

SCDO Laboratory · TECH PR · UNIT 01

Automated Contract Ledgers for AI Agents · Next-Gen Smart Payments

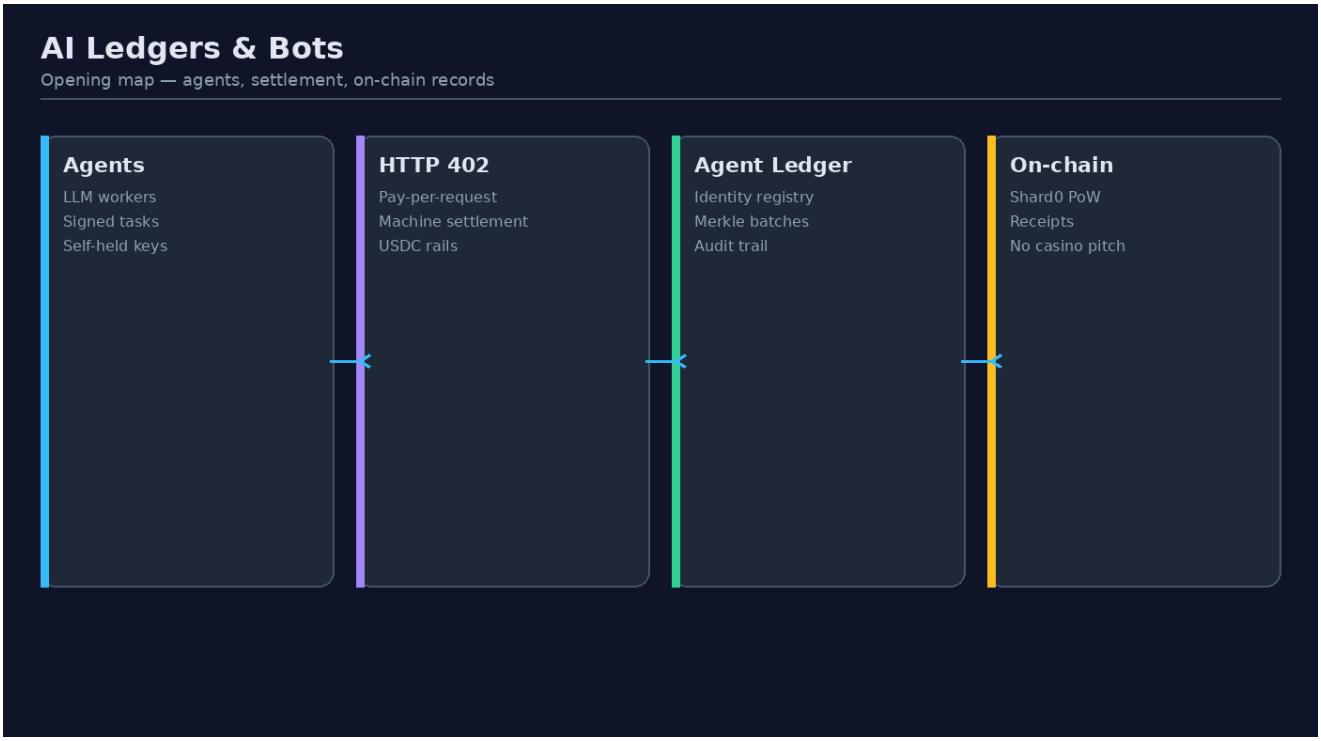
Genesis Block: Where AI Ledgers Begin

How Bitcoin turns trust into a verifiable ledger · Ying Willam Zhang · 2026

> Disclaimer: This primer is for education only — not investment, legal, or tax advice.

1. Bitcoin (starting from AI ledgers and bots)

SCDO Lab · *Automated Contract Ledgers for AI Agents · Next-Gen Smart Payments* · v2
Chinese: `01-bitcoin.md`
We open with **AI agent contract ledgers** and **bot per-call commerce**: why machines need verifiable books and keys—then return to Bitcoin as the peer-cash / PoW origin.
Not investment advice.



