

Kandungan

•	Penafian Risiko Kewangan	6
•	Penafian Maklumat Syariah	7
•	Notis Maklumat Regulatori	8
•	Pendedahan Kepentingan Pengarang	9
•	Nota Pengarang	11
•	Prakata	12
•	Cara Menggunakan Buku Ini	13
•	Peta Pembelajaran	14
•	RM100 Pertama dalam Dunia Kripto	17

BAHAGIAN I • KENALI DUNIA KRIPTO

01	Dari Wang Tunai ke Wang Digital	22
02	Apa Sebenarnya Bitcoin?	29
03	Blockchain Tanpa Pening Kepala	35
04	Bitcoin, Ethereum dan Ribuan Altcoin	42
05	Wallet, Private Key dan Pemilikan Aset	49

BAHAGIAN II • BELAJAR MEMBELI DAN MENJUAL KRIPTO

06	Spot Trading untuk Beginner	57
07	Cryptocurrency di Malaysia	64
08	Panduan Luno Malaysia	71
09	Panduan Hata Malaysia	84
10	Luno vs Hata — Mana Satu Sesuai untuk Anda?	98

BAHAGIAN III • BINA ASAS SEBAGAI CRYPTO INVESTOR

11	Membaca Carta Crypto	105
12	DCA, HODL dan Spot Trading	111
13	Risk Management dalam Crypto	118
14	Cara Mengelakkan Scam Crypto	125

BAHAGIAN IV • SYARIAH & STAKING

15	Adakah Cryptocurrency Patuh Syariah?	132
16	Memahami Staking Crypto	140
17	Staking di Luno dan Hata	147

BAHAGIAN V • MENGURUS PELABURAN KRIPTO

18	Cukai, Rekod Transaksi dan Portfolio	155
19	Empat Kajian Kes Pelabur Kripto	161
20	Pelan Pembelajaran Kripto 30 Hari	168

LAMPIRAN & RUJUKAN

A	Glosari Crypto A-Z	173
B	Checklist Sebelum Membeli Cryptocurrency	179
C	Luno Beginner Checklist	181
D	Hata Beginner Checklist	184
E	Shariah Verification Checklist	187
F	Staking Risk Checklist	189
G	30-Day Learning Tracker	191
H	Sample Trading Journal	193
I	Sample Portfolio Tracker	195
J	Verified Sources and Further Reading	196
K	Soalan Lazim (FAQ)	198
L	Preview Siri ezyKripto Buku 02-05	203
•	Rujukan & Sumber Disahkan	205

BAHAGIAN I

Kenali Dunia Kripto

Dari wang tunai hingga blockchain: memahami apa itu crypto, bagaimana ia berfungsi dan siapa yang memegang kunci.

BAB 01 Dari Wang Tunai ke Wang Digital

BAB 02 Apa Sebenarnya Bitcoin?

BAB 03 Blockchain Tanpa Pening Kepala

BAB 04 Bitcoin, Ethereum dan Ribuan Altcoin

BAB 05 Wallet, Private Key dan Pemilikan Aset

Dari Wang Tunai ke Wang Digital

Wang anda sudah lama menjadi digital. Persoalannya bukan lagi "tunai atau digital", tetapi siapa yang memegang buku rekod.

Di sebuah pasar malam di Kuantan, seorang peniaga kuih menampal kod DuitNow QR pada tiang khemahnya. Anda mengimbas kod itu, menaip RM6 dan menekan "bayar". Dalam beberapa saat, telefon peniaga itu berbunyi. Tiada sekeping wang kertas pun bertukar tangan.

Apa sebenarnya yang berlaku? Tiada sesiapa menghantar wang fizikal dari dompet anda ke kotak wang peniaga. Yang berubah hanyalah dua angka: baki dalam rekod bank anda berkurang RM6, dan baki dalam rekod bank peniaga bertambah RM6. Jika wang kita sudah begitu digital, mengapa dunia memerlukan sesuatu yang dipanggil "cryptocurrency"? Bab ini menjawab soalan itu dengan bermula dari asas: apa itu wang.

© OBJEKTIF PEMBELAJARAN

Selepas bab ini, anda akan dapat:

- | | |
|---|--|
| <p>01 Menerangkan bagaimana bentuk wang berubah daripada barter kepada wang digital.</p> <p>02 Membezakan baki bank, wang elektronik (e-money) dan aset kripto.</p> <p>03 Menerangkan maksud lejar berpusat dan peranan kepercayaan dalam sistem kewangan.</p> | <p>04 Memahami latar belakang kemunculan Bitcoin selepas krisis kewangan 2008.</p> <p>05 Menilai apa yang crypto boleh dan tidak boleh selesaikan.</p> |
|---|--|

