidak bertujuan untuk kegunaan produksi [SOL-052].

Frontend. Laman web dApp ialah perisian syarikat yang berasingan daripada protokol. Uniswap Labs, misalnya, pernah mengenakan yuran antara muka pada laman webnya sendiri — yuran yang boleh dielakkan melalui antara muka lain kerana ia bukan sebahagian daripada contract protokol [DFI-024, DFI-017]. Frontend juga boleh dirampas: pada Ogos 2022, DNS laman Curve dirampas dan laman tiruan meminta pengguna meluluskan contract berniat jahat, sedangkan contract Curve sendiri tidak terjejas [SEC-030]. Bab 11 membincangkannya.

Penerbit stablecoin. USDC dan USDT ialah token yang diterbitkan syarikat. Contract kedua-duanya mempunyai fungsi senarai hitam dan jeda, dan terma penerbit membenarkan mereka menyekat atau membekukan token pada alamat tertentu [STB-003, STB-005, STB-014, STB-016]. Penerbit juga menentukan di mana token ditebus: Tether

tidak lagi menebus USDT pada beberapa rangkaian lama, dan Circle tidak menebus USDC yang dibridge oleh pihak ketiga [L2B-063, L2B-048]. Maksudnya, self-custody melindungi anda daripada kegagalan platform, tetapi bukan daripada tindakan penerbit. Bab 18 menghuraikannya.

Sequencer dan admin contract. Banyak Layer 2 bergantung pada satu sequencer; dokumentasi Arbitrum sendiri menyatakan sequencernya masih berpusat (disemak Oktober 2026) [L2B-025]. Contract yang boleh dinaik taraf pula bermaksud pemegang kunci admin boleh mengubah logiknya; satu alamat pemilik ialah titik kegagalan tunggal [ETH-025, ETH-026].

↔ REALITY CHECK

Naratif: "Web3 tiada orang tengah." **Realiti:** Web3 mengurangkan pergantungan pada perantara di lapisan rekod dan penyelesaian, tetapi penyedia RPC, frontend, penerbit stablecoin, sequencer, pemegang kunci admin dan exchange untuk tukaran RM masih wujud. Soalan yang lebih tepat: perantara mana yang anda percayai, dan apa yang mereka boleh lakukan terhadap aset anda?

Peta ini bukan untuk menakutkan anda, tetapi supaya anda menilai setiap lapisan secara berasingan dan tidak menerima label "terdesentralisasi" untuk keseluruhan sistem.

× COMMON MISTAKE

Menganggap laman dApp sama dengan protokol

Salah faham: "Saya guna laman rasmi, jadi saya berinteraksi terus dengan blockchain yang terdesentralisasi."

Kenapa berbahaya: Laman web boleh dipalsukan, dirampas atau diubah untuk meminta tandatangan berniat jahat, walaupun contract protokol itu sendiri tidak berubah. **Cara elak:** Anggap frontend sebagai lapisan berasingan. Semak alamat laman, baca apa yang wallet minta anda tandatangani, dan fahami perbezaan connect, sign dan approve (Bab 09).

01.5 Had Web3 yang perlu diakui

Skalabiliti dan kos. Blockchain awam mempunyai ruang blok terhad, jadi yuran naik ketika sesak. Layer 2 dan blockchain berkapasiti tinggi cuba menyelesaikannya dengan pertukaran tersendiri (Bab 04).

Finaliti dan kebolehpercayaan. Di Ethereum, blok mengambil kira-kira 15 minit untuk dimuktamadkan [ETH-008]. Rangkaian juga boleh terganggu: Solana mencatatkan beberapa henti operasi antara 2021 dan Februari 2024 [SOL-059, SOL-061], dan sequencer Base pernah terhenti kira-kira 33 minit pada Ogos 2025 [L2B-035].

Pengalaman pengguna. Alamat panjang, pilihan rangkaian, gas dalam token asli dan mesej tandatangan yang teknikal memudahkan kesilapan — dan kebanyakannya tidak boleh dibatalkan.

Keselamatan dan penipuan. Apabila tiada pihak boleh membekukan transaksi untuk anda, penipu menyasarkan anda secara langsung melalui phishing, laman palsu dan tandatangan berniat jahat (Bab 20).

