《通往比特币之路》

假如

曾经有 1 枚比特币出现在我面前，我没有珍惜，等我失去的时候才后悔莫及，人世间最痛苦的事情莫过于此。如果上天能够给我再来一次的机会，我会对曾经的自己说三个字：不要卖。如果非要在这份投资上加一个期限，我希望是……**20 年。**

截止目前（2025 年 1 月 1 日），比特币在中国大陆地区无法交易，但持有合法。

发布声明

本书是为比特币 0 概念入门者提供的参考书，不涉及过多复杂的技术概念，且不涉及如何买卖比特币。为了便于理解，部分描述可能会有所简化且存在片面甚至错误，**也期待您的反馈，我会及时修改。**

风险提醒

请务必知晓，比特币领域充满不确定性与风险。其价格波动剧烈，可能在短时间内大幅涨跌 ,投资者需有强大的心理与资金承受力。同时，比特币交易的合法性在不同国家和地区存在差异，部分地区严格监管甚至禁止，务必提前了解当地法规政策，避免陷入法律困境。

bitcoin（比特币）

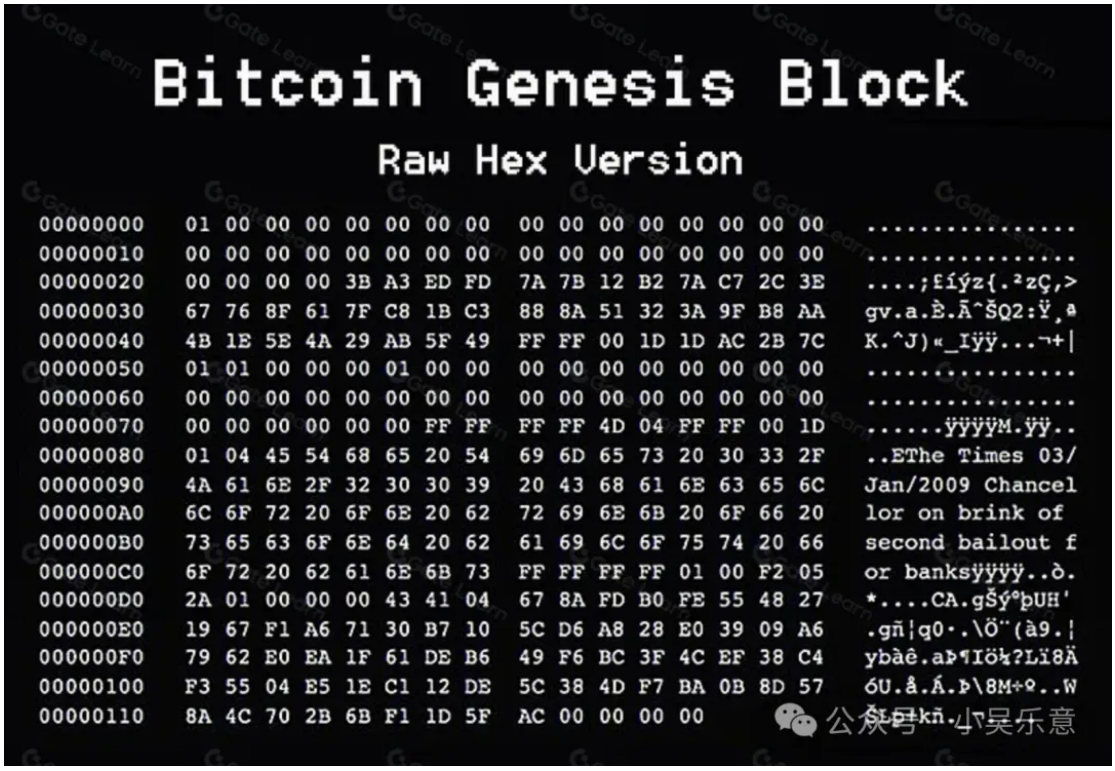
比特币是由一位自称为“中本聪（Satoshi Nakamoto）”的匿名人士或者匿名组织发明的。2008 年 11 月 1 日（北京时间），中本聪在 P2PFoundation 网站发布了白皮书《比特币：一种点对点的电子现金系统》（Bitcoin：A Peer-to-Peer Electronic Cash System）