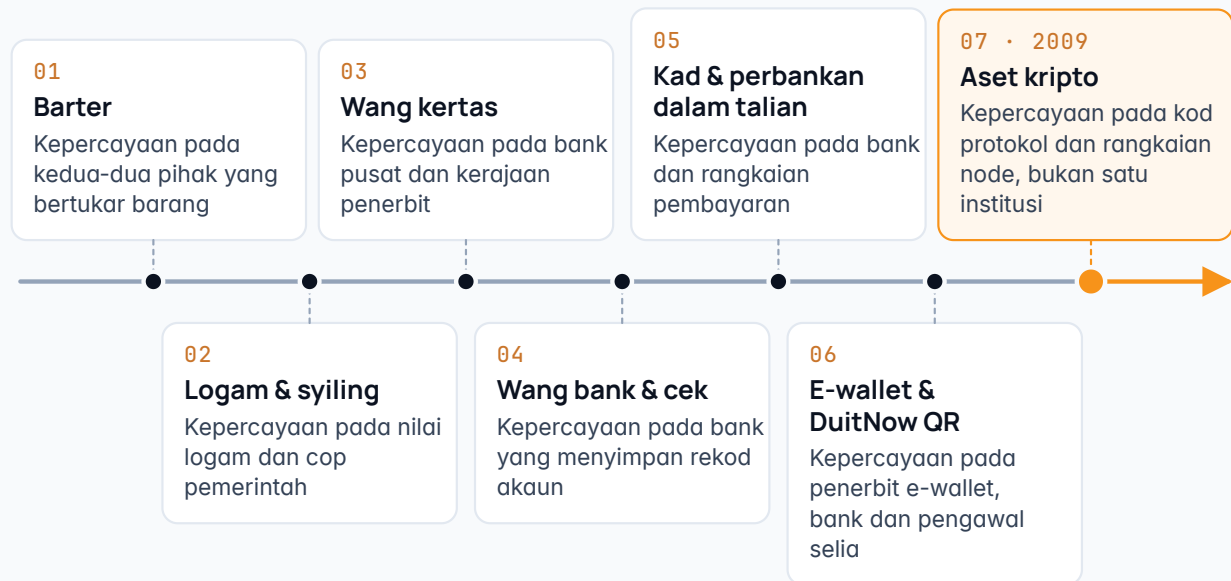
01.1 Wang Sentiasa Berubah Bentuk

Dari barter ke syiling dan kertas

Sebelum wang wujud, manusia berdagang melalui barter: beras ditukar dengan ikan, kain ditukar dengan garam. Masalahnya jelas. Anda perlu mencari seseorang yang mahukan barang anda *dan* mempunyai barang yang anda mahukan, pada masa yang sama.

Logam berharga dan syiling menyelesaikan masalah itu kerana ia diterima ramai, tahan lama dan mudah dibahagikan. Kemudian wang kertas muncul — pada asalnya sebagai resit yang boleh ditebus dengan logam, dan akhirnya sebagai wang yang nilainya bergantung pada kepercayaan terhadap penerbitnya, iaitu kerajaan dan bank pusat.

Rajah CH01-001 menunjukkan perjalanan ini hingga ke e-wallet dan aset kripto. Perhatikan bahawa setiap peringkat menjawab soalan yang sama dengan cara berbeza: siapa yang kita percaya untuk merekod nilai?



RAJAH CH01-001 — Evolusi Wang. Bentuk wang berubah, tetapi soalan asas kekal: siapa yang kita percaya untuk merekod nilai?

Apa yang menjadikan sesuatu itu "wang"

Ahli ekonomi biasanya menilai wang melalui tiga fungsi: **alat pertukaran** (diterima untuk membayar barang), **unit akaun** (harga dinyatakan dalamnya) dan **penyimpan nilai** (nilainya kekal munasabah dari semasa ke semasa). Ringgit memenuhi ketiga-tiganya dalam ekonomi Malaysia. Seperti yang akan kita lihat, crypto masih bergelut dengan sekurang-kurangnya satu daripadanya.

◆ ISTILAH PENTING

Legal tender (tender sah) — wang yang diiktiraf undang-undang sebagai cara sah untuk menjelaskan hutang dalam sesebuah negara. Di Malaysia, wang kertas dan syiling ringgit yang dikeluarkan oleh Bank Negara Malaysia (BNM) ialah legal tender. Crypto **bukan** legal tender di Malaysia ^[REG-020, REG-022]; kedudukan undang-undangnya dibincangkan dalam Bab 07.

01.2 Wang Anda Sudah Lama Digital

Baki bank ialah rekod

Apabila gaji masuk ke akaun bank, tiada timbunan wang kertas dengan nama anda di dalam peti besi. Anda memiliki satu entri dalam pangkalan data bank — janji bahawa bank berhutang jumlah itu kepada anda. Sebahagian besar wang dalam ekonomi moden wujud dalam bentuk ini: angka dalam rekod institusi kewangan.

Bayaran elektronik dalam kehidupan harian

Rakyat Malaysia sudah biasa dengan perbankan dalam talian, FPX untuk membayar bil, dan DuitNow untuk memindahkan wang menggunakan nombor telefon, nombor MyKad atau kod QR. Semua ini kaedah *memindahkan arahan* antara institusi yang menyimpan rekod. Ringgit tetap ringgit; yang berubah hanyalah cara rekod dikemas kini.

Wang elektronik (e-money)

E-wallet yang anda gunakan untuk membayar tol atau membeli kopi menyimpan **wang elektronik**. Anda menukar RM50 daripada akaun bank, dan penerbit e-wallet merekodkan baki RM50 untuk anda. Nilainya sentiasa dalam ringgit: RM50 hari ini kekal RM50 esok.

♦ ISTILAH PENTING

Wang elektronik (e-money) — nilai tersimpan dalam ringgit yang dikeluarkan oleh penerbit yang dibenarkan, sebagai pertukaran kepada wang yang anda bayar. Ia boleh digunakan untuk membuat bayaran dan nilainya ditetapkan sama dengan ringgit.

Aset digital — istilah luas untuk nilai yang wujud dalam bentuk digital dan boleh dimiliki atau dipindahkan. Aset kripto ialah satu jenis aset digital.

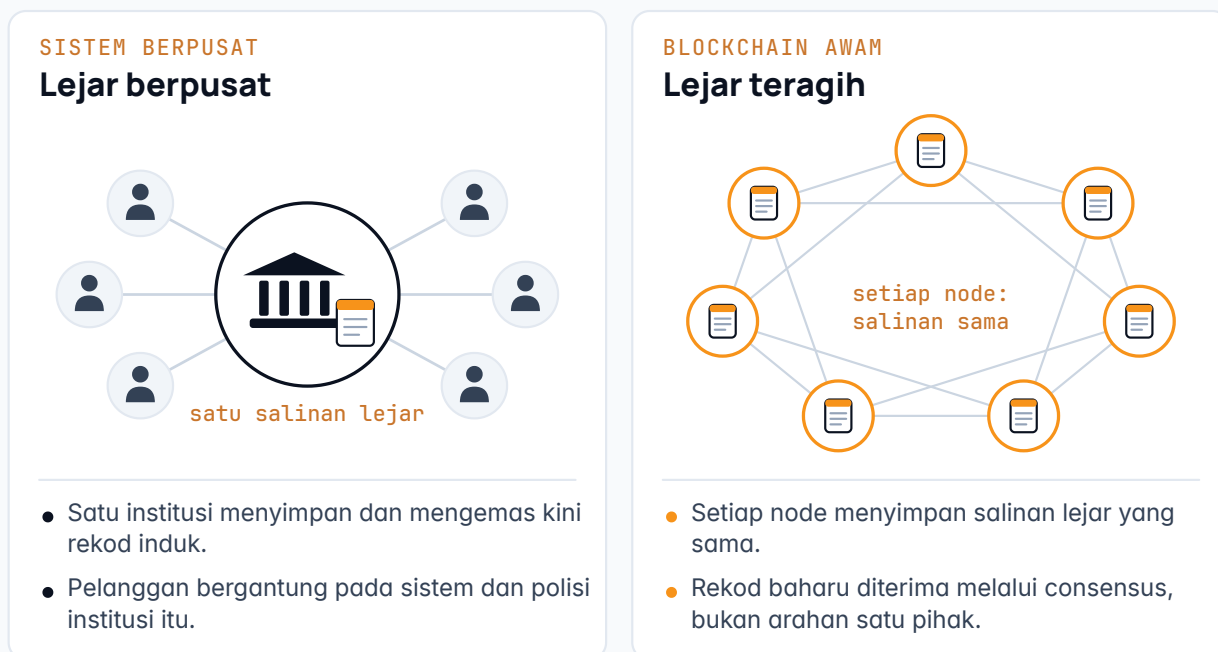
01.3 Lejar Berpusat: Siapa Memegang Buku Rekod?