Undang-undang. Label "terdesentralisasi" tidak memberi pengecualian daripada undang-undang sekuriti, anti-pengubahan wang haram atau cukai. Bab 23 membincangkan pertimbangan Malaysia.

🛡️ WALLET SECURITY

Tiada butang "lupa kata laluan"

Ancaman: Seed phrase hilang, dicuri atau diberikan kepada "khidmat pelanggan" palsu. **Akibat:** Dalam self-custody, tiada pihak yang boleh menetapkan semula akses atau membalikkan pindahan [ETH-059]. **Kawalan:**

Simpan seed phrase di luar talian, jangan menaipnya ke laman web atau menghantar gambarnya, dan mulakan dengan jumlah kecil (Bab 05).

● RINGKASAN BAB

5 Perkara Utama

1. Web3 dibina di atas Web2; yang berubah ialah lapisan rekod dan kawalan aset, bukan seluruh internet.

2. Dalam dApp, state dan logik berada di blockchain, tetapi frontend dan RPC sering masih berpusat.
3. Bank dan CEX boleh menetapkan semula akses dan menyiasat kesilapan; dalam self-custody, tanggungjawab itu sepenuhnya milik anda.
4. Perantara kekal dalam Web3: penyedia RPC, frontend, penerbit stablecoin, sequencer dan pemegang kunci admin.
5. Had Web3 termasuk skalabiliti, finaliti, pengalaman pengguna, penipuan dan undang-undang yang tetap terpakai.

5 Soalan Ulang Kaji

1. Apakah perbezaan utama antara Web2 dan Web3 dari segi siapa yang menyimpan rekod?
2. Kenapa dApp masih boleh terjejas walaupun smart contract tidak berubah?
3. Dalam jadual empat model, model manakah yang tiada pihak boleh menetapkan semula akses anda?
4. Namakan tiga perantara yang masih wujud apabila anda menggunakan dApp.
5. Kenapa label "terdesentralisasi" tidak bermaksud bebas daripada undang-undang?

Latihan Praktikal

Latihan kertas, tanpa dana. Pilih satu aplikasi bank, satu exchange yang anda guna dan satu dApp yang anda pernah dengar. Untuk setiap satu, tulis: siapa mengawal kebenaran transaksi, di mana rekod baki disimpan, apa berlaku jika anda hilang akses, dan sekurang-kurangnya dua perantara yang terlibat. Bandingkan jawapan anda dengan [Rajah 1.3](#).

→ SETERUSNYA

Web3 bukan satu rangkaian, tetapi ekosistem blockchain dengan seni bina berbeza. Bab 02 membandingkan Bitcoin, Ethereum, Solana dan rangkaian EVM lain — dan menerangkan kenapa alamat yang sama tidak bermaksud aset yang sama.

Ekosistem Ethereum, Solana & Blockchain

Alamat yang sama tidak bermakna baki yang sama — setiap blockchain mempunyai peraturan, aset asli dan rekodnya sendiri.

Mei Ling (watak rekaan), juruteknik makmal di Ipoh, baru sahaja mengeluarkan 0.05 ETH dari exchange ke wallet barunya. Exchange menunjukkan status "Selesai", tetapi wallet memaparkan baki 0 ETH. Selepas setengah jam panik, Mei Ling perasan pilihan rangkaian pengeluaran tadi ialah Arbitrum One, sedangkan wallet sedang memaparkan Ethereum Mainnet. Sebaik sahaja rangkaian ditukar, 0.05 ETH itu muncul.

Pada minggu yang sama, seorang kawan meminta "alamat Solana" untuk menghantar token, dan Mei Ling hampir memberikan alamat 0x... yang sama. Dua kejadian kecil ini menunjukkan perkara yang sering terlepas pandang: blockchain bukan satu sistem tunggal. Bitcoin, Ethereum, Solana dan puluhan rangkaian serasi EVM masing-masing mempunyai model transaksi, aset asli, format alamat dan rekod baki sendiri.

