

SCDO Laboratory · TECH PR · UNIT 01

AI智能體的合約賬本自動化 · 下一代智能支付系統

創世區塊：AI賬本從哪開始

比特幣如何把信任寫成可驗證賬本 · Ying Willam Zhang · 2026

免責聲明：本書內容僅供學習與科普，不構成投資、法律或稅務建議。

1、比特币（从 AI 账本与机器人说起）

SCDO Lab · 《AI智能体的合约账本自动化》· 下一代智能支付系统 · v2
全书从 **AI 智能体合约账本** 与 **机器人按次商务** 切入：先理解为何机器需要可验证账本与钥匙，再回到比特币——点对点现金与 PoW 的原点。
非投资建议。



开篇：AI Ledger、Bots，然后才是比特币

当你让一个 **AI agent** 替你调用 API、付稳定币、或把工作摘要写进账本时，它需要：

1. **自持钥匙**（谁签名谁负责）；
2. **可核对痕迹**（Agent Ledger / 合约事件）；
3. **小额结算**（HTTP 402 / x402、约 1¢ 直觉）。

这些能力不是从天而降——它们站在比特币开启的 **公开账本** + **私钥签名** + **PoW 防伪** 传统之上。本章用大白话讲比特币，作为后文 SCDO 五链、挖矿、Bots 与智能支付的地基。

SCDO Lab · Web3 新人必读指南 v2
本章用大白话讲清：比特币是什么、为什么互联网本身转不了“唯一的钱”、节点和挖矿怎么协作、钥匙与钱包、矿场与矿池。
不是投资建议。 任何涨跌幅故事都只是历史现象，不构成荐币。

开篇：先把人话说明白

比特币（Bitcoin，常写作 BTC）是一套**没有公司老板、没有总行清算中心**的数字货币系统。全世界有很多人运行同一种开源软件（节点），一起维护一份公开的交易账本——大家常说的**区块链**，在比特币里就是这条不断往后接的账本链。

你可以把它想成三件事叠在一起：

1. **一套规则**（协议与软件）：谁能记账、钱怎么转、总量怎么发。
2. **一张全球共享的账本**：转账记录公开可查，但不必绑定你的身份证姓名。
3. **一种记账奖励**：谁按规则成功打包新区块，谁就有机会拿到新发行的比特币和手续费——这就是挖矿激励。

比特币总量有规则上限（常见说法是约 **2100 万**枚），新币通过挖矿按计划进入流通，大约四年有一次“减半”，挖矿奖励变少。没有哪家央行可以一句话多印比特币；真要改规则，得说服网络里足够多的参与者——实际上极难。

下面分五块讲：双花问题、运作方式、它为何仍特殊、共识机制入门、钥匙钱包、矿场矿池。

什么是比特币?



2008 年，署名单名“中本聪”（Satoshi Nakamoto）的白皮书提出了点对点电子现金的设想；2009 年网络启动。十几年里，它经历过暴涨暴跌、分叉争论、监管风暴，也成了许多人认识区块链的第一课。

新人最该先问的不是“会不会涨”，而是：

互联网已经能传照片、传文件，为什么传“钱”以前必须找微信、支付宝、银行当中间人？比特币凭什么说自己能补上这块拼图？

互联网的“最后一块拼图”？——双花问题

网上发照片很简单：你发给我一张，你电脑里那张通常还在。传的是**副本**。

钱不行。如果我“发给”你 100 块，我这边还能继续花这 100，那就变成两个人都在花同一笔钱——这叫**双花**（double-spending）。

纯靠“复制粘贴式”的互联网传输，解决不了双花。现实生活中我们靠谁解决？靠**中介账本**：

- 你用支付宝转 100，本质是支付宝在自己的中心数据库里：我的余额 −100，你的余额 +100。
- 银行转账、银联刷卡，逻辑类似：有一个（或一组）受信任的机构说了算。

中介很有用，但也带来代价：要开户、要合规审核、可能冻结、可能服务中断、要抽手续费、数据在别人服务器上。你信任的是**机构**，不是数学和公开规则本身。

比特币要做的是：在**不依赖单一巨头账房**的前提下，让“我付你 1 个 BTC”这件事，全网最终承认**我少了、你多了**，且很难被偷偷改回去。做到这一点的底层账本技术，常被称作“价值互联网”的一块基石——这句话有点口号，但方向是对的：互联网补的是信息传输，比特币补的是**稀缺数字价值的转移**。