Bank, penerbit e-wallet dan rangkaian pembayaran semuanya menggunakan **lejar berpusat**: satu pihak menyimpan rekod induk tentang siapa memiliki apa. Apabila anda memindahkan RM6 kepada peniaga kuih, bank yang terlibat mengemas kini rekod masing-masing, dan sistem pembayaran memastikan kedua-dua rekod sepadan.

Model ini mempunyai kelebihan yang besar. Ada pihak yang boleh disoal apabila berlaku kesilapan, ada prosedur aduan untuk pindahan yang salah, dan ada pengawal selia yang mengawasi institusi tersebut.

Kelemahannya, anda bergantung sepenuhnya pada institusi itu untuk jujur, cekap dan sentiasa beroperasi. Institusi boleh membekukan akaun atau menolak transaksi, dan pindahan merentas negara biasanya melalui beberapa bank perantara dengan kos tambahan.

Rajah CH01-002 membandingkan lejar berpusat dengan idea yang dibawa oleh blockchain: lejar yang salinannya dipegang dan disemak oleh banyak pihak.



RAJAH CH01-002 — Lejar Berpusat vs Lejar Teragih. Dalam sistem berpusat, satu pihak memegang rekod induk. Dalam blockchain awam, rekod dikongsi dan disemak oleh banyak pihak.

01.4 Mengapa Bitcoin Muncul

Krisis kewangan 2008

Pada 2008, sistem kewangan global dilanda krisis. Beberapa institusi kewangan besar runtuh atau terpaksa diselamatkan dengan dana awam, dan keyakinan terhadap bank merosot di banyak negara. Dalam suasana inilah, pada Oktober 2008, seseorang yang menggunakan nama samaran Satoshi Nakamoto menerbitkan kertas cadangan bertajuk *Bitcoin: A Peer-to-Peer Electronic Cash System* ^[TEC-001, TEC-002]. Kisah penuhnya diceritakan dalam Bab 02.

Idea asas: rekod tanpa penjaga tunggal

Cadangan Satoshi menjawab satu soalan teknikal yang sukar: bolehkah orang yang tidak saling mengenali bersetuju tentang siapa memiliki apa, tanpa bergantung pada satu bank atau syarikat sebagai penjaga rekod? Jawapan Bitcoin ialah lejar awam yang disalin ke ribuan komputer, dengan peraturan yang dikuatkuasakan oleh perisian dan kos pengiraan. Bagaimana mekanisme ini berfungsi akan diterangkan dalam Bab 02 dan Bab 03.

Crypto berbanding wang elektronik biasa

Ramai beginner menyangka crypto hanyalah "e-wallet versi baharu". Hakikatnya, perbezaannya asas, seperti yang ditunjukkan dalam jadual berikut.

CIRI	BAKI BANK	E-WALLET	BITCOIN
Penerbit	Bank	Penerbit e-money	Tiada penerbit tunggal
Nilai dalam RM	Tetap	Tetap	Turun naik
Penjaga rekod	Bank	Penerbit	Rangkaian node
Pembatalan	Ada prosedur	Ada prosedur	Hampir mustahil
Kaitan dengan ringgit	Tuntutan dalam ringgit	Tuntutan dalam ringgit	Bukan ringgit; bukan legal tender

Baris kedua paling penting bagi poket anda. RM1,000 dalam e-wallet ialah tuntutan terhadap ringgit. RM1,000 yang ditukar kepada Bitcoin ialah pemilikan sejumlah unit aset yang harganya ditentukan oleh pasaran setiap saat.

◇ CONTOH RM

Nilai yang tetap berbanding nilai yang turun naik

Andaikan secara hipotetikal anda menyimpan RM1,000 dalam e-wallet dan menukar RM1,000 lagi kepada sejenis aset kripto (abaikan yuran untuk kejelasan).

SENARIO SEBULAN KEMUDIAN (HIPOTETIKAL)	E-WALLET	ASET KRIPTO
Harga aset naik 20%	RM1,000.00	RM1,200.00
Harga aset turun 20%	RM1,000.00	RM800.00

Baki e-wallet tidak berubah dalam ringgit. Nilai aset kripto bergerak mengikut pasaran — ke atas atau ke bawah.

01.5 Daya Tarikan Crypto — dan Hadnya

Mengapa crypto menjadi popular

Rangkaian seperti Bitcoin beroperasi 24 jam sehari tanpa cuti umum, pemindahan merentas negara tidak memerlukan bank perantara, dan bekalannya dihadkan oleh peraturan yang telus. Sudah tentu, kenaikan harga yang ketara dalam beberapa tempoh juga menarik ramai orang yang berharap untung cepat.

Apa yang crypto tidak selesaikan

Crypto tidak menghapuskan keperluan untuk percaya — ia mengalihkan kepercayaan. Daripada mempercayai bank, anda kini perlu mempercayai kod, rangkaian, platform yang anda gunakan, dan yang paling penting, diri sendiri dalam menjaga akses akaun.