© OBJEKTIF PEMBELAJARAN

- | | |
|---|---|
| 01 Menerangkan validator, consensus, finality, native asset, chainId, serta beza token dan coin. | 04 Membandingkan Bitcoin, Ethereum, Solana dan rangkaian EVM terpilih dari segi seni bina, keupayaan, aset asli dan had. |
| 02 Membezakan model UTXO Bitcoin dengan model akaun Ethereum dan Solana. | 05 Menjelaskan mengapa satu alamat EVM mempunyai baki berbeza pada setiap rangkaian. |
| 03 Menerangkan maksud EVM dan mengapa banyak rangkaian berkongsi format alamat yang sama. | |

02.1 Bahasa asas sesebuah blockchain

Buku 01 (Bab 03 dan Bab 04) telah menerangkan blockchain sebagai lejar yang dikongsi dan disahkan bersama, serta memperkenalkan Bitcoin, Ethereum dan altcoin. Bab ini melangkah setapak lagi: apabila anda mengawal wallet sendiri, anda perlu tahu *rantaian mana* yang sedang anda gunakan, kerana setiap rantai membuat pertukaran (trade-off) berbeza antara keselamatan, keupayaan dan kelajuan.

◆ DEFINISI TEKNIKAL

Istilah Ekosistem

- **Validator** — peserta yang mencadangkan dan mengesahkan blok, lazimnya dengan mempertaruhkan aset asli.
- **Consensus** — peraturan yang membolehkan node bersetuju tentang susunan transaksi dan keadaan terkini.
- **Finality** — tahap di mana transaksi tidak lagi boleh diterbalikkan secara munasabah; probabilistik atau berasaskan checkpoint.
- **Native asset (coin)** — aset asli untuk membayar yuran rangkaian, contohnya BTC, ETH dan SOL.
- **Token** — aset yang direkodkan oleh smart contract atau program, bukan oleh protokol asas.

- **EVM (Ethereum Virtual Machine)** — persekitaran pelaksanaan smart contract Ethereum, turut digunakan rangkaian lain; selebihnya disebut *non-EVM*.
- **chainId** — nombor pengenalan rangkaian EVM yang dimasukkan ke dalam transaksi bertandatangan.

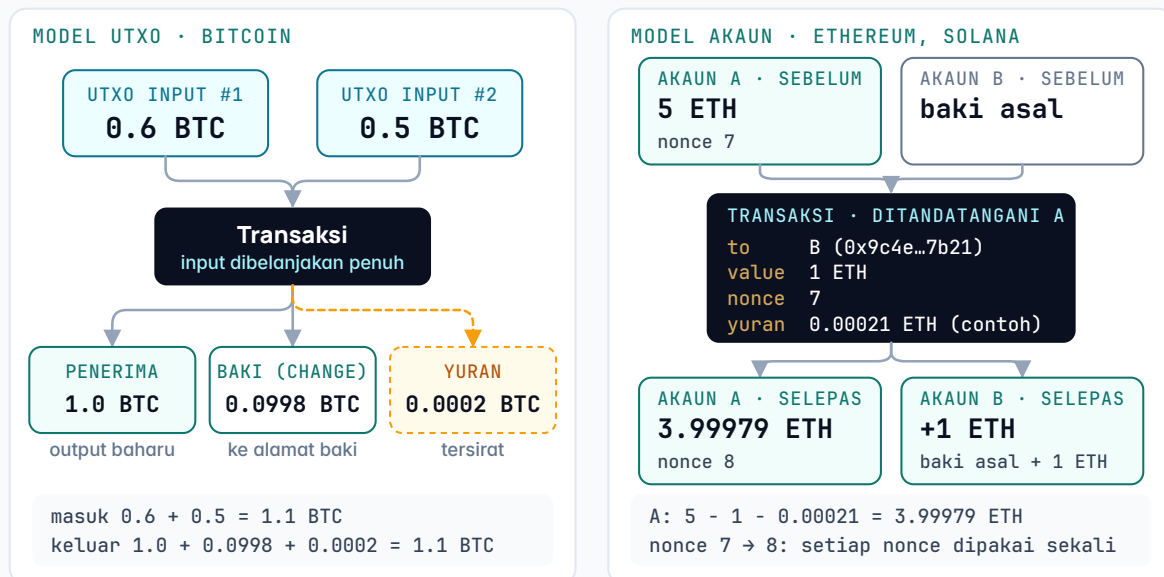
Perbezaan coin dan token amat praktikal. ETH di Ethereum ialah native asset yang direkodkan dalam baki akaun dan diperlukan untuk gas. USDC di Ethereum pula ialah token: bakinya dicatat dalam contract USDC. Anda boleh memegang 1,000 USDC tetapi masih gagal menghantarnya jika tiada ETH untuk membayar yuran.