注意两个分寸：

- 比特币并不是“完全匿名现金”。账本公开，地址像化名；若地址和你身份挂钩，轨迹可被分析。更准确说是**假名（pseudonymous）**。
- “不需要中介”指的是**结算与记账不必经过某一家支付公司**；你仍然可能通过交易所、托管钱包等中心化服务买卖，那些环节另有风险。

比特币是如何运作的？——把网络想成一场公开游戏

可以把比特币网络想成一场**自愿参加的大型协作游戏**（规则写在软件里）：

1. **谁都能进退**：你有一台能联网的电脑，就可以下载软件当节点，保存（或验证）账本；不玩了就退出。
2. **记账要抢，也要烧成本**：大约每十分钟，网络会产出一个新区块。想争取记账权的人（矿工）要比拼算力，不断做一种很难碰巧做对、但别人很容易核对的计算——这就是后面说的 **PoW（工作量证明）**。算力越大，短期内撞上正确答案的概率越高，但没有人能保证“下一秒一定是我”。
3. **转账要广播**：你发起转账，交易会传给节点；矿工挑选交易打包进区块。全网节点按规则校验：签名对不对、你有没有花过这些币、有没有双花。
4. **改规则、改历史极难**：想改已经确认的账，或强行改发币规则，需要压倒性的算力与社会共识；多数参与者会拒绝非法分支。

为什么有人愿意一辈子耗电记账？因为成功出块有**区块奖励**（新币）和用户付的**手续费**。激励让陌生人愿意维护安全：攻击网络往往贵到不划算，遵守规则反而能赚钱——这是比特币把“密码学 + 经济学”焊在一起的关键。

和支付宝对比一句话：

- 支付宝：一家公司改两行余额。
- 比特币：成千上万台机器按同一规则，把这笔变动写进公共账本，并层层确认。

和“Q 币、游戏点券”对比一句话：点券是公司数据库里的一串数字，公司能改能停服；比特币余额是公共账本上、由你私钥控制的未花费输出，没有“总公司客服”能一键给你回档。

为何比特币仍特殊?



（原稿这里大段粘贴了机构研报编译。v2 **不转载**。下面用我们自己的话，把新人真正需要的判断框架说短。）

市场上代币成千上万，为什么很多人仍把比特币单独一列？不是因为它“永远涨”，而是因为它的设计取舍和其他链常常不一样。

1. 网络和币是绑死的

“比特币”既指**网络**（大家跑的那套协议），也指**币**（网络里的原生单位）。你可以复制代码另开一条链，但那是**另一个网络、另一种币**，不会自动变成“正统比特币”。币也不能像拷文件一样无损搬到任意其他链上还能叫同一个 BTC（跨链桥是另一套信任假设，后面章节再讲）。

2. 更像“数字时代的货币商品”，不像公司股票

比特币不派息、没有CEO财报。人们看重的往往是：可转移、可分割、可验证稀缺、难以单方面增发。它更常被讨论成**价值储存 / 结算资产**候选，而不是“下一家独角兽股权”。这不保证它胜出，只说

明**评价框架不同**：别拿 PE 估值那套硬套。

3. 稀缺规则难改，是社会共识 + 激励，而不只是一行代码

2100 万上限写在规则里，但代码理论上能改。真正让上限“硬”起来的是：持币人、矿工、交易所、钱包、节点运营者——多数人不愿意接受稀释自己的增发。改上限等于跟自己的经济利益作对，协调成本极高。所以新人要理解：**安全不只来自密码学，也来自一群人不愿合谋改规矩**。