Opening: AI Ledger, bots, then Bitcoin

When an **AI agent** calls APIs, pays stablecoins, or writes work digests to a ledger, it needs:

1. **Self-held keys** (who signs is accountable);
2. **Checkable trails** (Agent Ledger / contract events);
3. **Micropayments** (HTTP 402 / x402, ~1¢ intuition).

None of that appeared from nowhere—it stands on Bitcoin’ s tradition of **public ledgers** + **private-key signatures** + **PoW anti-forgery**. This chapter explains Bitcoin in plain language as the foundation for later SCDO five-chain, mining, bots, and smart-payments chapters.

SCDO Lab · Web3 Primer for Newcomers v2 · English edition
This chapter explains in plain English: what Bitcoin is, why the internet alone cannot move “unique money,” how nodes and mining cooperate, keys and wallets, farms and pools.
Not investment advice. Price stories are history, not recommendations.

Opening: say it in human words

Bitcoin (BTC) is a **digital money system with no company boss and no central clearing bank**. Many people worldwide run the same open-source software (nodes) and jointly maintain a public transaction ledger—the **blockchain** people talk about is, in Bitcoin’s case, that continuously extended chain of ledger pages.

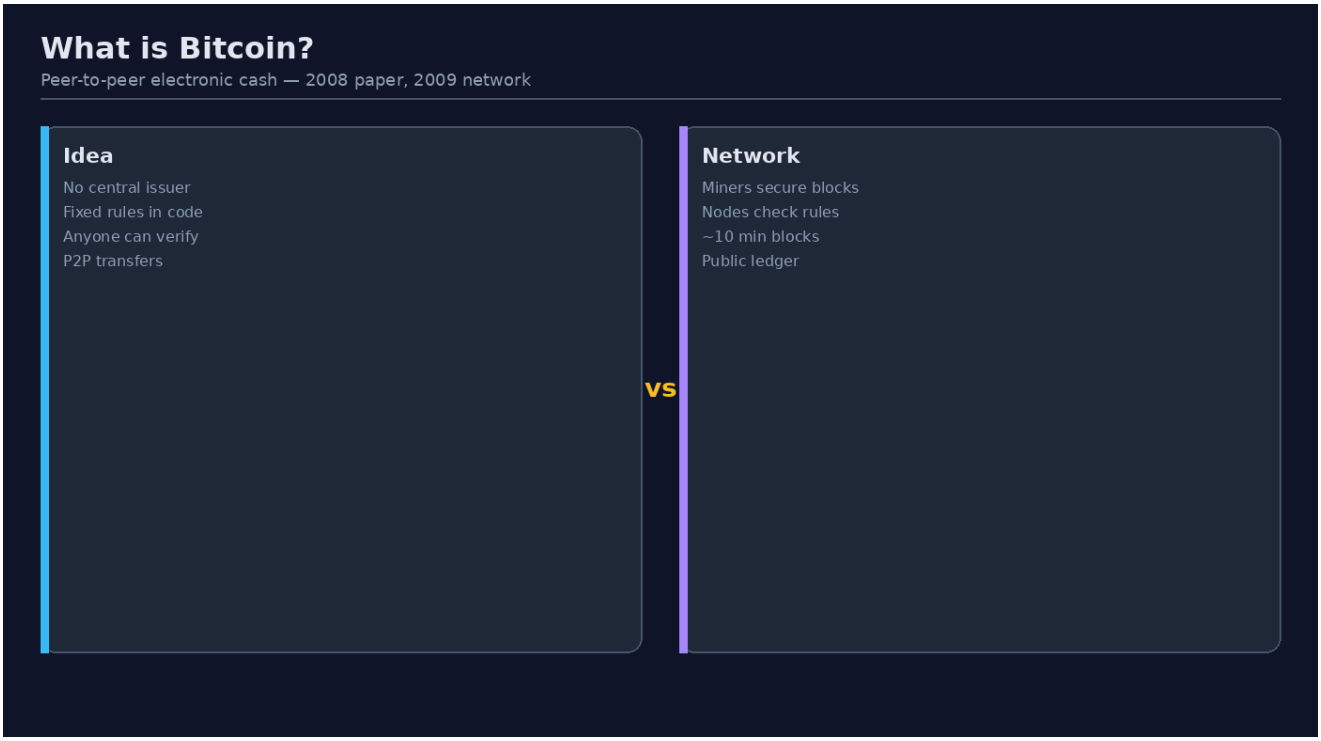
Think of three stacked pieces:

1. **A rule set** (protocol and software): who may write the ledger, how money moves, how supply is issued.
2. **A globally shared ledger**: transfers are public and checkable, without binding your legal name.
3. **A bookkeeping reward**: whoever packages a valid new block under the rules may earn newly issued bitcoin plus fees—that is mining incentive.

Supply has a rule-bound ceiling (commonly about **21 million** coins). New coins enter circulation on a schedule through mining; roughly every four years a “halving” cuts the block subsidy. No central bank can mint more by decree; changing the rules means persuading enough network participants—which is extremely hard in practice.

Five blocks below: double-spending, how it works, why it stays special, consensus basics, keys/wallets, farms/pools.

What is Bitcoin?



In 2008 a white paper under the name Satoshi Nakamoto proposed peer-to-peer electronic cash; the network launched in 2009. Over more than a decade it saw booms, crashes, fork fights, and regulatory storms—and became many people’s first blockchain lesson.

The first question for a newcomer is not “will it moon,” but:

> **The internet already moves photos and files. Why did moving “money” used to require WeChat Pay, Alipay, or a bank as middleman—and what puzzle does Bitcoin claim to complete?**

The internet’s “missing piece”? — Double-spending

Sending a photo online is easy: after you send it, your copy usually remains. You sent a **copy**.

Money cannot work that way. If I “send” you 100 units and can still spend the same 100, two people are spending one pot—that is **double-spending**.

Pure copy-paste internet transfer cannot solve double-spending. In real life we use **intermediated ledgers**:

- When you send 100 via a payment app, the company updates its central database: my balance −100, yours +100.
- Bank wires and card networks are similar: a trusted institution (or set of them) has the final say.

Intermediaries are useful—and costly: onboarding, compliance checks, freezes, outages, fees, data on someone else’s servers. You trust an **institution**, not math and public rules

themselves.

Bitcoin’s aim: without depending on a single giant bookkeeper, make “I pay you 1 BTC” eventually mean the whole network agrees **I have less and you have more**, and history is hard to rewrite quietly. The ledger tech underneath is often called a building block of a “value internet.” The slogan is a bit marketing, but the direction is right: the internet shipped information transfer; Bitcoin ships **scarce digital value transfer**.

Two boundaries:

- Bitcoin is not “fully anonymous cash.” The ledger is public; addresses are like pen names. If an address ties to your identity, trails can be analyzed. More accurate term: **pseudonymous**.
- “No intermediary” means **settlement and bookkeeping need not go through one payment company**; you may still buy via exchanges or custodial wallets—those layers have their own risks.

How does Bitcoin work? — A public game

Picture a **voluntary large-scale collaboration game** (rules live in software):

1. **Anyone can join or leave**: with a networked computer you can download node software and store (or verify) the ledger; quit when you want.
2. **Writing blocks is competitive and costly**: roughly every ten minutes the network produces a new block. Miners race on hard-to-guess, easy-to-check computations—**PoW (Proof-of-Work)**. More hashpower raises short-term odds; nobody is guaranteed the next second.
3. **Transfers are broadcast**: your transaction propagates; miners select txs into blocks. Nodes check signatures, unspent funds, and double-spends.
4. **Changing rules or history is extremely hard**: rewriting confirmed history or forcing issuance changes needs overwhelming hashpower and social consensus; most participants reject invalid branches.