02.2 Bitcoin: model UTXO dan finaliti probabilistik

Bitcoin tidak menyimpan "baki akaun". Ia menjejak *unspent transaction outputs* (UTXO), iaitu output transaksi terdahulu yang belum dibelanjakan. Setiap transaksi baharu merujuk UTXO sebagai input; UTXO hanya boleh dibelanjakan sekali, jadi nilai penuhnya mesti pergi ke output baharu atau yuran, dengan baki dikembalikan melalui output baki (*change*). Baki wallet Bitcoin anda sebenarnya jumlah semua UTXO yang dikawal oleh kunci anda [SOL-054].

Rajah 2.1 membandingkan kedua-dua model. Di sebelah kiri, dua UTXO 0.6 BTC dan 0.5 BTC digabungkan untuk membayar 1.0 BTC; 0.0998 BTC kembali ke alamat baki dan 0.0002 BTC menjadi yuran tersirat. Di sebelah kanan, model akaun hanya menolak baki dan menaikkan nonce.

NOMBOR ILUSTRASI • DUA CARA MENJEJAK NILAI



Contoh Hipotetikal — nombor ilustrasi, bukan data pasaran

RAJAH 2.1 — Model Akaun Blockchain: UTXO vs Akaun. Bitcoin menjejak output yang belum dibelanjakan; Ethereum dan Solana menjejak baki akaun. [EZX3-005]

Bahasa skrip Bitcoin sengaja direka terhad dan tidak *Turing complete* [SOL-054]. Ini mengurangkan permukaan serangan tetapi menghadkan aplikasi kompleks seperti AMM atau pinjaman. Blok dihasilkan melalui proof of work pada purata kira-kira 10 minit, dengan kesukaran diselaraskan setiap 2,016 blok [SOL-055]. Finality Bitcoin adalah probabilistik: transaksi tidak menjadi muktamad serta-merta, dan bitcoin.org mencadangkan sekurang-kurangnya enam pengesahan bagi pindahan bernilai tinggi [SOL-056].

02.3 Ethereum dan EVM: akaun, contract dan chainId

Ethereum menggunakan model akaun. Terdapat dua jenis akaun: *externally owned account* (EOA) yang dikawal oleh private key, dan akaun contract yang dikawal oleh kod dan tidak mempunyai private key [ETH-003]. Setiap akaun menyimpan nonce, baki dalam wei (1 ETH = 10^{18} wei) dan, bagi contract, kod serta storan [ETH-003, ETH-007]. Alamat EOA ialah 0x diikuti 40 aksara heksadesimal yang diterbitkan daripada public key [ETH-003].

Ethereum beralih daripada proof of work kepada proof of stake melalui The Merge pada 15 September 2022 [ETH-001]. Masa dibahagikan kepada slot 12 saat, dan setiap epoch mengandungi 32 slot [ETH-005]. Blok mencapai finality apabila checkpoint mendapat undian sekurang-kurangnya dua pertiga ETH yang dipertaruhkan; ethereum.org menganggarkan proses ini mengambil kira-kira 15 minit [ETH-005, ETH-008].

Kepentingan Ethereum bagi buku ini juga terletak pada EVM. Kerana banyak rangkaian lain melaksanakan EVM, smart contract dan wallet yang sama boleh digunakan merentasinya dengan format alamat yang sama. Setiap rangkaian dibezakan oleh chainId: Ethereum Mainnet ialah 1, OP Mainnet 10, BNB Smart Chain 56, Polygon PoS 137, Base 8453 dan Arbitrum One 42161 [ETH-055]. EIP-155 memasukkan chainId ke dalam tandatangan transaksi supaya transaksi yang ditandatangani untuk satu rangkaian tidak sah di rangkaian lain [ETH-011].