4. “改进比特币”往往是换一套取舍，不是免费升级

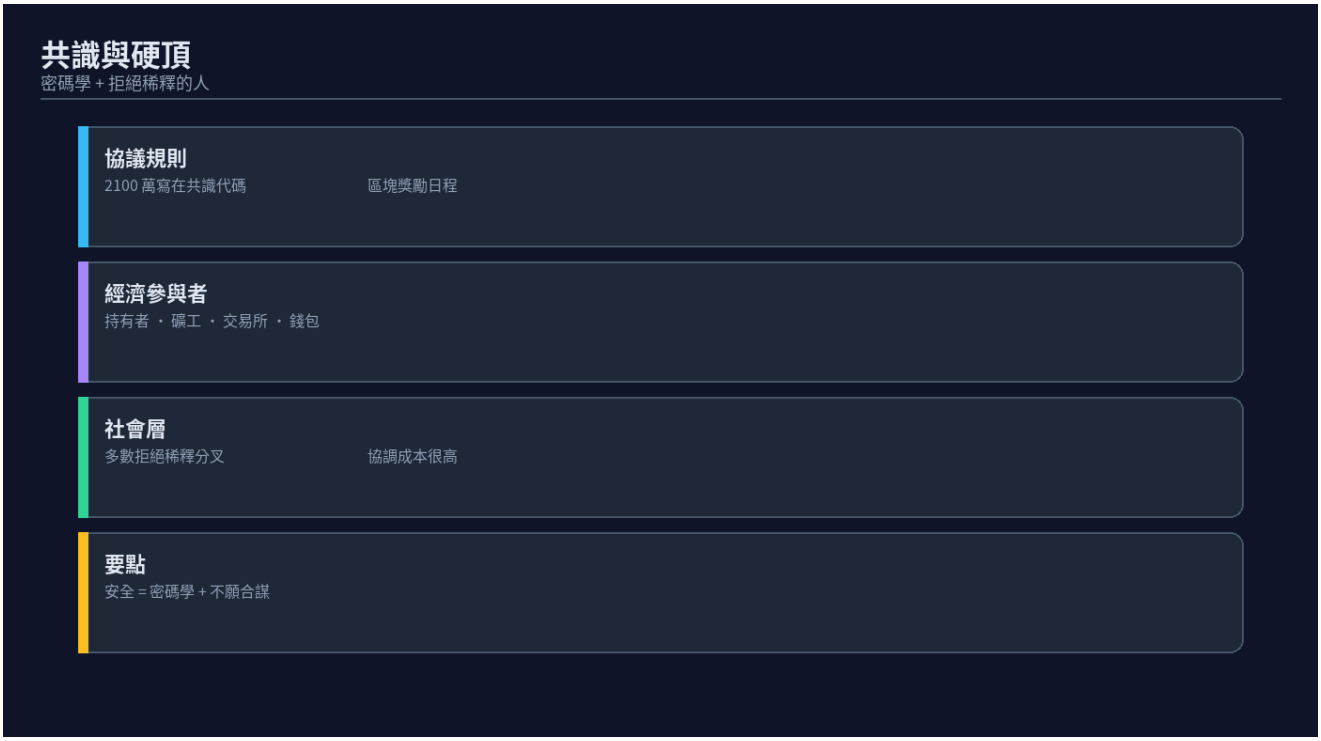
后来的公链常在速度、智能合约、手续费上更激进，但通常要在**去中心化、安全性、简单性**上付出代价。比特币刻意保守：脚本能力有限、升级极慢，换来的是长期抗审查与“少动刀”。其他项目可以服务别的需求（合约、游戏、DeFi），和比特币不必互相消灭；但若你的目标是“最保守的数字稀缺资产”，评估标准就应不同。

5. 到了 2026，外部世界也在变

机构通道（例如部分市场的现货 ETF）、托管与合规交易，改变的是**普通人接触 BTC 的入口**，没有改掉账本本身的规则。入口变方便，不代表你把币放在交易所就等于“自己掌控比特币”——托管风险另算。扩容方面，主链保持相对克制，更多小额高频需求会走到闪电网络等二层思路上（后文 Layer2 章会从以太坊侧展开，比特币侧同理：一层求稳，二层求快）。

一句话：比特币特殊，是因为它把“谁说了算”降到最低，并把稀缺和安全当成第一优先级；其他链特殊，往往是因为它们优先可编程与性能。选哪条路，取决于你要解决什么问题。

读懂区块链共识机制：PoW、PoS、DPoS



刚入门会一直撞上 PoW、PoS 这些缩写。别被英文吓到：**共识机制 = 一群互不信任的人，用什么规则决定“下一页账谁写、写得对不对”**。

家里投票去哪旅游：少数服从多数——那是一种共识。区块链要在全球、有人可能作恶的环境下记账，规则就得更硬，并且常常绑定真金白银的奖惩。

常见入门三分法如下（世界上还有更多变种，先掌握这三种就够读新闻）：

PoW（Proof-of-Work，工作量证明）

- **怎么选记账人**：拼算力，做大量哈希运算，谁先找到满足难度的解，谁大致获得出块权。
- **优点**：准入相对开放；攻击要砸真金白银的硬件和电费；比特币用的就是 PoW。
- **缺点**：耗能与硬件军备竞赛；普通笔记本早已挖不动 BTC。
- **人话**：谁愿意持续付出可验证的“体力劳动”（计算），谁才有较高概率记账分红。