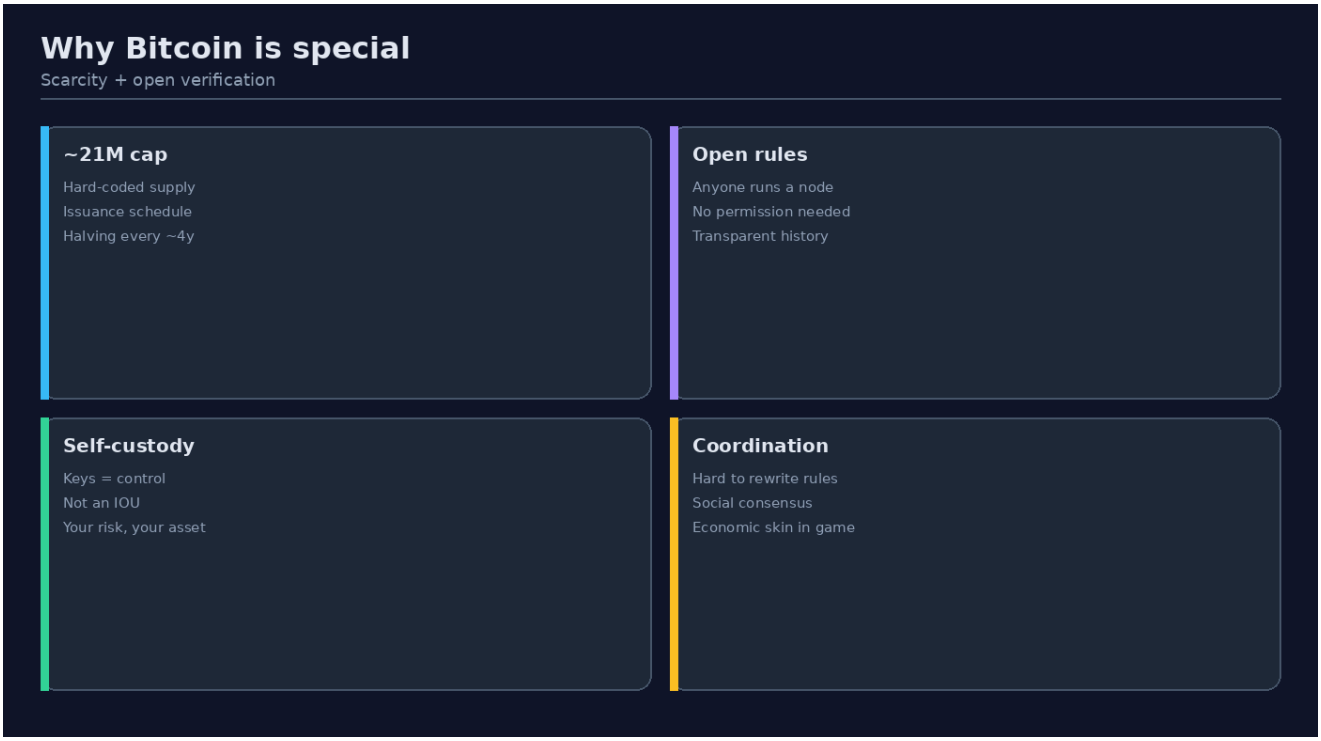
Why burn electricity forever? Successful blocks earn a **block subsidy** (new coins) and user **fees**. Incentives make strangers secure the network: attacking is often too expensive; following rules can pay—that is Bitcoin welding **cryptography** + **economics**.

Versus a payment app in one line:

- App: one company edits two balances.
- Bitcoin: thousands of machines write the change into a shared ledger under common rules, with layered confirmation.

Versus “game points”: points are a company database row the vendor can edit or shut down; bitcoin balances are unspent outputs on a public ledger controlled by your private key—there is no HQ support that can one-click restore them.