02.4 Solana: model akaun dengan program tanpa state

Solana juga menggunakan model akaun, tetapi strukturnya berbeza daripada Ethereum. State global Solana ialah stor kunci-nilai: setiap alamat 32 bait menunjuk kepada satu akaun yang menyimpan lamports, data, pemilik (*owner*) dan penanda sama ada ia boleh dilaksanakan [SOL-001]. Alamat lazimnya dipaparkan dalam format base58, bukan heksadesimal 0x [SOL-026]. Unit terkecil ialah lamport: 1 SOL = 1,000,000,000 lamports [SOL-025].

Smart contract di Solana dipanggil *program* dan tidak menyimpan state sendiri, manakala setiap token yang anda pegang berada dalam token account tersendiri [SOL-004, SOL-027] — butirannya dalam Bab 03 dan Bab 07. Yuran asas ialah 5,000 lamports setiap tandatangan, separuh dibakar dan separuh kepada validator, ditambah priority fee pilihan [SOL-002].

Solana sedang berubah dengan pantas. Sejak 9 Oktober 2026, sasaran masa slot ialah 200 ms, berbanding 400 ms sebelumnya [SOL-008]. Pada tarikh rujukan buku ini (20 Oktober 2026), consensus masih berasaskan Proof of History dan TowerBFT, dengan finality kira-kira 12.8 saat. Sehari kemudian, pada 21 Oktober 2026, mainnet beralih kepada Alpenglow (Votor), yang menyasarkan finality sekitar 150 ms — satu sasaran, bukan jaminan — dan pengguna tidak perlu mengambil sebarang tindakan [SOL-007].

Kelajuan juga bukan satu-satunya ukuran. Solana merekodkan beberapa gangguan rangkaian, termasuk kira-kira 17 jam pada September 2021 dan kira-kira lima jam pada Februari 2024, walaupun tiada insiden kluster mainnet disenaraikan selepas itu sehingga Oktober 2026 [SOL-061, SOL-060, SOL-059].

02.5 Perbandingan Bitcoin, Ethereum, Solana dan rangkaian EVM

Rajah 2.2 meringkaskan tiga rangkaian utama setakat Oktober 2026, termasuk peralihan Solana kepada Alpenglow pada 21 Oktober 2026.

PERBANDINGAN SENI BINA • RINGKAS

	Bitcoin	Ethereum	Solana
Model transaksi	UTXO	Akaun	Akaun + program
Aset asli	BTC	ETH	SOL
Smart contract	Terhad — Bitcoin Script	EVM penuh (cth. Solidity)	Program SVM (cth. Rust)
Konsensus	Proof of Work	Proof of Stake	Proof of Stake (Alpenglow, Okt 2026)
Finaliti	Probabilistik — lebih banyak blok, lebih yakin	Checkpoint selepas ~2 epoch	Sasaran ~150 ms (Alpenglow)
Contoh wallet	Hardware wallet, Sparrow	MetaMask, Rabby, hardware wallet	Phantom, Solflare, hardware wallet
Kegunaan biasa	Simpanan nilai, pembayaran	DeFi, token, NFT, asas L2	DeFi, token, dagangan pantas
Had utama	Pemrograman terhad; blok lebih perlahan	Yuran L1 boleh tinggi semasa sesak	Perkakasan validator mahal; pernah terhenti

RAJAH 2.2 — Bitcoin vs Ethereum vs Solana. Setiap rangkaian membuat pertukaran (trade-off) berbeza antara keselamatan, keupayaan dan kelajuan. [EZK3-004]

Jadual di bawah menambah lajur bagi rangkaian serasi EVM terpilih. Perhatikan bahawa "serasi EVM" tidak bermaksud "sama seperti Ethereum". Arbitrum One, OP Mainnet dan Base ialah rollup Layer 2 yang menghantar data ke Ethereum [L2B-003, L2B-004, L2B-005]. BNB Smart Chain mempunyai validatornya sendiri dan memerlukan bridge untuk berhubung dengan Ethereum [L2B-065]. Avalanche C-Chain ialah rangkaian EVM dalam rangkaian Avalanche [L2B-066]. Polygon PoS pula dikelaskan sebagai sidechain [L2B-015]. Klasifikasi ini diuraikan dalam Bab 04.