比特币白皮书（中文）：

https://bitcoin.org/files/bitcoin-paper/bitcoin_zh_cn.pdf

虽然对普通人而言，晦涩难懂，但我相信日拱一卒的力量，相信你会慢慢明白，我们共同进步。

2009 年 1 月 3 日格林威治标准时间（GMT）18:15:05，比特币网络正式启动。中本聪挖出了比特币的第 0 个区块——创世区块，并获得了 50 个比特币作为奖励。时至今日，比特币的主网里，依然记录着创世区块的详细信息。



看图片右侧，上面还记录着中本聪的“留言”，这句话也永远的刻在了比特币网络之中，凝聚在所有人的共识之中，甚至比刻在石头上的文字更能永久留存下去。

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”（2009 年 1 月 3 日，财政大臣正处于实施第二轮银行紧急援助的边缘）

比特币的故事，正是从这行文字开始的。

而它的未来，将由每一个参与者共同书写。

区块链技术：比特币的“灵魂”

区块链是一种去中心化的分布式账本技术，它将数据以区块的形式存储，并通过密码学技术确保数据的安全性和不可篡改性。这些区块按顺序链接在一起，形成一个链条，因此被称为“区块链”。

如果说比特币是一台精密的机器，那么“区块链技术”就是它的核心引擎。它不像传统的银行系统，由一个中央机构掌控所有交易和数据。比特币的网络是由全球成千上万的节点共同维护的，每个节点都有一份完整的账本副本，没有任何一个人或组织能够单独控制它，构成了去中心化的比特币系统。

去中心化是什么

想象一下，如果有一天你的银行突然倒闭，或者政府冻结了你的账户，你的钱可能会瞬间消失。但在比特币的世界里，这种情况几乎不可能发生。因为它的账本分布在无数台电脑上，除非你能同时摧毁所有这些电脑，否则比特币网络就会一直运转下去。

如果你在一个经济长期稳定的环境中生活，对此可能无法感同身受。

在一些国家，政府滥发货币导致恶性通胀，民众的储蓄在短短几个月内变得一文不值。比如，津巴布韦和委内瑞拉都曾经历过这样的噩梦。

在某些国家，政府可能会因为政治原因冻结个人或企业的资产。比如，2013 年塞浦路斯爆发金融危机时，政府直接冻结了民众的银行账户，并对存款征税。

全球仍有数十亿人没有银行账户，他们无法享受基本的金融服务。但在比特币的世界里，你只需要一部智能手机和互联网连接，就可以参与全球金融体系 ,在写这本书的时候 ,世界的金融体系正在慢慢重构。

如今回看中本聪在比特币白皮书的那句话：“**我们需要的是一个基于密码学原理而不是信任的电子支付系统，该系统允许任何有交易意愿的双方能直接交易而不需要一个可信任的第三方。**”

这就是比特币的内核，它不仅仅是技术创新，更是一种思想的突破，让个人在数字时代拥有真正的财富自由。

工作量证明：比特币的“根基”

如果说区块链是比特币的灵魂 ,那么工作量证明机制(Proof of Work, PoW) 就是比特币的根基。也是我们俗称的挖矿，挖矿不仅是比特币网络运行的根本保障，也是新比特币诞生的方式。正是因为有了工作量证明机制，才确保了比特币网络的安全性和去中心化。

挖矿是什么

比特币挖矿是指矿工通过解决复杂的数学问题来验证交易并将其打包成区块的过程。这些数学问题需要大量的计算能力来解决，而第一个成功解决问题的矿工将获得比特币奖励。这个过程不仅确保了交易的有效性，**最重要是解决了双重支付等欺诈行为。**

双重支付是什么

双重支付/双花支付（Double Spending）是数字货币领域的一个经典问题。简单来说，它指的是同一笔钱被花费两次或多次的情况。在传统的现金交易中，双重支付几乎不可能发生，因为你把一张纸币交给别人后，它就不再属于你了。即便是电子支付环境下，这个问题也可以通过中央机构（如银行）来避免和解决。

