

Kandungan

•	Tentang Pengarang	6
•	Penafian Kewangan	7
•	Notis Batasan Penyelidikan	8
•	Notis Privasi dan Etika Penyelidikan	9
•	Notis Regulatori Malaysia	10
•	Penafian Maklumat Syariah	11
•	Pendedahan Kepentingan Pengarang	12
•	Kata Pengantar	14
•	Prakata Pengarang	15
•	Cara Menggunakan Buku Ini	16
•	Prasyarat	17
•	Peta Pembelajaran	18
•	Blockchain Tak Bercakap — Tetapi Data Meninggalkan Jejak	22

BAHAGIAN I • ASAS ON-CHAIN RESEARCH

01	Apa Itu On-Chain Analysis?	27
02	Memahami Blockchain Data Structure	34
03	Membaca Data Melalui Block Explorer	42
04	Data Quality, Labels & False Signals	49

BAHAGIAN II • PENILAIAN ON-CHAIN BITCOIN

05	Realized Capitalization & Realized Price	58
06	MVRV, MVRV Z-Score & NUPL	65
07	SOPR, aSOPR & Realized Profits	72
08	Long-Term Holders, Short-Term Holders & Coin Age	79
09	Network Activity & On-Chain Adoption	86

BAHAGIAN III • ALIRAN MODAL & SMART MONEY

10	Exchange Inflows, Outflows & Reserves	93
11	Whale Tracking & Wallet Intelligence	102
12	Smart Money — Siapa yang Membeli dan Menjual?	110
13	Stablecoin Flows & Global Crypto Liquidity	117
14	Miners, Validators & Supply Pressure	123

BAHAGIAN IV • DERIVATIVES, TOKENOMICS & FUNDAMENTAL PROTOKOL

15	Derivatives Data sebagai Market Context	131
16	Tokenomics – Memahami Nilai & Bekalan Token	137
17	Token Unlocks, Vesting & Dilution	143
18	DeFi TVL, Fees, Revenue & Protocol Economics	151
19	Analisis Ekosistem Layer 1, Layer 2 & Sektor Kripto	160

BAHAGIAN V • ALAT ANALITIK PRAKTIKAL

20	Block Explorer & Wallet Investigation Lab	168
21	Glassnode & CryptoQuant Masterclass	175
22	Dune Analytics & SQL untuk Blockchain	182
23	DefiLlama, Nansen, Arkham & Token Terminal	196

BAHAGIAN VI • MEMBINA CRYPTO MARKET INTELLIGENCE

24	Menggabungkan On-Chain, Technical & Macro Analysis	205
25	Backtesting On-Chain Signals & Research Validation	212
26	Membina Crypto Intelligence Research Report	221

BAHAGIAN VII • KAJIAN KES & PENGUASAAN PRAKTIKAL

27	Lapan Kajian Kes On-Chain Market Intelligence	229
28	Program Pembelajaran Penganalisis On-Chain 30 Hari	239

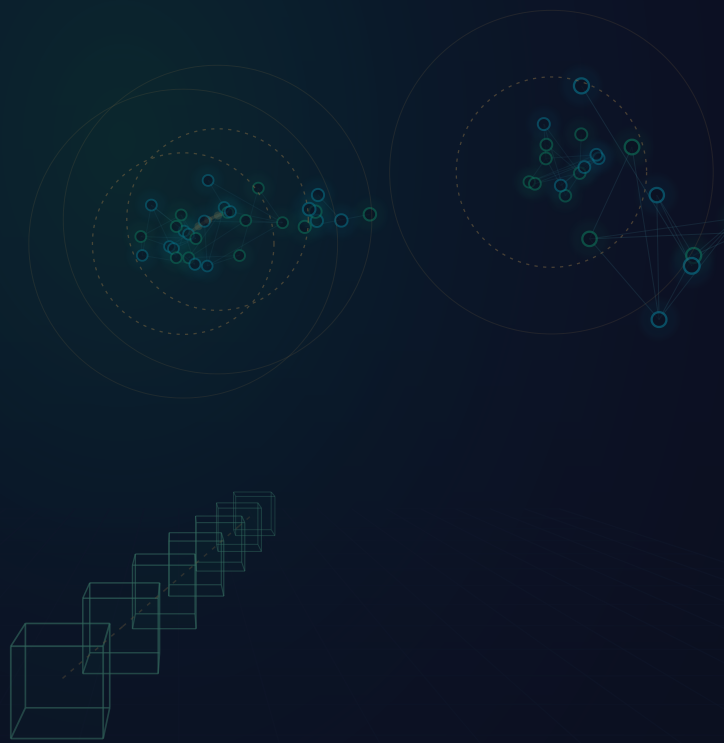
LAMPIRAN & RUJUKAN

A	Glosari Analisis On-Chain	246
B	Helaian Formula On-Chain Bitcoin	258
C	Rujukan Metrik Kitaran Pasaran	264
D	Panduan Tafsiran Exchange Flow	267
E	Senarai Semak Siasatan Wallet	271
F	Templat Penyelidikan Smart Money	274
G	Senarai Semak Due Diligence Tokenomics	277
H	Penjejak Token Unlock	279
I	Analisis Fundamental Protokol	281
J	Rujukan Metrik Kewangan DeFi	283
K	Rujukan Pantas DuneSQL	286
L	Rujukan Kod Python Penyelidikan	290
M	Perbandingan Sumber Data	293
N	Senarai Semak Penyelidikan Point-in-Time	296
O	Pelan Tindakan Dashboard Market Intelligence	298

P	Templat Laporan Penyelidikan Crypto	300
Q	Senarai Semak Due Diligence Syariah	303
R	Rujukan Peraturan Malaysia	305
S	Penjejak Penganalisis On-Chain 30 Hari dan Penilaian Akhir	309
T	Soalan Lazim (FAQ)	320
U	Sumber Rasmi dan Bacaan Lanjut	326
V	Pratonton Buku 05: Algorithmic & Agentic Crypto Trading	327
•	Rujukan & Sumber Disahkan	329

Asas On-Chain Research

Apa yang boleh dan tidak boleh didedahkan oleh blockchain: struktur data, block explorer, label alamat dan isyarat palsu.



BAB 01 Apa Itu On-Chain Analysis?

BAB 02 Memahami Blockchain Data Structure

BAB 03 Membaca Data Melalui Block Explorer

BAB 04 Data Quality, Labels & False Signals

BAB 01

BAHAGIAN I • ASAS ON-CHAIN RESEARCH

01

Apa Itu On-Chain Analysis?

Carta harga menunjukkan apa yang berlaku kepada harga. Laporan syarikat menunjukkan apa yang pengurusan pilih untuk dedahkan. Blockchain merekod apa yang berlaku kepada aset — tetapi tidak pernah menerangkan sebabnya.

Siti (watak rekaan), pelajar sarjana statistik di Bangi, membuka tiga tetingkap untuk satu tugas kaedah penyelidikan. Tetingkap pertama memaparkan carta harian Bitcoin. Tetingkap kedua ialah laporan suku tahunan sebuah syarikat tersenarai di Bursa Malaysia. Tetingkap ketiga ialah block explorer yang menyenaraikan transaksi terkini dalam rangkaian Bitcoin.