Why Bitcoin is still special



(The original manuscript pasted long institutional report translations here. v2 **does not reprint**. Below is our short judgment frame.)

Thousands of tokens exist. Why do many people still keep Bitcoin in its own column? Not because it "only goes up," but because its design trade-offs differ from many other chains.

1. Network and coin are bound together

"Bitcoin" means both the **network** (the protocol people run) and the **coin** (the native unit). You can copy the code and start another chain—that is **another network and another coin**, not automatically "canonical Bitcoin." You also cannot losslessly copy BTC onto arbitrary other chains and still call it the same BTC (bridges are a different trust model; later chapters).

2. More like a digital-age monetary commodity than company equity

No dividends, no CEO earnings call. What people emphasize is transferability, divisibility, verifiable scarcity, and hard unilateral inflation. It is more often discussed as a candidate **store of value / settlement asset** than as "the next unicorn stock." That does not guarantee it wins—it means the **evaluation frame differs**: do not force PE-style valuation onto it.

3. Scarcity rules are hard to change because of social consensus + incentives, not only a line of code



The ~21M cap is in the rules; code can theoretically change. What makes the cap “hard” is holders, miners, exchanges, wallets, and node operators—most refuse dilution. Changing the cap fights their own economic interest; coordination cost is huge. Newcomers should learn: **security comes from cryptography and from people unwilling to collude to rewrite the rules.**

4. “Improving Bitcoin” is usually a different trade-off, not a free upgrade

Later public chains often push speed, smart contracts, and fees harder—usually paying in **decentralization, security, or simplicity**. Bitcoin stays conservative: limited scripting, slow upgrades, in exchange for long-run censorship resistance and “few knives.” Other projects can serve other needs (contracts, games, DeFi); they need not annihilate each other. If your goal is “the most conservative digital scarce asset,” your scorecard should differ.

5. By 2026 the outside world also changed

Institutional rails (e.g. spot ETFs in some markets), custody, and compliant trading change **how ordinary people touch BTC**, not the ledger’s own rules. Easier on-ramps do not mean coins on an exchange equal “you control Bitcoin”—custody risk is separate. On scaling, the base layer stays restrained; smaller high-frequency needs lean on Lightning-style layer-two ideas (Chapter 4 develops the Ethereum side; Bitcoin is similar: L1 for stability, L2 for speed).

One line: Bitcoin is special because it minimizes “who decides” and prioritizes scarcity and security; other chains are special because they prioritize programmability and performance. Which path depends on the problem you solve.

Consensus: PoW, PoS, DPoS

Newcomers keep hitting these acronyms. Do not fear the English: **consensus** = **the rules by which mutually distrusting parties decide who writes the next ledger page and whether it is valid.**

Family vote on a trip: majority rules—that is one consensus. Blockchains must bookkeep globally with possible adversaries, so rules are harder and often bind real rewards and penalties.

A beginner triad (more variants exist; these three unlock the news):

PoW (Proof-of-Work)

- **Who writes:** race on hashpower; first valid solution roughly wins the block.
- **Pros:** relatively open entry; attacks cost real hardware and electricity; Bitcoin uses PoW.
- **Cons:** energy and hardware arms races; home laptops no longer mine BTC economically.
- **Plain:** whoever keeps paying verifiable “labor” (compute) gets higher odds of bookkeeping rewards.

PoS (Proof-of-Stake)

- **Who writes:** stake coins as collateral; selection/rotation under rules; misbehavior may be slashed.
- **Pros:** usually far less electricity; confirmations can be designed faster.
- **Cons:** “rich get more say” concerns; staking, liquidity, and penalties are more complex.
- **2026 note: Ethereum completed The Merge in 2022; mainnet is PoS, not PoW mining.** Old “mine ETH with GPUs” articles are history. Bitcoin remains PoW; both paths coexist.