Crypto juga tidak menghapuskan penipuan. Menurut JSJK PDRM (dilaporkan Bernama/RTM, April 2026), sindiket penipuan pelaburan semakin menggunakan crypto seperti USDT, dengan mangsa diarah memindahkan dana ke wallet sindiket melalui platform yang tidak dibenarkan ^[SCM-013]. Rekod blockchain yang telus tidak bermakna wang yang dicuri mudah dikembalikan.

↔ FAKTA VS MITOS

Mitos: Oleh sebab semua transaksi direkod di blockchain, penipuan crypto mudah dijejak dan wang mudah dipulangkan.

Fakta: Rekod transaksi memang awam, tetapi alamat tidak semestinya mendedahkan identiti pemiliknya. Pindahan yang sudah disahkan tidak boleh dibatalkan oleh mana-mana pihak tengah. Pencegahan jauh lebih berkesan daripada usaha mendapatkan semula wang — topik ini dibincangkan dalam Bab 14.

01.6 Kajian Kes: Online Banking berbanding Pindahan Bitcoin

Untuk melihat perbezaan ini secara praktikal, mari bandingkan dua cara menghantar nilai yang sama kepada orang yang sama.

◆ KAJIAN KES

Menghantar RM500 kepada adik di Kuching

Senario: Anda di Petaling Jaya ingin menghantar RM500 kepada adik yang belajar di Kuching.

Kaedah A — DuitNow melalui perbankan dalam talian. Anda memasukkan nombor telefon adik, sistem memaparkan nama pemilik akaun untuk disemak, dan anda mengesahkan dengan TAC atau pengesahan aplikasi. Adik menerima tepat RM500 dalam akaun banknya.

Kaedah B — Pindahan Bitcoin. Anda membeli Bitcoin bernilai RM500 dan menghantarnya ke alamat wallet adik — rentetan aksara panjang tanpa nama pemilik. Transaksi disiarkan, dimasukkan ke dalam blok dan disahkan. Anda membayar network fee, dan adik perlu menjual Bitcoin itu untuk mendapatkan ringgit.

Perbandingan:

- *Perantara:* Kaedah A melalui bank dan rangkaian pembayaran; Kaedah B melalui rangkaian node tanpa pengendali pusat.
- *Semakan penerima:* Kaedah A memaparkan nama; Kaedah B hanya alamat.
- *Tersalah hantar:* Kaedah A mempunyai prosedur aduan bank, walaupun pemulihan tidak dijamin; Kaedah B hampir mustahil dibatalkan selepas disahkan.
- *Nilai yang diterima:* Kaedah A tepat RM500; Kaedah B bergantung pada harga ketika adik menjual, ditolak yuran.

Pengajaran: Untuk menghantar ringgit dalam negara, sistem perbankan sedia ada biasanya lebih mudah dan lebih selamat bagi pengguna biasa. Kekuatan Bitcoin terletak pada perkara lain — rangkaian terbuka tanpa penjaga tunggal — dan kekuatan itu datang bersama tanggungjawab yang lebih besar.

Rajah CH01-003 meringkaskan kedua-dua aliran ini. Kedua-duanya digital, tetapi struktur kepercayaan dan perlindungan pengguna sangat berbeza.

BAYARAN BANK DuitNow / IBG



PINDAHAN CRYPTO Bitcoin



ASPEK

	DuitNow / IBG	Bitcoin
Perantara	Bank dan operator rangkaian pembayaran	Tiada bank; miner dan node mengikut peraturan protokol
Waktu operasi	DuitNow 24/7; IBG mengikut kitaran pemprosesan bank	24/7; blok dihasilkan sepanjang masa
Pembatalan	Ada saluran aduan dan pertikaian melalui bank	Tidak boleh dibatalkan selepas disahkan
Identiti	Akaun terikat pada identiti pemilik (KYC)	Alamat pseudonim; exchange tetap melakukan KYC
Yuran	Ditetapkan oleh bank atau rangkaian pembayaran	Network fee berubah mengikut kesesakan rangkaian

RAJAH CH01-003 — Online Banking vs Pindahan Bitcoin. Kedua-duanya digital, tetapi struktur kepercayaan, kebolehbalian dan perlindungan pengguna sangat berbeza.

01.7 Kesilapan Biasa Beginner

1. **Menyangka crypto sama dengan e-wallet.** E-wallet menyimpan ringgit yang nilainya tetap; crypto ialah aset yang harganya turun naik.
2. **Menganggap "digital" bermaksud "selamat".** Bentuk digital tidak menjamin perlindungan. Siapa yang menjaga rekod dan apa prosedur apabila berlaku kesilapan jauh lebih penting.
3. **Menyangka crypto boleh digunakan seperti ringgit di Malaysia.** Crypto bukan legal tender dan tidak wajib diterima oleh sesiapa.
4. **Percaya bahawa transaksi yang direkod mudah dibatalkan.** Pindahan crypto yang sudah disahkan secara praktiknya muktamad.
5. **Melihat crypto hanya dari sudut harga.** Memahami masalah yang cuba diselesaikan — dan yang tidak diselesaikan — membantu anda menilai dakwaan yang berlebihan.

● RINGKASAN BAB

5 Perkara Utama

1. Wang sentiasa berubah bentuk, tetapi asasnya kekal: kepercayaan terhadap pihak yang merekod nilai.
2. Kebanyakan wang anda hari ini sudah digital, dalam bentuk rekod pada lejar berpusat bank dan penerbit e-money.
3. Wang elektronik bernilai tetap dalam ringgit; aset kripto mempunyai harga pasaran yang turun naik.
4. Bitcoin muncul selepas krisis kewangan 2008 sebagai cadangan lejar awam tanpa penjaga tunggal.
5. Crypto mengalihkan kepercayaan, bukan menghapuskannya, dan bukan legal tender di Malaysia.

5 Soalan Ulang Kaji

1. Apakah tiga fungsi wang, dan fungsi mana yang paling mencabar bagi crypto?
2. Apakah maksud lejar berpusat? Berikan satu contoh dalam kehidupan harian anda.

3. Apakah perbezaan utama antara RM100 dalam e-wallet dan RM100 dalam Bitcoin?
4. Mengapakah tahun 2008 penting dalam sejarah Bitcoin?
5. Mengapakah rekod blockchain yang telus tidak menjamin wang yang ditipu dapat dikembalikan?