Penyelianya hanya memberi satu soalan: *bagi setiap sumber, apakah yang boleh dibuktikan, siapakah yang menghasilkan data itu, dan apakah yang langsung tidak kelihatan?* Selepas sejam, Siti sedar bahawa ketiga-tiga sumber menjawab soalan yang berbeza — dan block explorer, walaupun paling telus, ialah yang paling mudah disalah tafsir.

© OBJEKTIF PEMBELAJARAN

- | | |
|--|---|
| 01 Membezakan data on-chain dengan data off-chain dan mengenal pasti zon pertemuan antara keduanya. | 03 Menerangkan lima kelompok soalan on-chain intelligence. |
| 02 Membandingkan analisis carta harga, analisis fundamental syarikat dan analisis blockchain. | 04 Menyenaraikan perkara yang boleh dan tidak boleh didedahkan oleh data blockchain. |
| | 05 Menggunakan Kerangka Bukti lima langkah untuk menilai satu pemerhatian on-chain. |

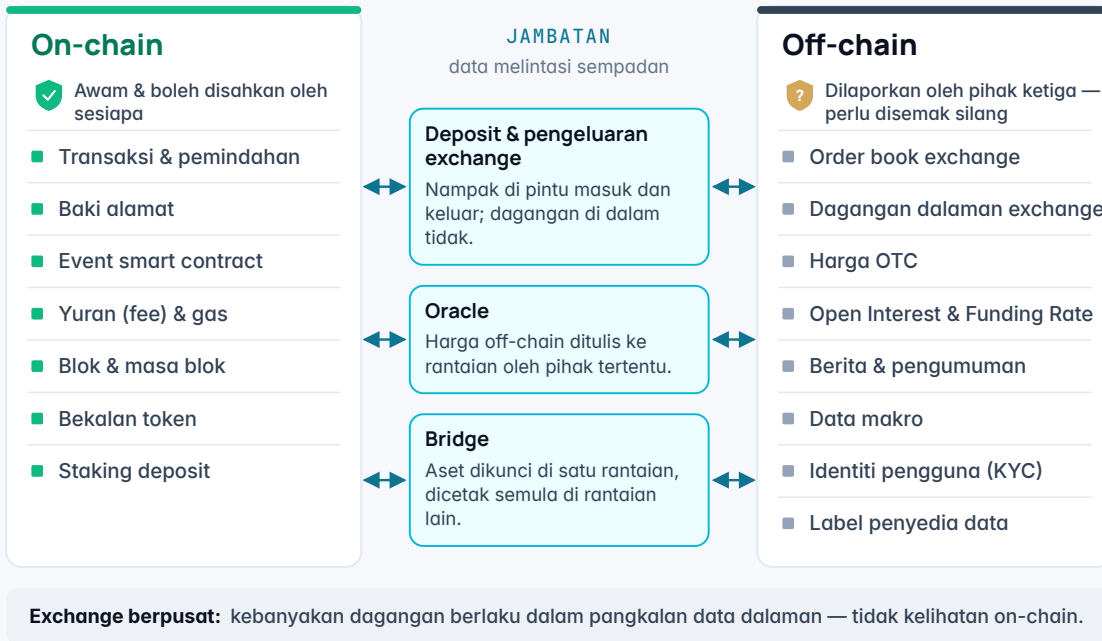
01.1 On-Chain dan Off-Chain: Dua Jenis Rekod

Data **on-chain** ialah apa sahaja yang direkodkan dalam blockchain: transaksi, baki alamat, yuran, blok, bekalan token dan event yang dipancarkan oleh smart contract. Data ini disahkan oleh nod rangkaian mengikut peraturan protokol, dan sesiapa sahaja boleh menyemaknya. Itulah maksud *telus* di sini. Ia tidak bermaksud semua orang tahu siapa pemilik sesuatu alamat; ia bermaksud rekod itu boleh disahkan secara bebas.

Data **off-chain** pula dihasilkan di luar rangkaian: order book dan dagangan dalaman exchange berpusat, harga OTC, data derivatives, berita, data makro, identiti pengguna dan label penyedia analitik. Data ini dilaporkan oleh pihak ketiga, jadi anda bergantung pada integriti dan metodologi pelaporannya.

Rajah 1.1 menunjukkan bahawa sempadannya tidak selalu kemas. Deposit dan pengeluaran exchange, oracle harga dan bridge berada di zon pertemuan: satu hujung kelihatan di rangkaian, hujung yang lain berlaku dalam pangkalan data sebuah syarikat. Apabila anda membeli BTC di exchange dan BTC itu kekal dalam akaun exchange, tiada transaksi on-chain baharu berlaku — hanya catatan dalam lejar dalaman. Banyak pembentukan harga crypto berlaku dengan cara ini.

SUMBER DATA • ON-CHAIN, OFF-CHAIN DAN ZON PERTEMUAN



RAJAH 1.1 — On-Chain vs Off-Chain Data. Data on-chain awam dan boleh disahkan, tetapi banyak aktiviti pasaran berlaku di luar rantai — terutamanya dalam exchange berpusat.

EZK4-001

Block explorer ialah tingkap paling mudah ke lebar awam. Ia membaca data daripada nod, mengindeksnya dan memaparkannya sebagai halaman yang boleh dicari mengikut hash, alamat atau nombor blok. Bab 03 membawa anda ke explorer sebenar; buat masa ini, ingat bahawa explorer memaparkan fakta rantai *bersama* label dan harga USD yang datang dari luar rantai.

◆ TERMINOLOGY

Istilah Asas Bab Ini

On-chain — data yang direkodkan dan disahkan dalam blockchain mengikut peraturan protokol.

Off-chain — data yang dihasilkan dan dilaporkan di luar blockchain oleh pihak ketiga.

On-chain intelligence — proses menukar data rantai, bersama konteks luar rantai, kepada kesimpulan penyelidikan yang dinyatakan dengan tahap keyakinan dan syarat pembatalan.

Market microstructure — kajian tentang cara dagangan berlaku: tempat pesanan dipadankan, siapa yang menyediakan kecairan, kos transaksi dan aliran aset antara tempat dagangan.

Banyak "metrik on-chain" yang popular sebenarnya hibrid: kuantiti dari rantai didarab dengan harga dari luar rantai.

Σ FORMULA

Metrik Hibrid: Market Cap

FORMULA

$$\text{Market Cap (USD)} = \text{Harga (USD, off-chain)} \times \text{Bekalan (unit, on-chain)}$$

Contoh hipotetikal: 100,000 USD × 8 BTC = 800,000 USD.

Implikasi: Jika sumber harga berubah, nilai metrik berubah walaupun tiada satu transaksi pun berlaku. Realized Cap (Bab 05) pula menggunakan harga pada masa setiap coin kali terakhir bergerak.

01.2 Tiga Lensa Analisis: Teknikal, Fundamental dan Blockchain

Analisis teknikal mengkaji harga, volum dan corak dagangan. Analisis fundamental menilai nilai asas berdasarkan aliran tunai, aset dan prospek perniagaan. Analisis kuantitatif menukar kedua-duanya kepada model statistik yang boleh diuji. On-chain analysis meminjam disiplin ketiga-tiganya, tetapi bahan mentahnya berbeza: rekod pergerakan aset dalam lejar awam.