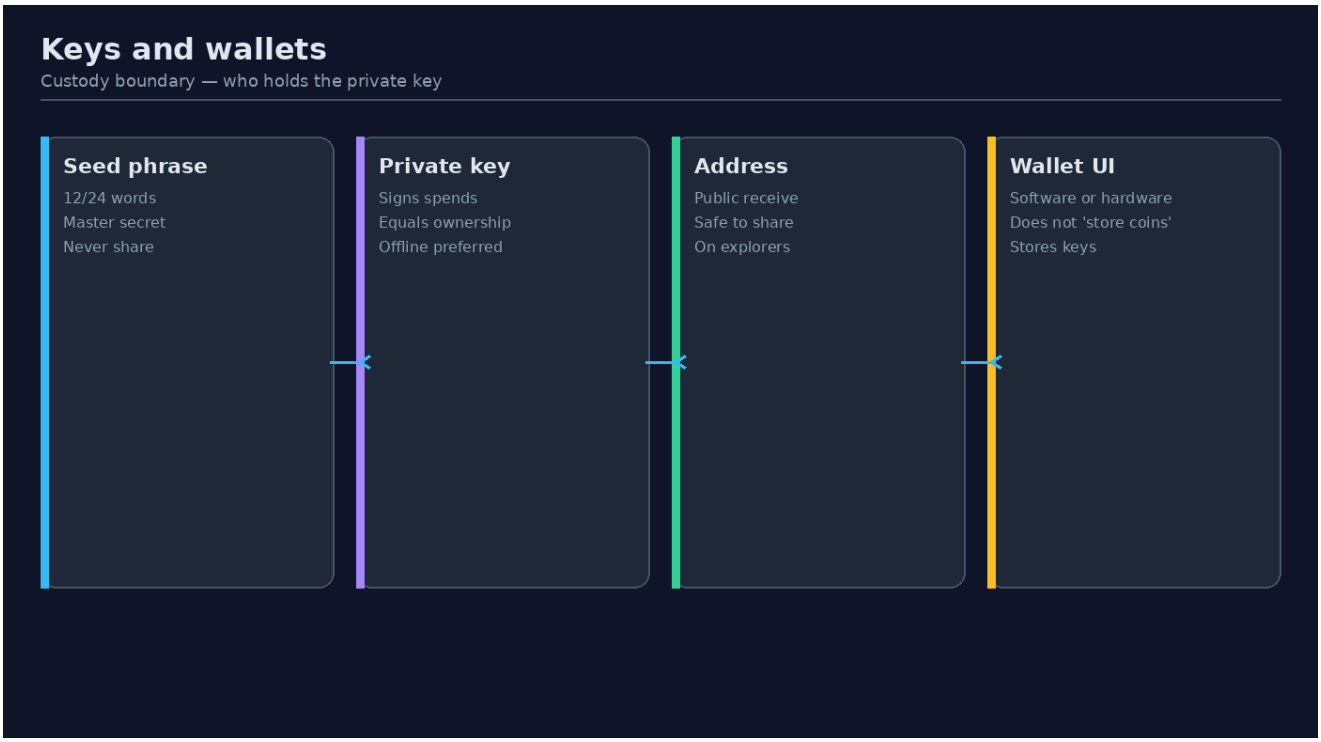
DPoS (Delegated Proof-of-Stake)

- **Who writes:** like shareholders electing a board—token holders vote a small set of producers.
- **Pros:** fewer nodes, faster coordination, often higher throughput.
- **Cons:** more like an elected committee; usually weaker decentralization than large PoW/PoS; watch vote-buying and oligopoly.

Wrap-up

No perfect consensus—only trade-offs among security, decentralization, and speed (a simplified "impossible triangle"). When reading a project ask: who may propose blocks? what does attack cost? can ordinary users run verifying nodes? Bitcoin's choice is clear—**favor security and decentralization; accept modest base-layer throughput.**

Private keys, accounts, and wallets



Three things closest to users: **private key, address (account), wallet software**. Intuition first; few formulas.