⇌ PROTOCOL COMPARISON

Empat Ekosistem (disemak Oktober 2026)

DIMENSI	BITCOIN	ETHEREUM	SOLANA	EVM TERPILIH
Model transaksi	UTXO	Akaun (EOA + contract)	Akaun + program tanpa state	Akaun (seperti Ethereum)
Aset asli	BTC (satoshi)	ETH (wei)	SOL (lamport)	Ikut rangkaian: ETH, BNB, POL, AVAX
Smart contract	Skrip terhad	EVM penuh	Program sBPF	EVM; keselamatan berbeza-beza
Consensus & finaliti	PoW; probabilistik	PoS; ~15 minit	PoS; Alpenglow sejak 21 Okt 2026	Bergantung pada reka bentuk
Wallet (contoh)	Wallet khusus Bitcoin	MetaMask dan lain-lain	Wallet sokongan Solana (Bab 07)	Wallet EVM yang sama
Had utama	Keupayaan terhad; finaliti perlahan	Yuran L1 berubah ikut permintaan	Sejarah gangguan; perubahan pantas	Andaian kepercayaan berbeza

Native gas token setiap rangkaian EVM juga berbeza: ETH digunakan di Arbitrum One, OP Mainnet dan Base, manakala BNB Smart Chain menggunakan BNB, Polygon PoS menggunakan POL dan Avalanche C-Chain menggunakan AVAX [ETH-055]. Memegang ETH di Ethereum tidak membantu anda membayar gas di Polygon PoS.

02.6 Satu alamat EVM, banyak rangkaian

Inilah punca kekeliruan Mei Ling. Secret Recovery Phrase yang sama menghasilkan alamat yang sama pada semua rangkaian serasi EVM, tetapi baki dan token adalah khusus kepada rangkaian tempat ia dihantar ^[ETH-057]. **Rajah 2.3** menunjukkan satu alamat contoh dengan empat baki berbeza.

BAKI ILUSTRASI · SATU ALAMAT, EMPAT RANGKAIAN



Contoh Hipotetikal — nombor ilustrasi, bukan data pasaran

RAJAH 2.3 — Alamat EVM yang Sama, Rangkaian Berbeza. Alamat yang kelihatan sama tidak bermakna aset yang sama — setiap rangkaian menyimpan baki dan state sendiri. [EZK3-072]

Analoginya seperti satu nombor kad pengenalan yang digunakan di beberapa bank berbeza: nombornya sama, tetapi setiap bank menyimpan baki akaunnya sendiri, dan wang tidak berpindah antara bank hanya kerana nombornya sepadan. Begitu juga, aset tidak berpindah sendiri antara rangkaian; ia memerlukan bridge atau pengeluaran semula dari exchange (Bab 10 dan Bab 14).

× COMMON MISTAKE

"Alamat Sama, Jadi Rangkaian Tidak Penting"

Salah faham: Kerana alamat 0x7a3F...c91D (contoh) sah di semua rangkaian EVM, mana-mana rangkaian boleh dipilih semasa pengeluaran.

Kenapa berbahaya: Penerima — terutamanya exchange atau smart account — mungkin tidak mengawal alamat itu di rangkaian yang anda pilih. Alamat Solana pula berformat berbeza sepenuhnya.

Cara elak: Sahkan rangkaian, format alamat dan sokongan penerima sebelum menghantar; mulakan dengan jumlah ujian kecil.

TRANSACTION LAB

Membaca Baki Satu Alamat pada Empat Rangkaian

Gunakan baki ilustrasi dalam **Rajah 2.3**: Ethereum Mainnet 0.80 ETH; Arbitrum One 0.05 ETH; Base 120 USDC; BNB Smart Chain 0. Andaian rumah: ETH = RM12,600; 1 USD = RM4.20; USDC dianggap 1 USD untuk latihan ini sahaja.