Latihan Praktikal

Buka sejarah transaksi bulan lepas dalam aplikasi bank atau e-wallet anda. Kira berapa banyak bayaran yang menggunakan tunai berbanding digital. Untuk satu pindahan digital, senaraikan semua pihak yang terlibat memprosesnya.

→ SETERUSNYA

Kita sudah melihat bahawa wang digital bukan perkara baharu — yang baharu ialah idea lejar tanpa penjaga tunggal. Dalam Bab 02, kita berkenalan dengan Bitcoin secara terperinci: siapa penciptanya, bagaimana bekalannya dihadkan, dan mengapa kekurangan bekalan tidak semestinya bermaksud harga akan naik.

Apa Sebenarnya Bitcoin?

Sebuah kertas cadangan, sebuah blok pertama dan satu peraturan bekalan yang tidak boleh diubah sesuka hati. Inilah Bitcoin, tanpa gambar-gembur.

Pada 31 Oktober 2008, satu e-mel muncul dalam senarai mel kriptografi yang dibaca oleh segelintir pakar keselamatan komputer. Penghantarnya memperkenalkan diri sebagai Satoshi Nakamoto dan berkongsi pautan ke sebuah kertas cadangan tentang "wang tunai elektronik" yang boleh dihantar terus antara dua pihak tanpa melalui institusi kewangan ^[TEC-002]. Tiada majlis pelancaran, tiada iklan, tiada syarikat di belakangnya.

Hampir dua dekad kemudian, nama Bitcoin disebut di kedai kopi dari Alor Setar hingga Tawau — kadangkala dengan teruja, kadangkala dengan curiga. Bab ini menerangkan apa sebenarnya Bitcoin: dari mana ia datang, bagaimana bekalannya dikawal, bagaimana blok baharu dihasilkan, dan apa yang ia tawarkan serta tidak tawarkan.

© OBJEKTIF PEMBELAJARAN

Selepas bab ini, anda akan dapat:

- | | |
|---|--|
| 01 Menerangkan asal-usul Bitcoin, termasuk whitepaper dan genesis block. | 04 Menukar nilai ringgit kepada unit satoshi. |
| 02 Menerangkan maksud desentralisasi dalam konteks Bitcoin. | 05 Menerangkan secara konsep cara mining dan Proof of Work berfungsi. |
| 03 Memahami had bekalan kira-kira 21 juta BTC dan mekanisme halving. | 06 Menilai kekuatan dan had Bitcoin secara seimbang. |

02.1 Asal-usul: Satoshi Nakamoto, Whitepaper dan Blok Pertama

Kertas cadangan itu bertajuk *Bitcoin: A Peer-to-Peer Electronic Cash System* ^[TEC-001]. Ia mencadangkan cara untuk menghalang masalah "perbelanjaan berganda" — iaitu menghantar wang digital yang sama dua kali — tanpa memerlukan bank sebagai pengadil.

Sehingga hari ini, identiti sebenar Satoshi Nakamoto tidak diketahui. Pelbagai individu pernah didakwa sebagai Satoshi, tetapi tiada bukti yang diterima umum. Bagi pengguna, perkara ini kurang penting berbanding yang disangka: Bitcoin tidak bergantung pada penciptanya untuk terus beroperasi.

Rangkaian Bitcoin bermula pada 3 Januari 2009 (UTC) apabila blok pertama, dikenali sebagai **genesis block**, dihasilkan ^[TEC-004]. Di dalam blok itu, Satoshi menyelitkan tajuk berita akhbar *The Times* hari itu tentang Canselor Britain yang hampir melancarkan pakej penyelamatan kedua untuk bank. Ramai melihatnya sebagai cap masa dan juga mesej tersirat tentang sebab Bitcoin dicipta. Ganjaran 50 BTC dalam blok itu tidak boleh dibelanjakan.

♦ ISTILAH PENTING

Satoshi Nakamoto — nama samaran pencipta Bitcoin; identiti sebenar tidak diketahui.

Whitepaper — dokumen yang menerangkan reka bentuk teknikal sesuatu projek. Whitepaper Bitcoin diumumkan pada 31 Oktober 2008.

Genesis block — blok pertama (blok 0) dalam sesuatu blockchain. Genesis block Bitcoin bertarikh 3 Januari 2009 (UTC).

02.2 Desentralisasi: Tiada Ibu Pejabat Bitcoin

Tiada syarikat bernama "Bitcoin Berhad". Tiada CEO, tiada ibu pejabat dan tiada khidmat pelanggan. Bitcoin ialah satu set peraturan yang dijalankan oleh perisian sumber terbuka pada ribuan komputer di seluruh dunia. Setiap komputer ini, dipanggil **node**, menyimpan salinan rekod transaksi dan menyemak sendiri sama ada setiap transaksi dan blok mematuhi peraturan.

Inilah maksud **desentralisasi**: kuasa untuk mengesahkan rekod tidak dipegang oleh satu pihak. Jika satu node ditutup, rangkaian terus berjalan. Jika satu pihak cuba menukar peraturan secara sepihak, node lain akan menolak blok yang tidak mematuhi peraturan asal.

Namun desentralisasi bukan "semua atau tiada". Dalam amalan, sebahagian besar kuasa mining tertumpu pada beberapa *mining pool* besar, dan perubahan perisian dibincangkan oleh komuniti pembangun. Lebih tepat untuk melihat desentralisasi sebagai spektrum, dan Bitcoin berada jauh lebih dekat ke hujung terdesentralisasi berbanding kebanyakan sistem kewangan lain.

02.3 Bekalan Terhad dan Halving

Kira-kira 21 juta, tepatnya sedikit kurang

Peraturan Bitcoin menetapkan bahawa hanya kira-kira 21 juta BTC akan wujud ^[TEC-003]. Angka teoritis yang tepat ialah 20,999,999.9769 BTC, sedikit kurang daripada 21 juta kerana pembundaran dalam unit terkecil ^[TEC-005]. BTC baharu dikeluarkan sebagai ganjaran kepada miner yang berjaya menghasilkan blok, dan pengeluaran terakhir dijangka sekitar tahun 2140.