但在数字货币的世界里，由于数据可以被复制，并且不存在一个中央机构来控制系统，那么如果没有一种机制来防止双重支付，整个系统将陷入混乱，更谈不上可信。

举个例子：

假设你有一个比特币，你同时向两个人发送了这笔比特币：一个人用来购买商品，另一个人用来支付服务费用。如果没有一种机制来验证交易的顺序和有效性，这两个交易可能会同时被确认，导致你实际上用了一个比特币，但却买了两个比特币的东西。

比特币如何解决双重支付问题？

比特币通过**工作量证明机制**和**区块链技术**完美解决了双重支付问题。以下是它的工作原理：

1. **交易广播**：当你发起一笔比特币交易时，这笔交易会被广播到整个比特币网络，等待被矿工打包进区块。

2. **区块确认**：矿工们通过解决复杂的数学问题（即挖矿）来竞争打包交易的权利。第一个成功解决问题的矿工将把交易打包进一个新的区块，并将其添加到区块链上。
3. **链上确认**：一旦交易被写入区块链，它就被认为是“已确认”的。随着后续区块的不断添加，这笔交易的确认次数也会增加。通常，6 个区块确认后，交易就几乎不可逆了。
4. **防止双重支付**：由于区块链是一个按时间顺序排列的账本，网络会自动选择最长的链作为有效链。如果有人试图发起双重支付，网络会拒绝确认这笔交易，因为它与已有的交易记录冲突。

假设你试图用同一笔比特币同时支付给 A 和 B。矿工会根据交易的先后顺序和网络共识，选择其中一笔交易进行确认，而另一笔交易会被拒绝。最终，只有一笔交易会被写入区块链，另一笔则会被视为无效。

工作量证明机制不仅解决了双重支付问题，还确保了比特币网络的安全性和去中心化。矿工们通过消耗计算资源来竞争记账权，这种竞争使得攻击者想要篡改区块链数据变得极其困难。因为要篡改一个区块，攻击者需要在极短时间内重新计算该区块及其后续所有区块的工作量证明，这需要至少掌握 30-51%的全网算力，成本极高。

举个例子：

你参加一场 200 米短跑比赛，且每跑完 200 米系统都会自动再次延长赛道 200 米。同时系统会给第一个完成的人奖励 50 个比特币，紧接

着系统就去下一个 200 米节点，等待给下一个第一个跑过去的人继续奖励 50 个比特币。所以大家都是不断的往前按照 200 米的节点去拼体力，投机取巧是不存在的，这就是工作量证明机制的魅力。

那如果有人想作弊，修改比赛结果，不仅要退回去先把上一个 200 米甚至上上一个 200 米重新跑一遍，且还必须是自己拿到第一名，紧接着在继续追赶后面的每个 200 米阶段比赛，保证每一次追赶都能拿到第一名。

随着比赛的进行，赛道越来越长，作弊的难度也呈指数级增长。除非作弊者拥有远超全网的算力，否则几乎不可能成功。

那么新问题又来了，什么是全网算力？

全网算力：比特币的“护盾”

全网算力（Total Network Hashrate）是指比特币网络中所有矿工计算能力的总和。它代表了整个网络每秒能够进行的**哈希运算**次数，是衡量比特币网络安全性和健康程度的重要指标。

哈希运算是什么

哈希运算（Hash Function）是一种复杂的数学计算，矿工通过不断尝试不同的随机数（Nonce）来寻找满足特定条件的哈希值。这个过程就像在猜一个巨大的密码锁，只有找到正确的组合，才能打开锁并获得奖励。

比特币算力有多强

全网算力的单位通常是**哈希每秒（H/s）**，常见的单位还包括：

- **千哈希每秒（kH/s）**
- **兆哈希每秒（MH/s）**
- **吉哈希每秒（GH/s）**
- **太哈希每秒（TH/s）**
- **拍哈希每秒（PH/s）**
- **艾哈希每秒（EH/s）**