Inilah jadual yang akhirnya dilukis oleh Siti:

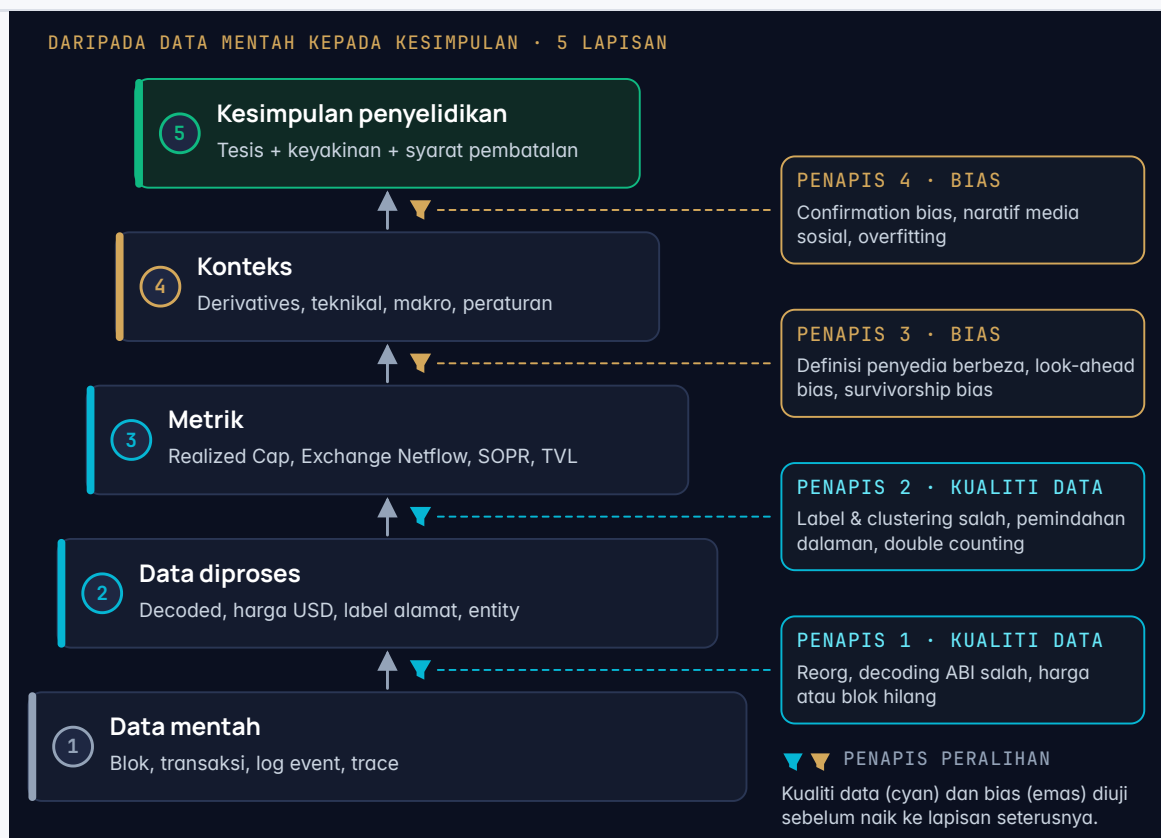
DIMENSI	CARTA HARGA	FUNDAMENTAL SYARIKAT	ANALISIS BLOCKCHAIN
Sumber	Exchange (off-chain)	Penyata & pengumuman	Lejar awam (on-chain)
Kekerapan	Setiap saat	Suku tahunan	Setiap blok
Identiti pihak	Tersembunyi	Dikenal pasti	Pseudonim
Soalan dijawab	Bagaimana harga bergerak	Bagaimana perniagaan berprestasi	Bagaimana aset bergerak
Kelemahan	Tiada sebab dagangan	Lewat; naratif pengurusan	Niat dan identiti tidak kelihatan

Konteks Malaysia menajamkan perbezaan ini. Syarikat tersenarai di Bursa Malaysia menerbitkan laporan suku tahunan dan pengumuman korporat dalam rangka kerja pendedahan yang dikawal selia. Laporan itu lewat beberapa minggu dan disusun oleh pengurusan, tetapi ia datang dengan nama, tanggungjawab undang-undang dan penjelasan. Data blockchain berlawanan sifatnya: hampir masa nyata dan sangat terperinci, tetapi tanpa nama, tanpa nota kaki dan tanpa sesiapa yang bertanggungjawab menerangkannya. Dalam laporan syarikat, cabarannya ialah menyemak naratif pengurusan. Dalam data blockchain, cabarannya ialah tidak mencipta naratif sendiri.

Data on-chain juga tidak semestinya mendahului harga. Kristoufek (2015) mendapati hash rate dan difficulty Bitcoin berkait positif dengan harga dalam jangka panjang, tetapi hargalah yang mendahului kedua-dua hubungan itu ^[MET-054]. Dua siri yang bergerak bersama menunjukkan hubungan statistik, bukan bukti sebab-akibat.

01.3 Lima Soalan dalam On-Chain Intelligence

Rajah 1.2 menggambarkan intelligence sebagai rantaian lapisan, bukan satu metrik. Data mentah diproses (dinyahkod, diberi harga, dilabel), dikira menjadi metrik seperti Realized Cap atau Exchange Netflow, diletakkan dalam konteks derivatives, teknikal, makro dan peraturan, dan barulah menjadi kesimpulan dengan tahap keyakinan. Pada setiap peralihan, kualiti data dan bias boleh merosakkan hasil.



RAJAH 1.2 — Kerangka Blockchain Intelligence. Intelligence bukan metrik tunggal: ia rantai dari data mentah, pemrosesan, metrik dan konteks hingga kesimpulan yang boleh dibatalkan.

EZK4-002

Kebanyakan penyelidikan on-chain cuba menjawab satu daripada lima kelompok soalan:

1. **Penggunaan rangkaian** — adakah aktiviti itu ekonomi sebenar atau spam dan pemindahan dalaman? (Bab 09, 19)
2. **Aliran modal** — adakah aset bergerak ke exchange, stablecoin atau DeFi? (Bab 10, 13)
3. **Ekonomi token** — bagaimana bekalan berubah melalui emission, unlock dan burn? (Bab 14, 16–18)
4. **Tingkah laku pelabur** — berapa lama coin dipegang, dan pada anggaran kos asas berapa? (Bab 05–08, 11–12)
5. **Struktur mikro pasaran** — bagaimana aliran on-chain berinteraksi dengan order book dan derivatives? (Bab 15, 24)

Setiap soalan memerlukan gabungan data on-chain dan off-chain.

01.4 Batasan Data On-Chain: Apa yang Boleh dan Tidak Boleh Didedahkan

Kekuatan data blockchain ialah ketepatannya tentang *apa* yang berlaku. Kelemahannya ialah kesenyapannya tentang *siapa* dan *mengapa*.

BOLEH DIDEBAHKAN (DENGAN PENGESAHAN)	TIDAK DIDEBAHKAN SECARA LANGSUNG
Jumlah, masa blok dan yuran transaksi	Identiti sebenar pemilik alamat
Baki alamat dan kontrak	Niat: jual, simpan, cagar atau lindung nilai
Bekalan token, mint dan burn	Dagangan dalaman exchange dan OTC
Umur coin dan harga kali terakhir bergerak	Posisi derivatives dan kos perakaunan sebenar

Lajur kiri pun tidak bebas masalah. Label yang menghubungkan alamat kepada exchange ialah lapisan tafsiran. Glassnode menyatakan bahawa baki exchange dalam datanya sebahagian besarnya anggaran batas bawah dan boleh disemak semula secara retrospektif ^[ONC-100], manakala siri berasaskan entity boleh berubah apabila kaedah clustering diperbaiki ^[WAL-063]. Carta yang anda lihat hari ini mungkin berbeza daripada carta yang sama sebulan lalu (Bab 04).