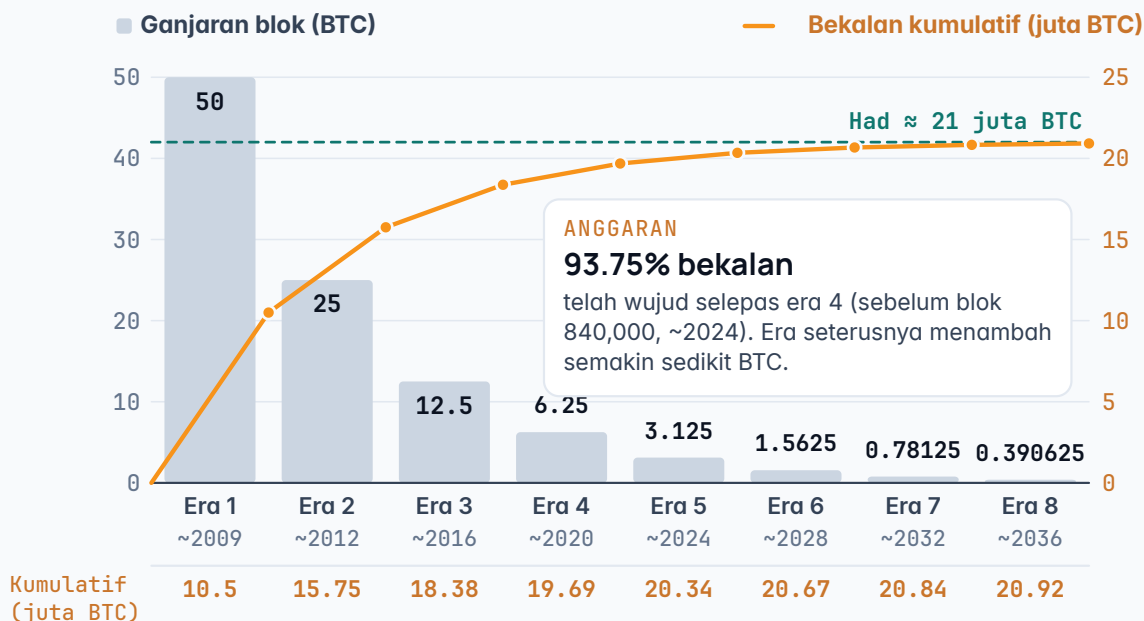
Halving: ganjaran dipotong separuh

Ganjaran blok baharu, dipanggil *block subsidy*, dipotong separuh setiap 210,000 blok — lebih kurang setiap empat tahun ^[TEC-005]. Peristiwa ini dipanggil **halving**.

HALVING	BLOK	TARIKH (UTC)	GANJARAN BLOK
—	0	3 Jan 2009	50 BTC
Pertama	210,000	28 Nov 2012	25 BTC
Kedua	420,000	9 Jul 2016	12.5 BTC
Ketiga	630,000	11 Mei 2020	6.25 BTC
Keempat	840,000	20 Apr 2024	3.125 BTC
Kelima	1,050,000	Sekitar 2028 (anggaran)	1.5625 BTC

Tarikh halving seterusnya hanya boleh dianggarkan kerana masa setiap blok berbeza-beza ^[TEC-006]. Rajah CH02-001 menunjukkan bagaimana ganjaran yang menurun separuh menyebabkan lengkung bekalan semakin mendatar menghampiri had.

DIKIRA DARIPADA PERATURAN PROTOKOL • TAHUN IALAH ANGGARAN



RAJAH CH02-001 — Jadual Ganjaran Blok dan Bekalan Bitcoin. Ganjaran blok separuh setiap 210,000 blok. Bekalan kumulatif dikira daripada peraturan protokol; tahun adalah anggaran.

Dikira daripada peraturan protokol (210,000 blok setiap era); tahun ialah anggaran.

Hasilnya, sebahagian besar Bitcoin sudah pun dikeluarkan. Sehingga Oktober 2026, kira-kira 20.1 juta BTC telah dilombong — lebih kurang 95.7% daripada had 21 juta ^[TEC-008]. BTC yang ke-20 juta dilombong pada Mac 2026 ^[TEC-009]. Baki kurang daripada satu juta BTC akan dikeluarkan secara perlahan sepanjang lebih satu abad akan datang.

Jadual bekalan berbanding dasar monetari bank pusat

Di Malaysia, BNM menguruskan dasar monetari — misalnya melalui Kadar Dasar Semalaman (OPR) — dan boleh bertindak balas terhadap keadaan ekonomi, sama ada untuk menyokong pertumbuhan atau mengekang inflasi. Fleksibiliti ini membolehkan bank pusat bertindak semasa krisis.

Bitcoin mengambil pendekatan sebaliknya. Jadual bekalannya ditetapkan dalam kod dan tidak bertindak balas terhadap keadaan ekonomi. Mengubahnya memerlukan persetujuan meluas daripada pengguna yang menjalankan node — sesuatu yang secara praktiknya sangat sukar. Bagi peminatnya, ini kekuatan: tiada pihak boleh "mencetak" lebih banyak Bitcoin. Bagi pengkritiknya, ini kelemahan: tiada mekanisme untuk menstabilkan nilai apabila keadaan berubah.