截至 2025 年 1 月初，比特币全网算力已经接近 **1000EH/s**，这意味着全球矿工每秒钟可以进行数百亿亿次哈希运算。

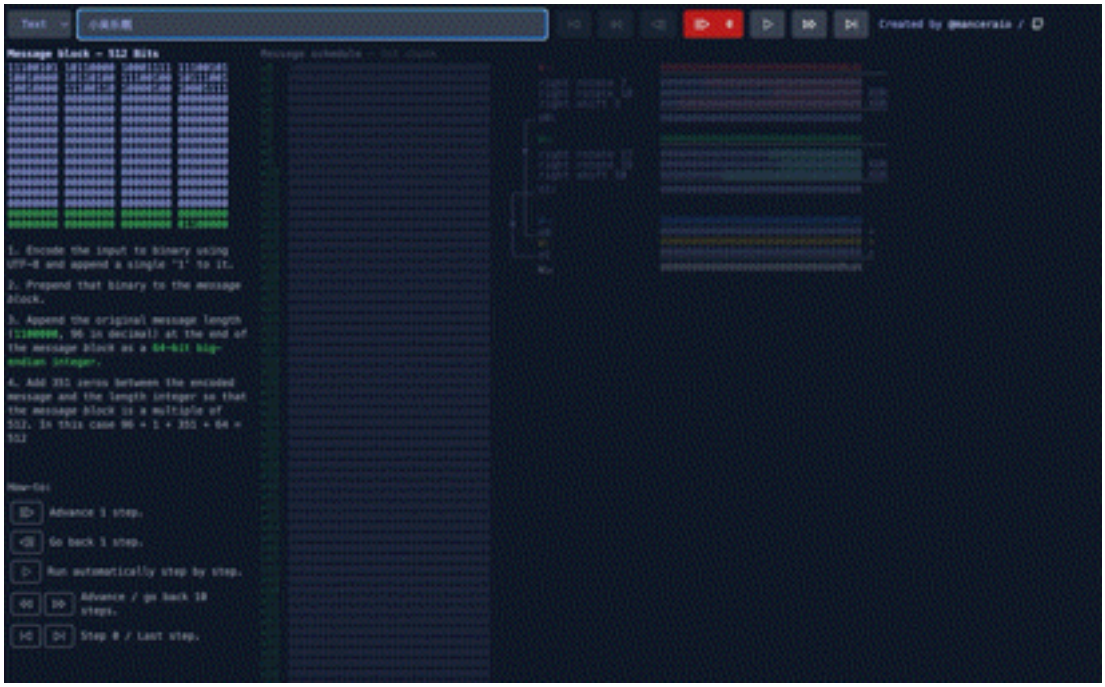
“地球人算力”与比特币算力对比

全球有 80 亿人 ,假如每个人每秒钟可以做一次 SHA256 运算。那么，全球所有人一起，每秒钟总共可以做 80 亿次 SHA256 运算。现在，让我们对比一下：

1. **全球 80 亿人口一起做 SHA256 运算**：
    - 全球人口：80 亿人
    - 每人每秒做 1 次 SHA256 运算
    - 总运算能力：80 亿次/秒（即 8×10^9次/秒）
2. **比特币全网算力**：
    - 1000 EH/s = 1000×10^{18}次/秒 = 1×10^{21}次/秒
3. **比特币算力与全球人口算力的对比**：

- 比特币算力 ÷ 全球人口算力 = $(1 \times 10^{21}) \div (8 \times 10^{9}) = 1.25 \times 10^{11}$
- 即比特币算力是全球人口算力的 **1250 亿倍。**

这里给你直观感受一下 SHA256 的计算过程，你也可以自行测试：



演示地址：https://sha256algorithm.com

超计算机与比特币算力对比

2024 年 11 月 18 日，在“2024 年超级计算”大会上，Top500 组织公布了全球最强超算 Top500 榜单。其中，位于美国劳伦斯利弗莫尔国家实验室（LLNL）的由 AMD 提供支持的 El Capitan 以 1.742 exaflops 的峰值性能成为目前地球上已知的最快的超级计算机

这是目前公布出来的“超级计算机”：

- **比特币全网算力**：1000 EH/s（每秒 1000 亿亿次哈希运算）。

- **El Capitan 超算**：1.742 EH/s（每秒 1.742 亿亿次浮点运算）。

从算力上看，比特币的全网算力是 El Capitan 超算的**约 574 倍**。这意味着比特币网络每秒钟进行的哈希运算次数远超 El Capitan 的浮点运算次数。

但值得注意的是两者的用途和架构完全不同。比特币算力主要用于维护区块链的安全性，而 El Capitan 则专注于高精度科学计算。对此感兴趣的朋友，可以自行查阅更多资料。