1. Berapakah jumlah nilai portfolio dalam RM?
2. Bolehkah pemilik menghantar 120 USDC di Base sekarang?
3. Jika wallet ditetapkan pada BNB Smart Chain, apakah yang dipaparkan, dan adakah aset hilang?

JAWAPAN:

1. ETH: $0.85 \times \text{RM}12,600 = \text{RM}10,710.00$; USDC: $120 \times \text{RM}4.20 = \text{RM}504.00$; jumlah **RM11,214.00**.

2. Belum. Base menggunakan ETH sebagai gas, dan baki ETH di Base ialah 0; 0.80 ETH di Ethereum Mainnet tidak boleh membayar gas di Base.
3. Baki 0. Aset tidak hilang — ia hanya tidak berada di rangkaian itu. Tukar paparan rangkaian untuk melihatnya.

Peraturan "tukar rangkaian untuk melihat" ada hadnya. Panduan MetaMask menyatakan token yang dihantar pada rangkaian EVM yang salah ke EOA anda sendiri masih boleh diakses, tetapi penghantaran ke alamat smart contract tiada jaminan pemulihan, dan penghantaran ke rangkaian bukan EVM berkemungkinan hilang [ETH-057]. Alamat contract atau smart account hanya wujud di rangkaian tempat ia dilancarkan; alamat yang sama di rangkaian lain mungkin kosong atau milik contract lain [ETH-054].

WALLET SECURITY

chainId Melindungi Tandatangan, Bukan Pilihan Anda

Ancaman: Menganggap chainId akan "menyekat" pindahan ke rangkaian yang salah.

Akibat: chainId hanya memastikan transaksi bertandatangan tidak boleh dimainkan semula di rangkaian lain [ETH-011]; ia tidak menghalang anda menghantar aset ke rangkaian yang salah secara sah.

Kawalan: Semak nama rangkaian pada skrin pengesahan wallet setiap kali, terutamanya selepas menukar rangkaian atau menambah RPC tersuai.

● RINGKASAN BAB

5 Perkara Utama

1. Setiap blockchain mempunyai consensus, finality, aset asli dan rekod baki sendiri.
2. Bitcoin menggunakan UTXO dan finaliti probabilistik; Ethereum dan Solana menggunakan model akaun dengan reka bentuk berbeza.
3. EVM membolehkan rangkaian berkongsi format alamat dan contract, tetapi keselamatan dan native gas token berbeza.
4. Solana menyasarkan slot 200 ms sejak 9 Oktober 2026 dan beralih kepada Alpenglows pada 21 Oktober 2026, sehari selepas tarikh rujukan buku.
5. Satu alamat EVM boleh wujud di banyak rangkaian, tetapi baki adalah khusus rangkaian dan aset tidak berpindah sendiri.

5 Soalan Ulang Kaji

1. Apakah perbezaan coin (native asset) dan token?
2. Mengapa baki wallet Bitcoin dipanggil jumlah UTXO?
3. Apakah fungsi chainId, dan apakah yang tidak dilindunginya?
4. Mengapa "serasi EVM" tidak bermaksud "sama selamat seperti Ethereum"?
5. Mengapa 0.80 ETH di Ethereum Mainnet tidak boleh membayar gas di Base?

Latihan Praktikal

- **Baca-sahaja:** Melalui senarai chainId yang dirujuk ethereum.org, catat chainId dan native gas token bagi lima rangkaian dalam bab ini.
- **Baca-sahaja:** Salin satu alamat EVM awam (contohnya contract token terkenal daripada laman rasmi penerbitnya) ke explorer dua rangkaian berbeza dan bandingkan apa yang dipaparkan.
- **Pengiraan:** Ulang TRANSACTION LAB dengan andaian ETH = RM10,080 (turun 20%). Berapakah jumlah nilai portfolio?

→ SETERUSNYA

Kini anda tahu di mana aset direkodkan. Bab 03 menerangkan apa yang mengawal rekod itu — smart contract dan program — termasuk mengapa kod di blockchain bukan jaminan keselamatan kewangan.