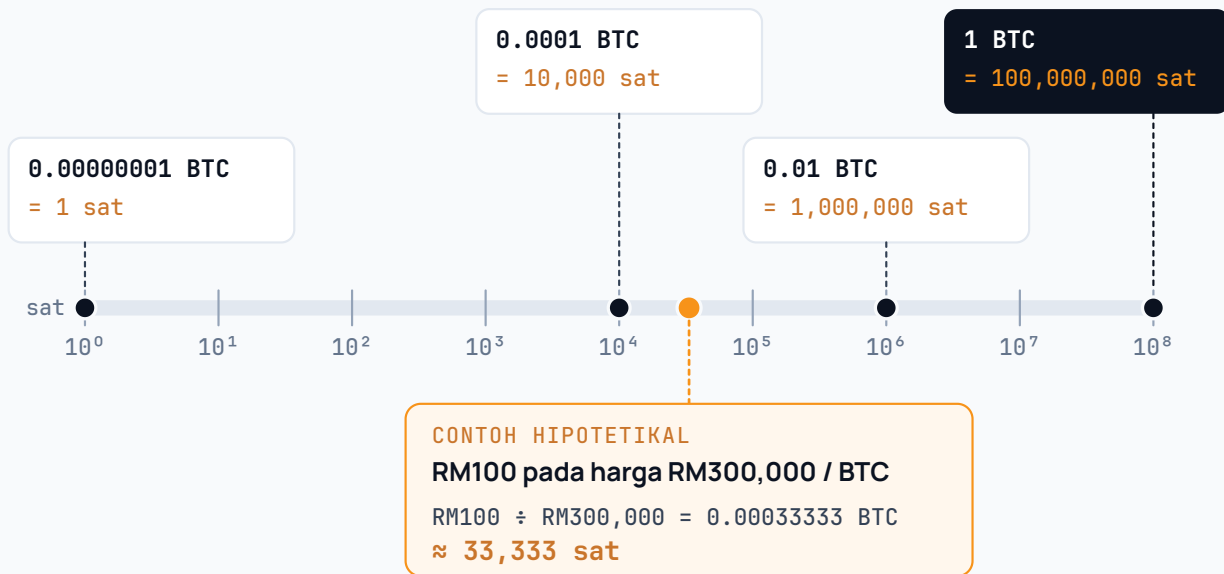
↔ FAKTA VS MITOS

Mitos: Bekalan Bitcoin terhad, jadi harganya pasti naik dalam jangka panjang.

Fakta: Harga ditentukan oleh bekalan *dan* permintaan. Bekalan yang terhad tidak menjamin permintaan akan kekal atau meningkat. Banyak token dengan bekalan terhad telah jatuh hampir ke sifar kerana tiada siapa lagi mahu membelinya. Kekurangan ialah ciri reka bentuk, bukan janji harga.

02.4 Satoshi: Anda Tidak Perlu Membeli Satu BTC Penuh

Satu BTC boleh dibahagikan kepada 100,000,000 unit terkecil yang dipanggil **satoshi** atau "sat" — iaitu lapan tempat perpuluhan, 0.00000001 BTC ^[TEC-003]. Apabila anda membeli dengan jumlah ringgit tertentu, anda sebenarnya membeli pecahan BTC, bukan satu unit penuh. Jumlah minimum pembelian berbeza mengikut platform (Bab 08 dan Bab 09). Rajah CH02-002 menunjukkan skala unit ini.



Skala logaritma: setiap sela ke kanan = 10 kali ganda.

RAJAH CH02-002 — Unit Satoshi. Anda tidak perlu membeli satu Bitcoin penuh. Contoh harga RM300,000 adalah hipotetikal.

◇ CONTOH RM

Berapa satoshi untuk RM100?

Andaikan harga hipotetikal 1 BTC = RM300,000 (abaikan yuran).

FORMULA

Jumlah BTC = Jumlah RM ÷ Harga 1 BTC
RM100 ÷ RM300,000 = 0.00033333 BTC ≈ 33,333 sat

Dengan RM10 pula, anda mendapat kira-kira 3,333 sat.

Sekarang andaikan harga BTC berubah, tetapi anda tidak membeli atau menjual:

- Harga naik 20% → 33,333 sat anda bernilai kira-kira RM120.
- Harga turun 20% → 33,333 sat yang sama bernilai kira-kira RM80.

Bilangan sat anda tidak berubah; yang berubah ialah nilai ringgitnya.

02.5 Mining dan Proof of Work

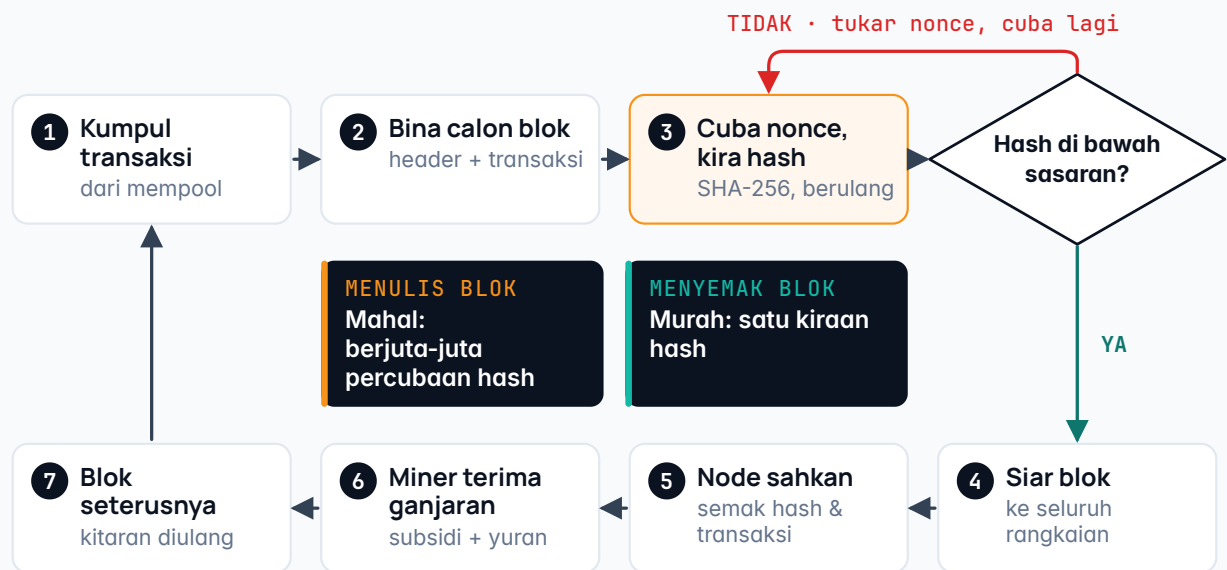
Bagaimanakah rangkaian tanpa ketua memutuskan siapa yang berhak menambah blok seterusnya? Jawapan Bitcoin ialah **Proof of Work**.

Miner mengumpul transaksi yang sedang menunggu, menyusunnya menjadi calon blok, kemudian berulang kali menukar satu nombor kecil dalam blok itu (dipanggil *nonce*) dan mengira hash-nya. Matlamatnya ialah mencari hash yang lebih kecil daripada sasaran yang ditetapkan oleh rangkaian. Tiada jalan pintas; satu-satunya cara ialah mencuba berbilion-bilion kali. Konsep hash diterangkan dengan lebih lanjut dalam Bab 03.