算力高有什么用？

当哈希运算次数越高，也就是算力越高的时候，才能提供：

1. **比特币系统安全**：全网算力越高，攻击者想要篡改区块链数据所需的成本就越高。要成功发起 51%攻击（即控制超过 30%-51%的全网算力），攻击者需要投入巨大的资金和资源，这几乎是不可能的。
2. **维持区块生成速度**：比特币网络的设计目标是每 10 分钟生成一个新区块。随着全网算力的增加，挖矿难度也会动态调整，以确保区块生成速度保持稳定。
3. **促进去中心化**：全网算力的分布反映了比特币网络的去中心化程度。如果算力过于集中在少数矿池手中，可能会威胁到网络的安全性。因此，算力的分散是比特币网络健康运行的重要指标。

虽然目前比特币是几大矿池平分天下，但从矿池自身利益出发，它们并没有动机去破坏比特币网络。相反，矿池的存在实际上是为了让更多的小矿工能够参与挖矿，从而进一步分散算力，增强网络的去中心化特性。

因为不管是占据多少算力比例的矿池，都是由更分散在全球的矿厂组成的，背后是成千上万的个体矿工和矿场运营者。这些矿工和矿场分布在不同国家和地区，使用不同的能源和设备，共同构成了比特币网络的算力基础。这种分散性不仅增强了网络的抗风险能力，也使得单一实体或组织难以控制整个网络，从而维护了比特币的去中心化特性。

即使某个矿池试图发起 51%攻击，其内部的矿工也会因为利益冲突而拒绝参与，进一步降低了攻击的可能性。

51%攻击是什么

51%攻击是一种潜在的攻击方式，攻击者通过控制比特币网络中超过一半的算力，能够篡改交易记录，实施“双重支付”或者“回滚”已确认的交易。然而，成功进行此类攻击的难度极高，因为它需要巨大的计算能力和资源投资。

举个例子，假设一个矿池或一个国家的组织试图通过占据超过 51%的算力来发起攻击。首先，他们需要投入数十亿美元甚至上百亿美元，去购买并运营大量的专用矿机，才能达到此算力水平。即使攻击者成

功控制了一部分网络算力，他们也必须面对其他矿池和社区的反制，如通过技术升级来提高网络的抗攻击能力。

也可以参考前面提到的跑 200 米的例子。

当然在区块链的历史上真实发生过 51%算力攻击：

- **比特币黄金（BTG）**：2018 年，比特币黄金（一种比特币的分叉币）曾遭到 51%攻击，攻击者成功回滚了交易并窃取了价值数百万美元的 BTG。然而，比特币黄金的算力远低于比特币，攻击者只需控制少量算力即可实施攻击。
- **以太坊经典（ETC）**：2020 年，以太坊经典也遭到了 51%攻击，攻击者通过租用算力成功回滚了交易。然而，这些案例都发生在算力较低的小型区块链上，比特币的全网算力使得这种攻击几乎不可能。

51%算力攻击是比特币网络的“终极挑战”，尽管在理论上可行，但在实际操作中几乎不可能实现。比特币的高算力、去中心化架构和强大的社区支持，使得这种攻击的成本和风险远远超过了潜在的收益。

正如比特币的创始人中本聪所说：“比特币网络的安全性依赖于诚实节点的算力。”只要大多数矿工和节点保持诚实，比特币网络就会继续安全运行。

况且，比特币还有难度调整机制，可以有效应对算力波动，确保网络始终按照约 10 分钟出块的节奏运行。即便发生恶意攻击，难度调整机制也会在下一个周期重新平衡挖矿难度，削弱攻击者的优势。此外，比特币网络的开源透明性和社区监督，使得异常活动能够迅速被发现和应对。因此，51%攻击不仅成本高昂且难以维持，反而会动摇攻击者自身持有比特币的价值。

那么，什么是难度调整机制？

难度调整机制：比特币的“压舱石”

比特币的难度调整机制是其网络运行的核心机制之一，确保了区块生成速度的稳定性。无论全网算力如何变化，比特币网络始终能够保持大约每 10 分钟生成一个新区块的速度。这一机制不仅维护了比特币网络的正常运行，也长期确保了其安全性和去中心化特性。