× KESILAPAN ANALITIKAL

Menyamakan "Telus" dengan "Lengkap"

Kesilapan: Menganggap bahawa kerana blockchain bersifat awam, semua aktiviti pasaran boleh dilihat.

Kenapa berbahaya: Dagangan exchange, penyelesaian OTC dan hedge derivatives berlaku di luar rantai. Pemindahan besar mungkin hanya penyusunan semula wallet, manakala jualan sebenar mungkin tidak meninggalkan jejak.

Cara elak: Bagi setiap kesimpulan, tandakan bahagian yang disokong data on-chain, bahagian yang bergantung pada data off-chain, dan bahagian yang hanya inferens.

01.5 Kerangka Bukti: Cara Berfikir Sepanjang Buku Ini

Pembukaan buku ini memperlihatkan satu tabiat: berhenti, pisahkan fakta daripada tafsiran, dan tulis apa yang akan membuktikan anda salah. **Rajah 1.3** menjadikan tabiat itu kerangka rasmi.

KERANGKA BUKTI • LIMA LANGKAH SETIAP KESIMPULAN



RAJAH 1.3 — Kerangka Bukti Lima Langkah. Setiap kesimpulan dalam buku ini mengikut lima langkah yang sama — termasuk bukti yang akan membuktikan kita salah.

EZK4-087

Pemerhatian ialah apa yang data tunjukkan secara langsung, dengan sumber, unit dan masa — tanpa kata sifat. **Tafsiran** ialah maksud yang mungkin. **Penjelasan alternatif** memaksa anda menyenaraikan sebab lain yang munasabah, termasuk masalah data. **Keyakinan** dinyatakan sebagai rendah, sederhana atau tinggi, berserta sebabnya. **Pembatalan** ialah bukti khusus yang akan melemahkan atau menolak tafsiran anda. Gelung balik ke Pemerhatian bermaksud kesimpulan sentiasa dipantau dan dikemas kini.

Siti menguji kerangka ini pada dakwaan yang sering muncul dalam kumpulan pelaburan: "rangkaian token ini sedang berkembang pesat".

↳ KERANGKA BUKTI

Lonjakan Active Addresses (contoh hipotetikal)

PEMERHATIAN (OBSERVATION): Purata harian active addresses bagi satu rangkaian Layer 1 meningkat daripada 20,000 kepada 28,000 dalam seminggu, iaitu kenaikan 40% (hipotetikal; tarikh dalam UTC).

TAFSIRAN (INTERPRETATION): Lebih ramai pengguna mungkin mula menggunakan rangkaian.

PENJELASAN ALTERNATIF (ALTERNATIVE EXPLANATIONS): Airdrop farming melalui ribuan alamat milik satu pihak; perubahan cara exchange mengumpul deposit; transaksi spam; perubahan definisi "aktif" oleh penyedia data.

KEYAKINAN (CONFIDENCE): Rendah. Tempohnya pendek, dan alamat bukan pengguna.

PEMBATALAN (INVALIDATION): Tafsiran "pertumbuhan pengguna" lemah jika kebanyakan alamat baharu dibiayai oleh sumber yang sama, jika aktiviti jatuh selepas tarikh snapshot airdrop, atau jika yuran dan nilai pemindahan tidak meningkat seiring.

Kerangka ini tidak melarang tafsiran optimistik. Ia memastikan tafsiran itu bersaing secara adil dengan penjelasan lain, dan bahawa anda tahu terlebih dahulu bukti apa yang akan mengubah fikiran anda. Penganalisis yang baik dinilai berdasarkan sejauh mana keyakinannya sepadan dengan bukti.

CALCULATION LAB

Berapa Banyak yang Kelihatan di Rangkaian?

Pada satu hari hipotetikal, sebuah exchange melaporkan volum dagangan spot 120,000 BTC. Data on-chain menunjukkan 8,000 BTC dipindahkan ke alamat berlabel milik exchange itu.

1. Berapakah inflow on-chain sebagai peratus volum yang dilaporkan?
2. Kemudian didapati 5,000 BTC daripada inflow itu ialah pemindahan antara wallet dalaman exchange yang sama. Berapakah inflow daripada pihak luar, dan berapa peratus daripada inflow asal?

JAWAPAN:

1. $8,000 \div 120,000 = 6.67\%$. Ini bukan pecahan tepat, kerana satu coin boleh didagangkan berkali-kali, tetapi ia menunjukkan bahawa kebanyakan dagangan direkodkan dalam lejar dalaman exchange — dan volum itu sendiri data off-chain.
2. $8,000 - 5,000 = 3,000$ BTC, iaitu 37.5% daripada inflow asal.

Pada akhir tugasannya, Siti menulis satu ayat di atas jadualnya: setiap sumber data menjawab soalan yang berbeza, dan tugas penganalisis ialah mengetahui soalan mana yang sedang dijawab.

● RINGKASAN BAB

5 Perkara Utama

1. Data on-chain disahkan oleh rangkaian; data off-chain dilaporkan oleh pihak ketiga; deposit exchange, oracle dan bridge berada di zon pertemuan.
2. Banyak metrik "on-chain" ialah hibrid kuantiti rangkaian dan harga luar rangkaian.
3. Analisis blockchain melengkapkan, bukan menggantikan, analisis teknikal dan fundamental.
4. Blockchain tidak mendedahkan identiti, niat atau dagangan dalaman exchange; label dan siri entity boleh disemak semula.
5. Setiap kesimpulan mengikut Kerangka Bukti: Pemerhatian → Tafsiran → Penjelasan alternatif → Keyakinan → Pembatalan.

5 Soalan Ulang Kaji

1. Mengapakah pembelian BTC yang kekal dalam akaun exchange tidak menghasilkan transaksi on-chain?
2. Apakah yang menjadikan Market Cap sebuah metrik hibrid?
3. Bezakan laporan suku tahunan syarikat Bursa Malaysia dengan data blockchain dari segi kekerapan, identiti dan tanggungjawab.
4. Apakah implikasi dapatan bahawa harga mendahului hash rate?
5. Nyatakan dua bukti yang akan membatalkan tafsiran "pertumbuhan pengguna" dalam contoh active addresses.

Latihan Praktikal

Pilih satu dakwaan on-chain daripada media sosial (contohnya "whale sedang mengumpul"). Tanpa menyambung wallet, tulis lima baris Kerangka Bukti untuknya, termasuk sekurang-kurangnya tiga penjelasan alternatif. Simpan nota itu dan semak semula selepas Bab 04.

→ SETERUSNYA

Sebelum mentafsir aliran, kita perlu faham bagaimana data itu disusun. Bab 02 membuka struktur dalaman blockchain — UTXO Bitcoin, model akaun Ethereum, event log dan finality — dan menunjukkan mengapa metrik satu rantaian tidak boleh dipindahkan begitu sahaja ke rantaian lain.