PoS（Proof-of-Stake，权益证明）

- **怎么选记账人**：把币质押（stake）进来当保证金，按规则抽选或轮流出块；作恶可能被罚没（slashing）。
- **优点**：一般远比 PoW 省电；确认可以设计得更快。
- **缺点**：容易让人担心“币多的人话语权更大”；质押与流动性、惩罚规则都更复杂。
- **2026 提醒**：**以太坊已在 2022 年完成合并（The Merge），主网不再靠 PoW 挖矿，而是 PoS 质押验证**。 老文章里“以太坊矿工显卡挖 ETH”属于历史。比特币仍然是 PoW，两套路线并存。

DPoS（Delegated Proof-of-Stake，委托权益证明）

- **怎么选记账人**：像股东选董事——持币人投票选出少数代表节点来出块。
- **优点**：节点少，协作快，吞吐往往更高。
- **缺点**：更像“选出来的小委员会”，去中心化程度通常弱于大规模 PoW/PoS；要盯防贿选与寡头。

小结

没有完美共识，只有取舍：安全、去中心化、速度（常被称作“不可能三角”的简化版）。读项目时先问：谁有权出块？作恶成本是什么？普通用户能不能自己跑节点验证？比特币的选择很明确——**偏安全和去中心化，接受链上吞吐不高**。

什么是比特币私钥、账户与钱包?



和用户关系最紧的三样东西：**私钥、地址（账户）、钱包软件**。下面按直觉讲，故意少堆公式。

公钥密码体制（直觉版）

现代密码学可以生成一对钥匙：

- **私钥**：只有你能有的秘密，用来**签名**（证明“这笔花费是我同意的”）。
- **公钥**：可以从私钥推导出来，别人用来**验证**签名，却很难反推私钥。

在比特币里：私钥掌控币；网络用数学检查签名，不必让你把私钥亮给全世界。

什么是私钥?

私钥本质上是一个**极大空间里随机出来的数**（通常再编码成一串字符）。谁掌握私钥，谁就能花对应地址上的币。

因此：

- **泄露 ≈ 丢币**，而且往往无法冻结追回。
- **丢失且无备份 ≈ 币其实还在链上，但你永远花不出去**。
- 不要截图存在相册、不要发聊天软件、不要存在他人“帮你保管”的不明网页。

什么是比特币账户 / 地址?

日常说的“比特币账户”，多半指**地址**：由公钥经过哈希等步骤变成的一串字符（不同地址格式外观不同）。别人给你转账，是转到地址；链上记录的是这些地址之间的支付关系。

更精确一点：比特币用的是 UTXO 模型——你的“余额”是若干笔**还没花掉的交易输出**之和，不是银行那种单一账户字段。入门阶段记住一句即可：**地址用来收款；私钥用来授权付款**。

什么是钱包?

钱包主要是**帮你保管密钥、展示余额、构造并签名交易**的工具。
钱包里通常并不“存着一堆币文件”，币在链上；钱包里是钥匙。

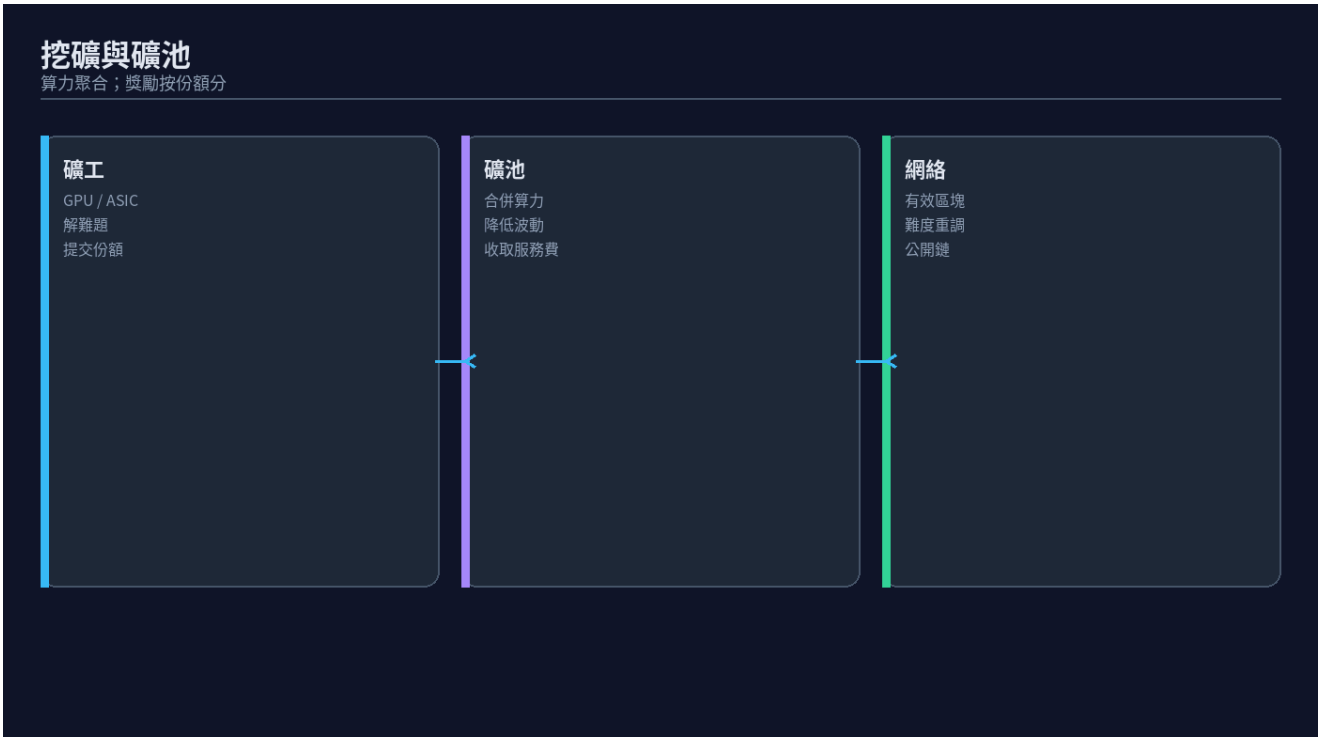
常见分类:

类型	特点	适合
热钱包	联网的手机/浏览器/桌面应用，方便	小额日常
冷钱包	私钥离线（如硬件钱包、离线签名）	大额长期
托管钱包	交易所等替你持股	图方便，但你承担平台风险

首次创建钱包时常见 **助记词（种子短语）**：一串单词能推导出私钥。助记词 = 总钥匙，任何人拿到都能掏空。只写在离线介质、多重备份、永不联网打字上传。

转账时你在本地签名，再把已签名交易广播出去；矿工打包后，经过若干确认，对方才宜视为到账。

什么是比特币矿场和矿池?



挖矿从“笔记本玩玩”演变成高度专业化的产业。三个词常混:

1、矿机

专用计算设备。简史可以记一条进化线：

CPU → GPU → FPGA → ASIC（专用芯片）

如今比特币主流是 ASIC 矿机：只会（或主要）干挖矿相关的哈希，效率远高于普通电脑。家用电脑参与 BTC 挖矿基本没有经济意义。

2、矿场

把大量矿机集中放置、供电、散热、运维的场所。为什么要集中?

- **电费**往往是最大成本，场址靠近廉价稳定电力；
- 专业运维（宕机、更换板子、监控）比家里散养可靠；
- 噪音、散热、合规用电，家用环境很难扛。

矿场是**物理与运维层**的生意：托管机器、保障在线率。

3、矿池

挖矿像不断买彩票：算力小，可能很久不开一张“中奖票”（出块），收入波动极大。于是矿工把算力**逻辑上集中**到矿池：

- 矿池分配计算任务；
- 谁贡献了多少有效份额，按规则分奖励（具体分成模式各异）；
- 小矿工获得更平滑的现金流，常不必自己操心完整出块流程。

人话：**矿场是厂房；矿池是项目组组长**。
矿机可以放在甲矿场，算力接到乙矿池——物理托管与逻辑分红可以分开选。

矿池变大也会带来中心化担忧（少数矿池占比过高）。健康的网络希望矿池分散、矿工可迁移。对新人：如果你不挖矿，只需理解——**网络安全预算很大一部分，来自这些为奖励而竞争的算力**。

本章收束

若你只带走五句话：

1. 互联网擅长复制信息；**钱不能靠复制**，否则双花。
2. 中心化支付靠机构账本；比特币靠**全球复制的规则账本 + 激励**。
3. 比特币刻意保守，强调稀缺与抗审查；**和其他公链是不同考卷**。
4. **私钥 = 所有权**；钱包是钥匙串，不是银行金库本身。
5. 矿机/矿场/矿池让 PoW 安全变得工业化；你不挖矿也可以当节点验证规则。

下一章我们离开“单个货币系统”，讲 **Web3** 这个更大的筐：当账户、合约、身份和应用都往链上搬时，新人到底会碰到什么——以及哪些是泡沫话术、哪些是真能上手的能力。

（第 1 章完 · v2 原创重写 · SCDO Lab）