Miner pertama yang menemui jawapan menyiarkan bloknya. Node lain menyemak jawapan itu — proses yang sangat cepat dan murah — dan jika sah, blok itu diterima. Miner tersebut menerima ganjaran blok serta semua network fee daripada transaksi dalam blok itu. Kemudian perlumbaan bermula semula.

Purata satu blok dihasilkan setiap kira-kira 10 minit ^[TEC-003]. Untuk mengekalkan kadar ini walaupun lebih ramai miner menyertai, tahap kesukaran dilaraskan setiap 2,016 blok, iaitu lebih kurang setiap dua minggu ^[TEC-007].

Rajah CH02-003 menunjukkan kitaran ini.



Purata ~10 minit setiap blok; tahap kesukaran dilaras setiap 2,016 blok.

RAJAH CH02-003 — Kitaran Proof of Work. Proof of Work menjadikan penulisan blok mahal, tetapi semakan oleh node lain murah dan pantas.

● MUDAH FAHAM

Seperti mencari kombinasi mangga

Bayangkan ribuan orang serentak cuba membuka mangga nombor dengan mencuba setiap kombinasi satu demi satu. Orang pertama yang berjaya menunjukkan kombinasinya, dan sesiapa sahaja boleh menyemaknya dalam sesaat.

Di mana analogi ini tidak tepat: dalam Bitcoin, "kombinasi" yang sah bukan satu sahaja, tahap kesukaran dilaraskan secara automatik, dan kos sebenar ialah tenaga elektrik serta perkakasan khusus. Kos inilah yang menjadikan penulisan semula sejarah blok sangat mahal.

02.6 Nilai dan Had Bitcoin

Apa yang ditawarkan

Bitcoin menawarkan beberapa ciri yang sukar ditiru oleh sistem tradisional: bekalan dengan peraturan yang telus, rangkaian yang beroperasi tanpa henti, pemindahan nilai tanpa memerlukan kebenaran mana-mana pihak tengah, dan pilihan untuk memegang aset sendiri melalui private key (Bab 05). Rekod sejak 2009 boleh disemak oleh sesiapa sahaja.

Had dan risiko

Bitcoin juga mempunyai had yang nyata. Harganya sangat volatile, menjadikannya kurang sesuai sebagai alat pembayaran harian atau unit akaun. Kapasiti rangkaian untuk memproses transaksi terhad, dan network fee boleh meningkat apabila rangkaian sibuk. Mining menggunakan tenaga elektrik yang besar, satu isu yang terus dibahaskan. Kesilapan pengguna — tersalah alamat atau kehilangan private key — biasanya tidak boleh dipulihkan. Anggaran jumlah BTC yang hilang selama-lamanya pula berbeza-beza antara penganalisis.

▲ AMARAN RISIKO

Bitcoin bukan simpanan tetap

Risiko: Harga Bitcoin boleh jatuh dengan ketara dalam tempoh yang singkat, dan tiada jaminan ia akan pulih.

Akibat: Jika anda memerlukan wang itu ketika harga rendah, kerugian menjadi nyata.

Cara mencegah: Jangan gunakan wang perbelanjaan, simpanan kecemasan atau wang pinjaman. Saiz kedudukan dan pengurusan risiko dibincangkan dalam Bab 13.

02.7 Kesilapan Biasa Beginner

1. **Menyangka perlu membeli satu BTC penuh.** Anda boleh membeli pecahan BTC; jumlah minimum bergantung pada platform.
2. **Mempercayai dakwaan seseorang ialah "Satoshi".** Identiti Satoshi tidak diketahui; dakwaan sebegini sering digunakan untuk mempromosikan skim.
3. **Menyamakan bekalan terhad dengan harga pasti naik.** Permintaan boleh jatuh, dan harga mengikutnya.
4. **Menganggap halving sebagai isyarat beli yang dijamin.** Halving hanya mengurangkan bekalan baharu; kesannya terhadap harga tidak pasti dan tidak boleh diramal.
5. **Melihat Bitcoin sebagai syarikat.** Tiada pihak yang boleh dihubungi untuk membatalkan transaksi atau memulangkan aset.

● RINGKASAN BAB

5 Perkara Utama

1. Whitepaper Bitcoin diumumkan pada 31 Oktober 2008 oleh Satoshi Nakamoto, dan genesis block dihasilkan pada 3 Januari 2009 (UTC).
2. Bitcoin dijalankan oleh rangkaian node tanpa pihak pusat; desentralisasinya ialah spektrum, bukan mutlak.
3. Bekalan dihadkan kira-kira 21 juta BTC; ganjaran blok dipotong separuh setiap 210,000 blok, dan kira-kira 20.1 juta BTC telah dilombong setakat Oktober 2026.
4. Proof of Work menjadikan penghasilan blok mahal tetapi semakannya murah.
5. 1 BTC = 100,000,000 sat; bekalan terhad tidak menjamin kenaikan harga.

5 Soalan Ulang Kaji

1. Apakah masalah utama yang cuba diselesaikan oleh whitepaper Bitcoin?
2. Apakah yang berlaku pada halving April 2024?
3. Bagaimanakah jadual bekalan Bitcoin berbeza daripada dasar monetari BNM?
4. Mengapakah node lain boleh menyemak blok dengan cepat walaupun menghasilkannya sangat sukar?
5. Jika harga hipotetikal 1 BTC ialah RM300,000, berapa sat yang anda peroleh dengan RM100?

Latihan Praktikal

Pilih satu jumlah yang realistik bagi anda — contohnya RM50. Dengan harga hipotetikal RM300,000 bagi 1 BTC, kira jumlah BTC dan sat yang diperoleh. Kemudian kira nilainya jika harga naik 30% dan jika harga turun 30%. Tulis satu ayat tentang perasaan anda terhadap kedua-dua keputusan itu.

→ SETERUSNYA

Kita sudah beberapa kali menyebut blok, hash dan node. Dalam Bab 03, kita membuka "enjin" di bawah Bitcoin — blockchain — dan mengikuti perjalanan satu transaksi dari saat ia dihantar hingga disahkan, tanpa memerlukan latar belakang teknikal.