Memahami Blockchain Data Structure

Bitcoin tidak menyimpan baki; ia menyimpan output yang belum dibelanjakan. Ethereum menyimpan baki, tetapi pemindahan token tersembunyi dalam log. Salah faham tentang struktur ini ialah punca banyak kesimpulan on-chain yang silap.

Seorang guru di Ipoh (watak rekaan) memindahkan 0.80 BTC daripada wallet peribadinya kepada seorang rakan. Aplikasi wallet memaparkan baki baharu seperti dijangka. Tetapi apabila dia menyemak alamat lamanya di block explorer, baki alamat itu sifar, dan transaksinya mempunyai dua output: 0.80 BTC kepada rakannya dan 0.2997 BTC kepada alamat yang tidak pernah dilihatnya. Dia segera bertanya kepada adik iparnya: "Wallet saya kena godam?"

Tiada apa yang dicuri. Wallet itu memulangkan lebih nilai ke alamat change baharu yang dikawal oleh kunci yang sama. (Senario hipotetikal; angkanya sama dengan [Rajah 2.1](#).) Salah faham kecil ini ialah versi peribadi bagi kesilapan penganalisis pada skala besar: membaca data satu rantaian dengan andaian rantaian lain.

© OBJEKTIF PEMBELAJARAN

- | | |
|---|---|
| <p>01 Menerangkan model UTXO: input, output, change output dan yuran tersirat.</p> <p>02 Menerangkan model akaun: baki, nonce, gas, event log dan internal transaction.</p> <p>03 Membezakan address, wallet dan entity.</p> | <p>04 Memahami timestamp, mempool, confirmation, finality dan reorg sebagai sumber ketidakpastian.</p> <p>05 Menjelaskan mengapa metrik UTXO tidak boleh dipindahkan terus ke ETH atau SOL.</p> |
|---|---|

02.1 Model UTXO Bitcoin: Input, Output dan Change

Bitcoin tidak mempunyai medan "baki akaun". Rantaian menyimpan **output transaksi**, setiap satu dengan nilai dalam satoshi dan skrip yang menetapkan syarat untuk membelanjakannya. Output yang belum dibelanjakan dipanggil **UTXO**. "Baki" dalam wallet ialah jumlah semua UTXO yang dikawal oleh kunci wallet itu.

Untuk membayar, wallet memilih satu atau lebih UTXO sebagai **input**. Setiap input merujuk output terdahulu melalui pasangan txid:vout, dan dibelanjakan *sepenuhnya* — tiada konsep membelanjakan separuh UTXO. Transaksi kemudian mencipta output baharu: satu kepada penerima dan, lazimnya, satu **change output** yang memulangkan lebih kepada penghantar.

Dalam [Rajah 2.1](#), dua UTXO (0.60 BTC dan 0.50 BTC) berjumlah 1.10 BTC. Outputnya ialah 0.80 BTC kepada penerima dan 0.2997 BTC sebagai change. Yuran tidak muncul sebagai output; ia ialah beza antara jumlah input dan jumlah output, iaitu 0.0003 BTC, yang dituntut oleh pelombong melalui transaksi coinbase blok itu.

MODEL UTXO (BITCOIN) • SATU TRANSAKSI

Contoh Hipotetikal

INPUT • UTXO SEDIA ADA

UTXO #1 • milik penghantar

0.60 BTC

DIBELANJAKAN

UTXO #2 • milik penghantar

0.50 BTC

DIBELANJAKAN

Dibelanjakan sepenuhnya

Tiada 'baki separuh': lebihan mesti dihantar semula sebagai change.

TRANSAKSI

Jumlah input 1.10 BTC

Jumlah output 1.0997 BTC

Yuran 0.0003 BTC

yuran = input - output

Yuran 0.0003 BTC dituntut miner melalui transaksi coinbase blok
yuran tidak muncul sebagai output

OUTPUT • UTXO BAHARU

Output 0 • penerima

0.80 BTC

UTXO baharu milik penerima

Output 1 • change

0.2997 BTC

ke alamat baharu penghantar

Change output

Dari luar, change kelihatan seperti pembayaran biasa — heuristik diperlukan.

Baki 'wallet' = jumlah UTXO yang boleh dibelanjakannya— di sini, UTXO change 0.2997 BTC.

RAJAH 2.1 — Model Transaksi UTXO. Dalam model UTXO, transaksi memusnahkan output lama dan mencipta output baharu; baki 'wallet' ialah jumlah UTXO yang boleh dibelanjakannya.

EZYK4-003 • Contoh Hipotetikal

● MUDAH FAHAM

UTXO seperti Wang Kertas

Anda membayar RM8 dengan dua keping RM5 dan menerima RM2 baki. Kedua-dua keping diserahkan sepenuhnya; lebihannya kembali kepada anda.

Batas analogi: Dalam Bitcoin, "wang kertas" lama dimusnahkan, baki biasanya pergi ke alamat baharu, dan yuran ialah jurang yang tidak dikembalikan, bukan item tersendiri dalam rekod.

Rajah 2.2 memecahkan medan transaksi seperti yang dipaparkan oleh explorer: txid, block height, masa blok (UTC), pengesahan, input dengan rujukan txid:vout, output dengan alamat dan jenis skrip, saiz dalam vbyte, yuran, kadar yuran (sat/vB) dan witness. Setiap medan ialah fakta teknikal; siapa membayar siapa secara ekonomi masih memerlukan tafsiran.



RAJAH 2.2 — Pecahan Transaksi Bitcoin. Medan transaksi Bitcoin memberi fakta teknikal — siapa yang membayar siapa secara ekonomi masih memerlukan tafsiran.

EZK4-008 • Ilustrasi Konsep — Bukan Paparan Sebenar Platform

Struktur input juga mendedahkan maklumat. Transaksi 10,000 BTC yang lazim dikaitkan dengan "transaksi pizza" membelanjakan 131 input daripada alamat yang sama kepada satu output 10,000 BTC tanpa change; bezanya, 0.99 BTC, ialah yuran ^[WAL-018]. Kertas putih Bitcoin sendiri mengakui bahawa transaksi berbilang input mendedahkan bahawa input-inputnya dimiliki oleh pemilik yang sama ^[WAL-032]. Inilah asas heuristik clustering dalam Bab 04 dan Bab 11 — heuristik yang tidak boleh digunakan pada model akaun.

Σ FORMULA

Yuran dan Kadar Yuran Bitcoin

FORMULA

$$\begin{aligned} \text{Yuran (BTC)} &= \Sigma \text{ nilai input} - \Sigma \text{ nilai output} \\ \text{Kadar yuran (sat/vB)} &= \text{Yuran (sats)} \div \text{Saiz transaksi (vbyte)} \end{aligned}$$

Unit: 1 BTC = 100,000,000 sats. Kadar yuran ialah kadar per unit saiz data, bukan peratus nilai yang dipindahkan.

Contoh (Rajah 2.1, hipotetikal): $(0.60 + 0.50) - (0.80 + 0.2997) = 0.0003 \text{ BTC} = 30,000 \text{ sats}$.