Public-key crypto (intuition)

Modern cryptography can generate a key pair:

- **Private key:** your secret, used to **sign** ("I authorize this spend").
- **Public key:** derived from the private key; others **verify** signatures but cannot easily reverse to the private key.

In Bitcoin: the private key controls coins; the network checks math without you broadcasting the private key.

What is a private key?

Essentially a **random number from a vast space** (often encoded as a character string). Whoever holds it can spend the corresponding coins.

Therefore:

- **Leak ≈ lose coins**, often irreversibly.
- **Lose with no backup ≈ coins still on-chain, forever unspendable by you**.
- Do not screenshot to albums, send in chat apps, or type into unknown “custody” pages.

What is a Bitcoin account / address?

Daily “Bitcoin account” usually means an **address**: characters derived from hashing the public key (formats differ). Others send to your address; the chain records payments among addresses.

More precisely Bitcoin uses UTXO: your “balance” is the sum of **unspent outputs**, not a single bank-style field. Beginner line: **addresses receive; private keys authorize spends.**

What is a wallet?

A wallet mainly **holds keys, shows balances, builds and signs transactions**.
Coins are on-chain; the wallet holds keys—not a pile of coin files.

Type	Trait	Fit
Hot wallet	Online phone/browser/desktop apps	Small daily amounts
Cold wallet	Keys offline (hardware, offline signing)	Larger long-term holds
Custodial wallet	Exchange etc. holds for you	Convenience; you take platform risk

First setup often shows a **seed phrase**: words that derive keys. The seed is a master key—anyone with it can empty the wallet. Write offline, multiple backups, never type it into networked forms.

You sign locally, then broadcast; after miner inclusion and confirmations, the recipient may treat it as received.

Mining farms and pools

Mining evolved from “laptop hobby” into a specialized industry. Three words often get mixed:

1. Mining machines

Specialized compute. Evolution line to remember:

CPU → GPU → FPGA → ASIC (application-specific chips)

Bitcoin today is dominated by ASICs: they mainly do mining hashes, far more efficient than PCs. Home PCs mining BTC is generally uneconomic.

2. Farms

Places that pack machines with power, cooling, and ops. Why concentrate?

- **Electricity** is often the largest cost—sites chase cheap stable power;
- Professional ops beat basement hobbyist reliability;
- Noise, heat, and compliance are hard at home.

Farms are a **physical and ops** business: host machines, keep uptime.

3. Pools

Mining is like buying lottery tickets: small hashpower may wait long for a "winning ticket" (a block), so income is lumpy. Miners **logically pool** hashpower:

- The pool assigns work;
- Contributors share rewards by valid shares (payout schemes vary);
- Small miners get smoother cash flow without running full solo block workflows.

Plain: **the farm is the factory; the pool is the project lead.**
Machines can sit in farm A while hashpower points to pool B—physical hosting and logical payouts can be chosen separately.

Large pools raise centralization concerns. Healthy networks prefer dispersed pools and migratable miners. If you do not mine, remember: **a large share of network security budget comes from hashpower competing for rewards.**

Chapter wrap

Five takeaways:

1. The internet copies information well; **money cannot be copied**, or you get double-spending.
2. Centralized payments rely on institutional ledgers; Bitcoin relies on a **globally replicated rule ledger** + **incentives**.
3. Bitcoin is deliberately conservative on scarcity and censorship resistance; **it is a different exam from other public chains**.
4. **Private key** = **ownership**; a wallet is a keychain, not the bank vault itself.
5. Machines/farms/pools industrialize PoW security; you can still run a verifying node without mining.

Next chapter leaves "one money system" for the larger **Web3** basket: when accounts, contracts, identity, and apps move on-chain, what newcomers actually meet—and which

parts are foam versus usable skill.

(End of Chapter 1 · v2 English edition · SCDO Lab)