比特币的难度调整机制是通过动态调整挖矿难度来实现的。挖矿难度决定了矿工需要解决的数学问题的复杂程度。难度越高，矿工找到有效哈希值的概率就越低，反之亦然。

难度调整的具体过程如下

1. **区块生成时间监控**：比特币网络每生成 2016 个区块（大约两周时间），就会进行一次难度调整。网络会计算这 2016 个区块的实际生成时间，并与理论生成时间（2016 个区块 × 10 分钟/区块 = 20160 分钟，即 14 天）进行比较。

2. **难度调整计算**：如果实际生成时间少于 14 天，说明全网算力增加，挖矿难度将相应提高；如果实际生成时间多于 14 天，说明全网算力减少，挖矿难度将相应降低。
3. **难度调整公式**：新难度 = 旧难度 × (实际生成时间 / 理论生成时间)

难度调整机制的作用

难度调整机制的主要作用是保持区块生成速度的稳定，确保比特币网络的正常运行。具体来说，它有以下几个重要作用：

1. **维持区块生成速度**：无论全网算力如何变化，难度调整机制都能确保区块生成速度保持在每 10 分钟一个新区块的水平。这使得比特币的发行速度保持稳定，避免了通货膨胀或通货紧缩的风险。
2. **保障网络安全**：难度调整机制确保了比特币网络的安全性。随着全网算力的增加，挖矿难度也会相应提高，这使得攻击者想要发起 51%攻击的成本大幅增加。
3. **促进去中心化**：难度调整机制使得小矿工也有机会参与挖矿。即使全网算力增加，小矿工仍然可以通过加入矿池等方式参与挖矿，从而维护了比特币网络的去中心化特性。

难度调整机制的实际案例

比特币的历史上，难度调整机制多次发挥了重要作用。以下是几个典型的案例：

1. **2017 年比特币算力暴涨**：2017 年，随着比特币价格的飙升，大量矿工加入网络，导致全网算力急剧增加。难度调整机制迅速响应，大幅提高了挖矿难度，确保了区块生成速度的稳定。
2. **2021 年中国矿工迁移**：2021 年，中国对比特币挖矿进行了严格监管，导致大量矿工迁移到海外。全网算力短期内大幅下降，难度调整机制迅速降低了挖矿难度，确保了网络的正常运行。

图片中红色区域，就是当时中国矿机大面积关机后导致的全网算力暴跌。但随后，比特币全网算力又超过之前，继续上升。

比特币的难度调整机制确保了网络的稳定性和安全性，它像一个精准的“稳定器”，无论算力如何波动，都能让区块生成保持在约 10 分钟的节奏中。这种动态调整不仅提升了抗攻击能力，也为比特币的长期

运行奠定了基础。然而，除了难度调整，比特币还有另一项独特的经济设计——**减半机制**。

那么，什么是减半机制？

减半机制：比特币的“稀缺性”

比特币的稀缺性是其价值的重要支撑之一。与“不限量发行”的法定货币不同，比特币的总量是固定的，上限为 2100 万枚。这种设计使得比特币具有非常明显的“稀缺性”，虽然我不想用这个词，但这也是大家普遍的共识，比特币就是“数字黄金”。

为什么是 2100 万枚？

在比特币白皮书里面说的很明确，比特币自上线开始运行后，将按照代码规定好的规则产出 :每 10 分钟产生一个新区块 ,每个区块的初始奖励为 50 个比特币。每 21 万个区块（大约 4 年），区块奖励会减半一次。这个过程被称为“**减半**”（Halving）。

- **第一次减半**：2012 年 11 月 28 日，区块奖励从 50 个比特币减少到 25 个。
- **第二次减半**：2016 年 7 月 9 日，区块奖励从 25 个减少到 12.5 个。
- **第三次减半**：2020 年 5 月 11 日，区块奖励从 12.5 个减少到 6.25 个。
- **第四次减半：**2024 年 4 月 21 日，区块奖励将从 6.25 个减少到 3.125 个。

- ……
- **减半计算：21 万 × (50 / 2^n) BTC**

于是计算比特币总量的方式就是：

21 万区块 × (50 + 25 + 12.5 + 6.25 + 3.125 + …) BTC = 2100 万 BTC

如果按照目前比特币系统减半规律，在 2140 年前后，比特币的区块奖励将趋近于零，届时比特币的总量将达到接近 2100 万枚的上限。所以，如果你是 00 后，有很大概率会活到 150 岁，看到最后那一点点比特币被挖出来的历史时刻。