02.2 Model Akaun Ethereum: Baki, Nonce, Gas dan Log

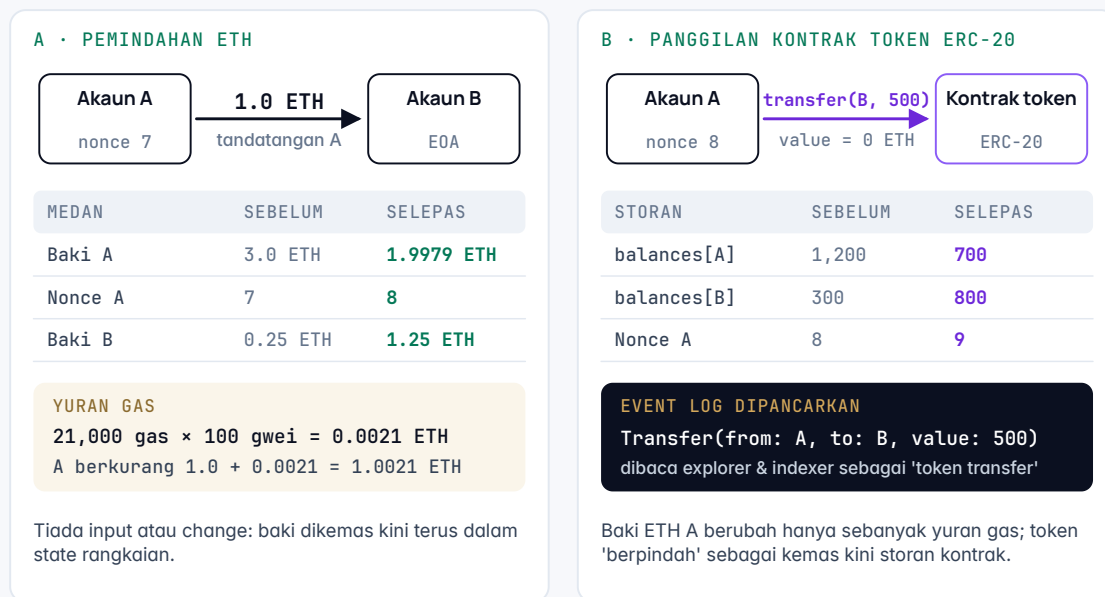
Ethereum menggunakan **model akaun**. Setiap akaun mempunyai baki dan nonce; smart contract juga mempunyai kod dan storan. Transaksi tidak memusnahkan output — ia mengemas kini keadaan (state) secara terus. **Nonce** ialah kiraan transaksi yang telah dihantar oleh akaun. Ia memastikan setiap transaksi diproses sekali sahaja dan mengikut urutan; transaksi pending boleh digantikan dengan transaksi bernonce sama dan yuran lebih tinggi.

Dalam panel pertama **Rajah 2.3**, akaun A (3.0 ETH, nonce 7) menghantar 1.0 ETH kepada akaun B. Selepas itu A memegang 1.9979 ETH — 1.0 ETH dihantar dan 0.0021 ETH dibayar sebagai yuran gas — dan nonce A menjadi

8. Tiada change output kerana tiada output langsung; baki A hanya ditolak.

MODEL AKAUN (ETHEREUM) • KEADAAN SEBELUM & SELEPAS

Contoh Hipotetikal



Harga gas 100 gwei, baki B dan baki token dipilih untuk ilustrasi.

RAJAH 2.3 — Model Transaksi Berasaskan Akaun. Model akaun mengemas kini baki secara langsung; pemindahan token ialah perubahan storan kontrak yang direkodkan sebagai event log.

EZK4-004 • Contoh Hipotetikal

Panel kedua lebih penting bagi penganalisis. Apabila A memindahkan token ERC-20, ETH yang keluar hanyalah yuran gas. Baki token disimpan dalam storan kontrak token, bukan dalam akaun A. Kontrak mengemas kini storan itu dan memancarkan **event log** Transfer(from, to, value) — log yang dibaca oleh explorer dan pangkalan data analitik untuk membina sejarah pemindahan token.

Dua implikasi timbul. Pertama, medan to transaksi tidak semestinya penerima aset. Dalam transaksi blok 20,000,000 (Bab 03), to ialah router Uniswap sedangkan USDC mengalir ke kolam, dan satu swap itu menghasilkan 9 log serta 5 pemindahan ERC-20 menurut Etherscan [WAL-009]. Kedua, apa yang dipancarkan bergantung pada kod kontrak. USDC memancarkan Transfer daripada alamat sifar apabila token dicipta [DUN-068], tetapi fungsi issue() USDT di Ethereum hanya memancarkan event Issue [DUN-067]. Analisis yang hanya mengira log Transfer akan terlepas pertambahan bekalan USDT itu.

Kontrak juga boleh memindahkan ETH tanpa transaksi peringkat atas yang baharu. Pergerakan ini, dipanggil **internal transaction** atau **trace**, hanya kelihatan dengan menjejak pelaksanaan transaksi; Dune menyimpannya dalam jadual ethereum.traces [DUN-034]. Solana pula berasaskan akaun dengan susunan berbeza: baki token SPL disimpan dalam akaun token berasingan, manakala akaun mint merekod bekalan, decimals dan autoriti mint [WAL-028].

◆ TERMINOLOGY

Istilah Struktur Data

UTXO — output transaksi Bitcoin yang belum dibelanjakan; unit asas pemilikan dalam model UTXO.

Change output — output yang memulangkan lebih nilai input kepada penghantar, lazimnya ke alamat baharu.

Nonce — kiraan transaksi yang dihantar oleh sesuatu akaun; menentukan urutan dan menghalang ulangan.

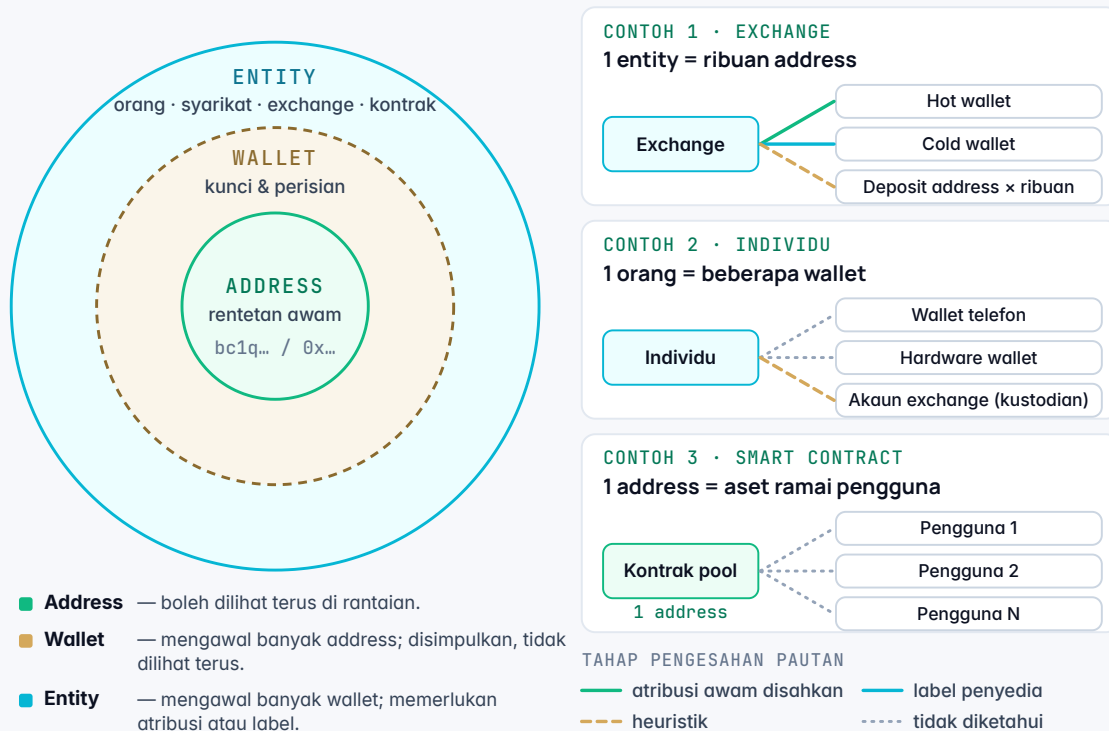
Event log — rekod yang dipancarkan oleh smart contract semasa pelaksanaan, seperti Transfer.

Internal transaction / trace — panggilan dan pemindahan nilai di dalam pelaksanaan transaksi, dicetuskan oleh kontrak.

02.3 Address, Wallet dan Entity

Rajah 2.4 memisahkan tiga lapisan yang sering dicampur adukkan. **Address** ialah rentetan awam yang kelihatan di rantaian. **Wallet** ialah perisian atau set kunci yang mengawal banyak address — wallet guru tadi mencipta alamat baharu untuk setiap change. **Entity** ialah pihak sebenar, sama ada individu, syarikat, exchange atau kontrak, yang mungkin mengawal banyak wallet.

TIGA LAPISAN IDENTITI DALAM DATA ON-CHAIN



RAJAH 2.4 — Wallet vs Address vs Entity. Satu address bukan semestinya satu orang; satu entity boleh mengawal ribuan address, dan satu address boleh mewakili ramai pengguna.

EZK4-005

Hubungan ini tidak satu-dengan-satu. Satu exchange boleh mengawal ribuan alamat deposit, hot wallet dan cold wallet, manakala satu kontrak kolam DeFi atau bridge boleh memegang aset ribuan pengguna. Jadi "alamat terbesar" bukan "orang terkaya", dan "100,000 alamat aktif" bukan "100,000 pengguna".

Menghubungkan alamat kepada entity memerlukan heuristik. Heuristik berbilang input Bitcoin tidak terpakai pada Ethereum kerana transaksi biasa hanya mempunyai satu pengirim. Friedhelm Victor mendapati heuristik penggunaan semula alamat deposit exchange paling berkesan bagi Ethereum; bersama dua heuristik lain, ia mengelompokkan 17.9% akaun luaran aktif dalam empat tahun pertama Ethereum ^[WAL-035]. Setiap pautan mempunyai tahap keyakinan sendiri, seperti yang dibincangkan dalam Bab 04 dan Bab 11.

02.4 Blok, Masa, Mempool dan Finality

Setiap blok mempunyai **block height**, hash blok sebelumnya dan timestamp. Dalam Bitcoin, timestamp ditetapkan oleh pelombong dan hanya menghampiri masa sebenar. Blok 840,000 mempunyai timestamp 20 April 2024, 00:09:27 UTC, tetapi medan `mediantime`-nya bersamaan 19 April 2024, 23:43:28 UTC — kira-kira 26 minit lebih awal ^[WAL-020]. Untuk kajian peristiwa, susun data mengikut block height atau median time, dan tukar kepada MYT (UTC+8) hanya semasa paparan.

Sebelum masuk ke blok, transaksi menunggu dalam **mempool**, iaitu kumpulan transaksi belum disahkan yang disimpan oleh setiap nod — dan setiap nod mungkin melihat kandungan yang sedikit berbeza. Transaksi pending

boleh digantikan, tersekat atau tidak pernah dimasukkan; mempool.space sendiri menyatakan cadangan yurannya tidak menjamin pengesahan ^[WAL-016]. Transaksi dalam mempool ialah niat, belum fakta.

Selepas masuk ke blok, setiap blok baharu di atasnya menambah satu **confirmation**. **Finality** ialah tahap di mana transaksi secara praktikal tidak lagi boleh diterbalikkan. Dalam Bitcoin, finality bersifat kebarangkalian dan setiap platform menetapkan ambang pengesahannya sendiri. Dalam Ethereum proof-of-stake, blok menjadi *finalized* melalui checkpoint, lazimnya selepas kira-kira dua epoch; satu epoch ialah $32 \text{ slot} \times 12 \text{ saat} = 6.4 \text{ minit}$.

Reorg berlaku apabila rangkaian menggantikan satu atau beberapa blok terkini dengan cabang lain, lalu transaksi di dalamnya boleh kembali ke mempool, berubah susunan atau hilang. Atas sebab ini, Dune sengaja melewati pengambilan data mentah Ethereum, dan data yang dinyahkod tiba kira-kira 15–60 saat selepas data mentah ^[DUN-016]. Data minit terakhir ialah data yang paling mudah berubah.

02.5 Batasan: Metrik dan Kiraan Tidak Boleh Dipindahkan Begitu Sahaja

Realized Cap (Bab 05), SOPR (Bab 07) dan coin age (Bab 08) bergantung pada satu sifat model UTXO: setiap unit coin berada dalam output diskret yang mempunyai masa penciptaan dan nilai tersendiri. Apabila UTXO dibelanjakan, kita tahu bila ia dicipta dan bila ia dimusnahkan, lalu boleh menganggarkan harga pada kedua-dua titik.

Model akaun tidak mempunyai lot diskret sebegini. Jika satu akaun menerima ETH lima kali pada harga berbeza lalu menghantar sebahagiannya, rantaian tidak menyatakan "unit" mana yang keluar — baki hanya ditolak. Sebarang versi Realized Cap atau SOPR untuk rantaian akaun memerlukan andaian tambahan, seperti FIFO atau kos purata bagi setiap akaun, dan kontrak yang mengumpul dana ramai pengguna merumitkan lagi andaian itu. Apabila metrik bernama sama muncul untuk BTC, ETH dan SOL, semak metodologi penyedia; nama yang sama tidak menjamin konsep yang sama.

Batasan kedua: **bilangan event tidak sama dengan aktiviti ekonomi bebas**. Satu swap boleh memancarkan beberapa log Transfer. Satu transaksi exchange boleh membayar ramai pelanggan serentak. Transaksi yang gagal tetap dicatat dan tetap membayar gas. Pemindahan antara alamat satu entity kelihatan sama seperti pembayaran antara dua pihak. Bagi setiap kiraan, tanya: berapa banyak daripadanya pemindahan nilai antara pemilik yang berbeza?

× FALSE SIGNAL

"Pemindahan Token Meningkatkan Tiga Kali Ganda"

KESIMPULAN MENGELIRUKAN: Event Transfer sesuatu token meningkat tiga kali ganda dalam sebulan, jadi penggunaannya juga meningkat tiga kali ganda.

KENAPA SALAH: Satu tindakan pengguna boleh menghasilkan banyak log; kontrak boleh memindahkan token secara dalaman; pemindahan antara alamat satu entity atau akaun Sybil dikira sebagai aktiviti; sesetengah kontrak tidak memancarkan Transfer untuk semua perubahan bekalan.