在这之前，请务必保管好你的私钥，因为它是通往你财富与自由的唯一钥匙。私钥不仅是比特币所有权的证明，更是你在去中心化世界中掌握主动权的核心。无论你选择硬件钱包、纸钱包还是其他存储方式，确保私钥的安全都是重中之重。记住，比特币的去中心化特性意味着没有第三方可以帮你找回丢失的私钥，一旦丢失，你的比特币将永远沉睡在区块链中。

那么，问题又来了，什么是比特币的私钥？

私钥：比特币的“命脉”

中本聪在设计比特币时，充分依赖了密码学技术。Ta 曾表示，“**只要私钥不被泄露，比特币就是安全的。**”

在比特币的世界里，私钥就像是你的“数字身份证”和“保险箱钥匙”的结合体。它不仅仅是一串复杂的字符，更是你掌控比特币的唯一凭证，请跟我重复读一遍：**私钥是你掌控比特币的唯一凭证。**没有私钥，你就无法证明自己拥有比特币，也无法进行任何交易。因此，保护好私钥，就是保护你的财富和自由。

私钥是什么？

私钥是一串由 64 个十六进制字符组成的字符串，看起来像这样：5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF。这串字符是通过复杂的数学算法生成的，几乎不可能被猜测或破解。私钥的作用是生成你的比特币地址，并用于签署交易，证明你对这笔比特币的所有权。

为什么私钥如此重要？

在传统的金融系统中，如果你的银行卡丢失或密码忘记，你可以通过银行找回或重置。但在比特币的世界里，没有中央机构可以帮你找回私钥。一旦丢失，你的比特币将永远无法找回。这就是为什么私钥被称为比特币的“命脉”。

当然，如果你丢了私钥，也算用另一种独特的方式为比特币网络了贡献。因为丢失的私钥意味着对应的比特币将永远无法被使用，这些比特币将永久退出流通，进一步减少了比特币的总供应量。

从某种意义上说，这增强了比特币的稀缺性，就像大航海时代那些装满黄金珠宝的沉船，永远沉睡在深海之中，无法被打捞。不过，这种

“贡献”显然是以个人财富的损失为代价的，所以还是建议大家妥善保管私钥，避免成为“比特币考古学家”未来的研究对象。毕竟，比特币的未来需要每个人的参与，而不是“沉睡”的财富。

如何保管私钥？

1. **硬件钱包**：硬件钱包是一种专门用于存储私钥的物理设备，通常以 USB 的形式存在。它的优点是安全性高，即使连接到被感染的电脑，私钥也不会泄露。常见的硬件钱包品牌有 Ledger 和 Trezor。
2. **纸钱包/钢板钱包**：纸钱包是将私钥和比特币地址打印在纸上，然后妥善保管。这种方式虽然简单，但需要注意防火、防水和防丢失。也可以刻在钢板上，或者了解一下“助记词钢板”。
3. **脑钱包**：脑钱包是通过记忆一个复杂的密码短语来生成私钥。这种方式虽然方便，但风险也很高，因为一旦忘记密码，比特币就无法找回。
4. **多重签名钱包**：多重签名钱包需要多个私钥共同签署才能完成交易。这种方式适合团队或家庭使用，可以增加安全性。

私钥丢失的后果

历史上，有很多人因为丢失私钥而失去了大量的比特币。最著名的例子是 James Howells，他在 2013 年不小心将一个存有 7500 枚比特币的硬盘丢进了垃圾填埋场。按照 2025 年的比特币价格，这些比特

币的价值已经超过数亿美元。然而，由于私钥丢失，这些比特币将永远无法找回。

私钥的安全建议

1. **备份**：无论你选择哪种存储方式，务必备份私钥。可以将备份存放在不同的安全地点，如保险箱或银行的保管箱。
2. **离线存储**：尽量将私钥存储在离线设备上，避免连接到互联网，减少被黑客攻击的风险。
3. **定期检查**：定期检查你的私钥存储设备，确保它们处于良好状态，没有被损坏或丢失。
4. **不要分享**：永远不要将你的私钥分享给任何人，即使是信任的朋友或家人。私钥一旦泄露，你的比特币就可能被盗。

关于私钥的安全性强调不管多少次，都值得重复强调。没有“找回私钥”机制的比特币是所有比特币持有者必须同步的认知。因此，请对自己的私钥负责，正如中本聪早期不断强调的：**“比特币的安全性最终取决于用户自己。”**

最终，回归比特币的第一性原理：“**比特币是一种基于密码学证明而非信任的系统。**” 而私钥，正是其中的核心体现。

比特币的未来：由你书写

比特币的故事，从 2009 年的创世区块开始，已经走过了 16 年了。在这 16 年里，比特币经历了无数的质疑、挑战和突破，但它依然屹立不倒，并且越来越强大。它的未来，将由每一个参与者共同书写。

你的角色

比特币的未来，不仅仅取决于技术的发展，更取决于每一个参与者的选择和行动。无论你是矿工、开发者、投资者还是普通用户，你都在为比特币的未来贡献力量。你的每一个决定，都可能影响比特币的发展方向。

最后

比特币的代码是开源的，规则是透明的，权力是分散的。它不属于任何国家、任何组织，甚至不属于中本聪本人。它属于每一个相信它的人，属于每一个为它贡献力量的人。

比特币不仅是一项技术创新，它更是一种信仰，一种关于**自由与公平**的追求。它代表着我们对现有金融体系的反思，也承载着人类对未来无限可能的探索。从一行行代码到一个个区块，从一个小社区到如今覆盖全球的网络 ,比特币的成长是无数普通人你与我共同努力的结果。未来并不确定，但正是这种不确定性，赋予了我们无限的想象空间。也许在某一天，比特币会成为全球认可的主流货币，改变我们对金钱和信任的理解；也许，它会作为一种革命的象征，持续推动金融系统的变革。无论未来如何，比特币已经启发了我们：**改变世界并不一定**

需要庞大的力量，有时候，一个简单的理念，一群相信的人，就足以点燃燎原之火。

愿每一个选择与比特币同行的人，都能在这个去中心化的未来里，找到属于自己的自由与力量。

中本聪的设计理念，充满了对自由的追求和对权力的警惕。Ta 用密码学技术取代了信任，用数学规则取代了人为干预。比特币的每一行代码，都在诉说着一个理想：**让每个人都能成为自己财富的主人。**

愿你穿越周期，归来手里仍有比特币。

（本书完）

关于本书

本书为免费阅读与传播的参考书，旨在为比特币初学者提供入门指导。书中内容力求简洁易懂，部分描述可能存在简化或片面之处，欢迎读者反馈，我将及时修正。请保留作者署名，未经授权不得用于商业用途。未来可能会根据技术发展和读者建议进行修订。

致谢

感谢每一位阅读本书的读者，你们的支持是我持续创作的动力。特别感谢比特币社区的开发者、矿工和爱好者们，正是你们的努力和坚持，让比特币从一个小众实验成长为全球瞩目的技术创新。

未来计划

本书将根据比特币技术的发展和读者的反馈持续更新。未来可能会增加更多关于比特币生态、Layer 2 技术（如闪电网络）、以及区块链在其他领域的应用等内容。如果你对某些主题特别感兴趣，欢迎告诉我，我会优先考虑将其纳入更新计划。

分享传播

如果你觉得本书对你有帮助，欢迎分享给更多朋友。比特币的未来需要更多人的参与和了解，而你的每一次分享，都是在为去中心化的未来贡献力量。

反馈与互动

本书的内容虽然力求准确，但由于比特币技术的快速发展和复杂性，难免存在疏漏或不足之处。如果你在阅读过程中发现任何问题，或有改进建议，欢迎通过以下方式与我联系：

公众号微博/X：小吴乐意

博客：https://blog.xiaowuleyi.com

Email：xiaowuleyi@gmail.com

赞赏支持

如果你觉得本书对你有帮助，欢迎通过以下方式支持我的创作。你的每一份赞赏都是我继续写作和分享知识的动力：

比特币地址（Ly=乐意）：

3KLy733p6vQDyaKdEY61iGdQPf9pYt9hPv