CARA MENGESAHKAN: Kira transaksi unik, bukan log; asingkan laluan router dan kolam; kelompokkan alamat kepada entity jika boleh; bandingkan dengan yuran dan nilai dipindahkan; semak sama ada kenaikan bertahan selepas program insentif tamat.

Kini cuba sendiri. Semua angka di bawah ialah hipotetikal.

CALCULATION LAB

Yuran, Kadar Yuran dan Baki

1. Andaikan transaksi **Rajah 2.1** bersaiz 209 vB. Berapakah kadar yurannya dalam sat/vB?
2. Jika wallet menetapkan 20 sat/vB untuk saiz yang sama, berapakah yuran dalam BTC, dan berapakah change jika penerima tetap menerima 0.80 BTC?
3. Akaun Ethereum dengan 3.0 ETH menghantar 1.0 ETH menggunakan 21,000 gas pada harga gas efektif 100 gwei. Berapakah yuran dan baki akhirnya? (1 gwei = 0.000000001 ETH)

JAWAPAN:

1. $30,000 \text{ sats} \div 209 \text{ vB} \approx 143.54 \text{ sat/vB}$.

2. $20 \times 209 = 4,180$ sats = 0.0000418 BTC; change = $1.10 - 0.80 - 0.0000418 = 0.2999582$ BTC.
3. $21,000 \times 100$ gwei = 2,100,000 gwei = 0.0021 ETH; baki = $3.0 - 1.0 - 0.0021 = 1.9979$ ETH, sepadan dengan Rajah 2.3.

Peraturan "belanja sepenuhnya, cipta yang baharu" juga boleh dimodelkan dengan beberapa baris kod, termasuk cara rangkaian menolak perbelanjaan berganda.

>_ PYTHON LAB

Simpan Kira UTXO Ringkas

FAIL: analysis/labs/ch02_utxo_bookkeeping.py

TUJUAN: Membelanjakan dua UTXO sepenuhnya, mencipta output penerima dan change, mengira yuran tersirat, dan menolak percubaan membelanjakan UTXO yang sama dua kali.

analysis/labs/ch02_utxo_bookkeeping.py PYTHON

```

1  """Bab 02 – Simpan kira UTXO ringkas (contoh hipotetikal, unit BTC).
2
3  Set UTXO: kunci = (txid, vout); nilai = (pemilik, jumlah BTC).
4  "Pemilik" hanya diketahui kerana kita mereka contoh ini;
5  rantaian sebenar hanya menyimpan skrip/alamat, bukan nama.
6  """
7  from decimal import Decimal as D
8
9  utxo_set = {
10     ("tx_a", 0): ("penghantar", D("0.60")),
11     ("tx_b", 1): ("penghantar", D("0.50")),
12 }
13
14
15 def spend(utxo_set, inputs, outputs, new_txid):
16     """Belanjakan input sepenuhnya, cipta output baharu, pulangkan yuran."""
17     if len(set(inputs)) != len(inputs):
18         raise ValueError("Input yang sama digunakan dua kali")
19     missing = [ref for ref in inputs if ref not in utxo_set]
20     if missing:
21         raise ValueError(f"Input tiada atau sudah dibelanjakan: {missing}")
22     total_in = sum(utxo_set[ref][1] for ref in inputs)
23     total_out = sum(amount for _, amount in outputs)
24     if total_out > total_in:
25         raise ValueError("Jumlah output melebihi jumlah input")
26     for ref in inputs:
27         del utxo_set[ref] # UTXO dibelanjakan sepenuhnya
28     for vout, (owner, amount) in enumerate(outputs):
29         utxo_set[(new_txid, vout)] = (owner, amount)
30     return total_in - total_out # yuran tersirat
31
32
33 def balance(utxo_set, owner):
34     return sum((a for o, a in utxo_set.values() if o == owner), D("0"))
35
36
37 if __name__ == "__main__":
38     fee = spend(
39         utxo_set,
40         inputs=[("tx_a", 0), ("tx_b", 1)],
41         outputs=[("penerima", D("0.80")), ("penghantar", D("0.2997"))],
42         new_txid="tx_c",
43     )
44     print("Yuran (BTC):", fee)
45     print("Baki penghantar (BTC):", balance(utxo_set, "penghantar"))
46     print("Baki penerima (BTC):", balance(utxo_set, "penerima"))
47     print("Bilangan UTXO:", len(utxo_set))

```

```

48     try:
49         spend(utxo_set, [{"tx_a", 0}], [{"penerima", D("0.10")}], "tx_d")
50     except ValueError as e:
51         print("Ditolak:", e)

```

DATA CONTOH: Dua UTXO hipotetikal, 0.60 BTC dan 0.50 BTC (**Rajah 2.1**).

PENGESAHAN: Yuran mesti 0.0003 BTC, dan UTXO baharu ($0.80 + 0.2997 = 1.0997$ BTC) mesti sama dengan jumlah input tolak yuran. Medan "pemilik" wujud hanya kerana contoh ini direka.

OUTPUT:

TEKS

```

1  Yuran (BTC): 0.0003
2  Baki penghantar (BTC): 0.2997
3  Baki penerima (BTC): 0.80
4  Bilangan UTXO: 2
5  Ditolak: Input tiada atau sudah dibelanjakan: [{"tx_a", 0}]

```

Guru di Ipoh tadi akhirnya faham bahawa alamat lamanya kosong kerana UTXO di situ telah dibelanjakan sepenuhnya. Penganalisis memerlukan kefahaman yang sama sebelum membaca sebarang carta: unit asas rantaian, tempat nilai sebenarnya bergerak, dan bila data boleh dianggap muktamad.

● RINGKASAN BAB

5 Perkara Utama

1. Bitcoin menyimpan UTXO, bukan baki; input dibelanjakan sepenuhnya, dan yuran = jumlah input – jumlah output.
2. Ethereum mengemas kini baki dan nonce secara terus; pemindahan token direkodkan sebagai event log, dan sesetengah aliran hanya kelihatan dalam trace.
3. Address, wallet dan entity ialah tiga lapisan berbeza yang dihubungkan oleh heuristik.
4. Timestamp blok hanya anggaran, transaksi mempool belum menjadi fakta, dan data terkini boleh berubah akibat reorg.
5. Metrik UTXO memerlukan andaian tambahan pada rantaian akaun, dan bilangan event bukan ukuran aktiviti ekonomi bebas.

5 Soalan Ulang Kaji

1. Mengapakah alamat lama guru di Ipoh menunjukkan baki sifar?
2. Bagaimanakah yuran 0.99 BTC dalam transaksi 131 input dikira?
3. Mengapakah kiraan log Transfer terlepas pertambahan bekalan USDT di Ethereum?
4. Apakah beza timestamp dengan mediantime blok 840,000?
5. Mengapakah Realized Cap untuk ETH memerlukan andaian tambahan?

Latihan Praktikal

Buka transaksi a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d di mempool.space (baca-sahaja), jumlahkan nilai input dalam sats dan sahkan bahawa yuran sama dengan jumlah input tolak output. Kemudian jalankan fail Python bab ini dengan change 0.31 BTC dan terangkan mesej ralatnya.

→ SETERUSNYA

Kini anda tahu bagaimana data disusun di dalam rantaian. Bab 03 membawa kefahaman ini ke block explorer sebenar – mempool.space, Etherscan, Blockscout dan Solscan – menggunakan blok, transaksi dan kontrak yang telah disahkan.