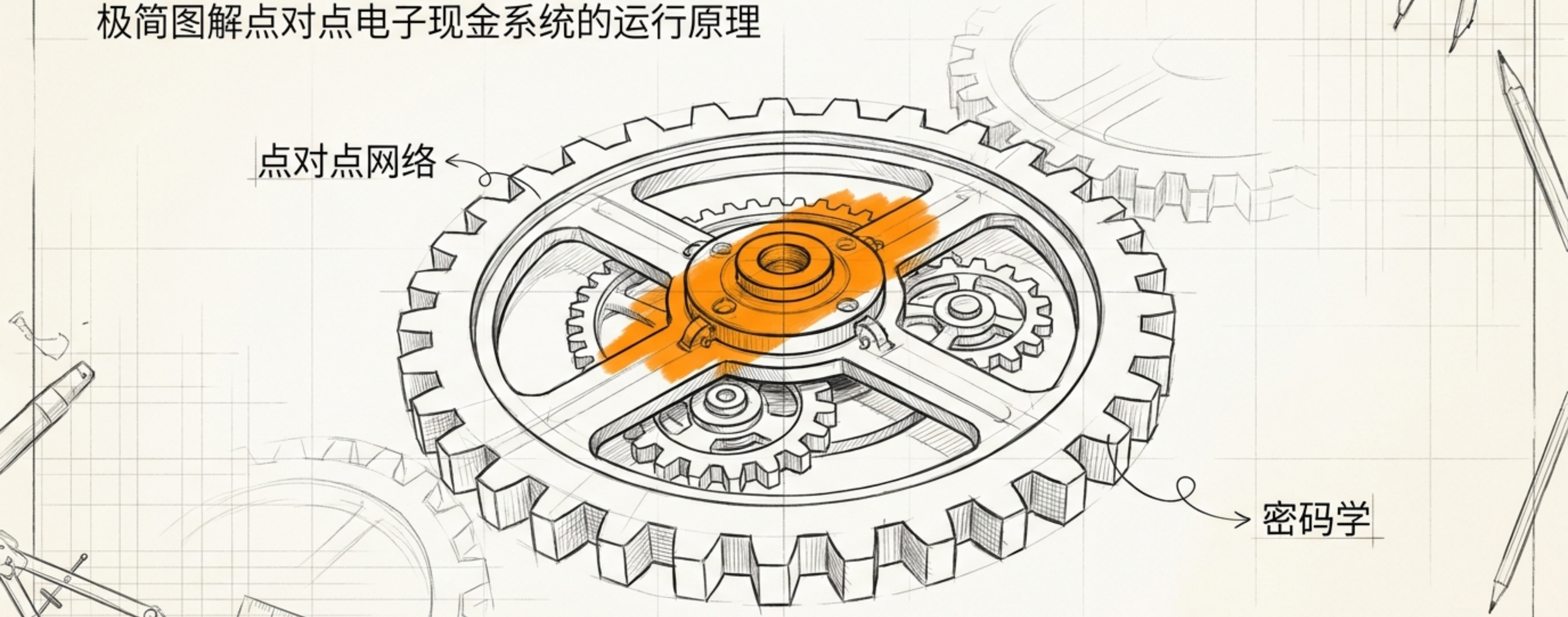
比特币：一台无需信任的信任机器

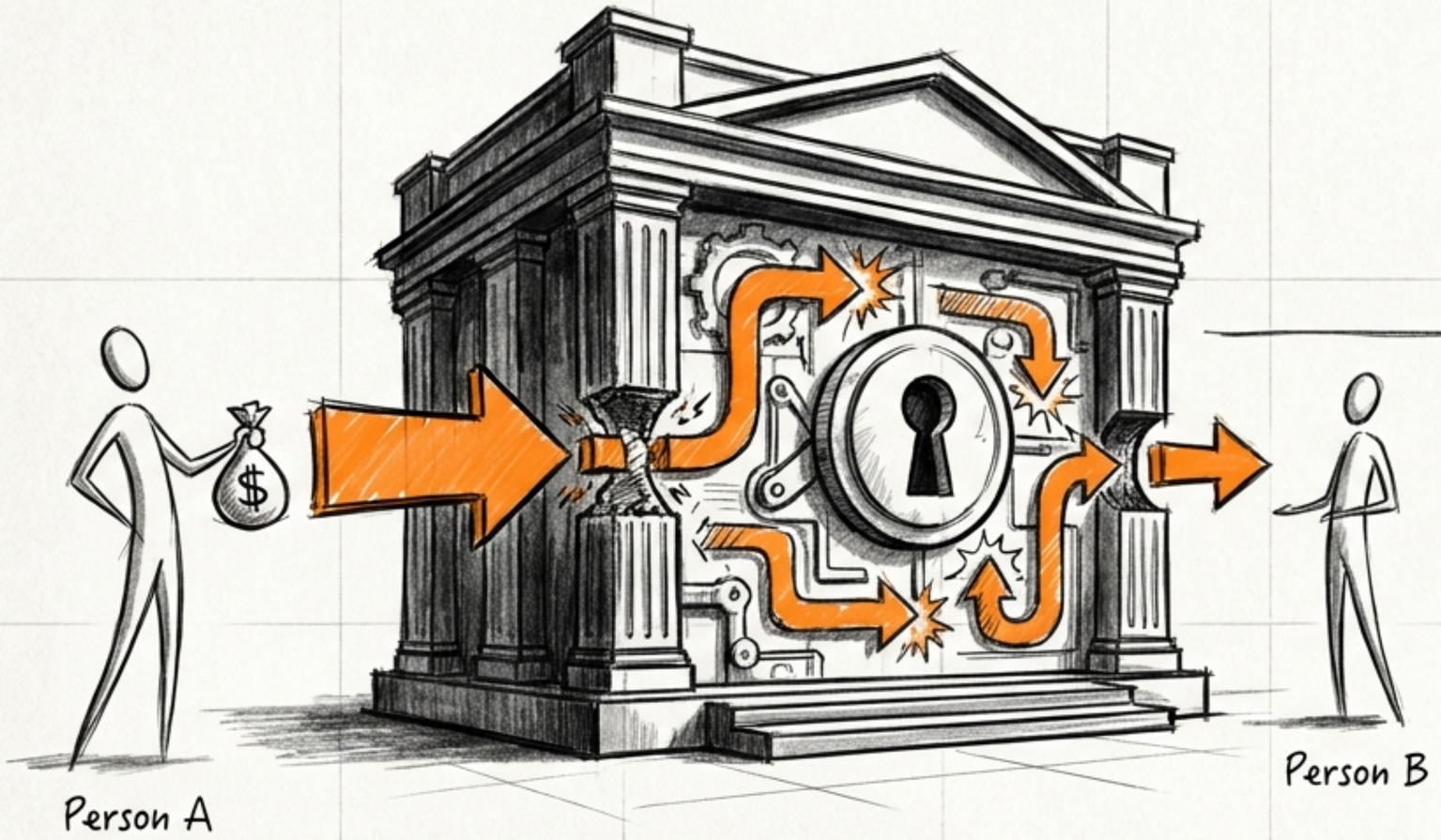
极简图解点对点电子现金系统的运行原理



Gemini Notebook

传统金融的中心化瓶颈

“基于信任模型”的固有缺陷带来了高昂的摩擦成本。



仲裁成本：机构必须调解纠纷，导致交易无法真正做到“不可撤销”。

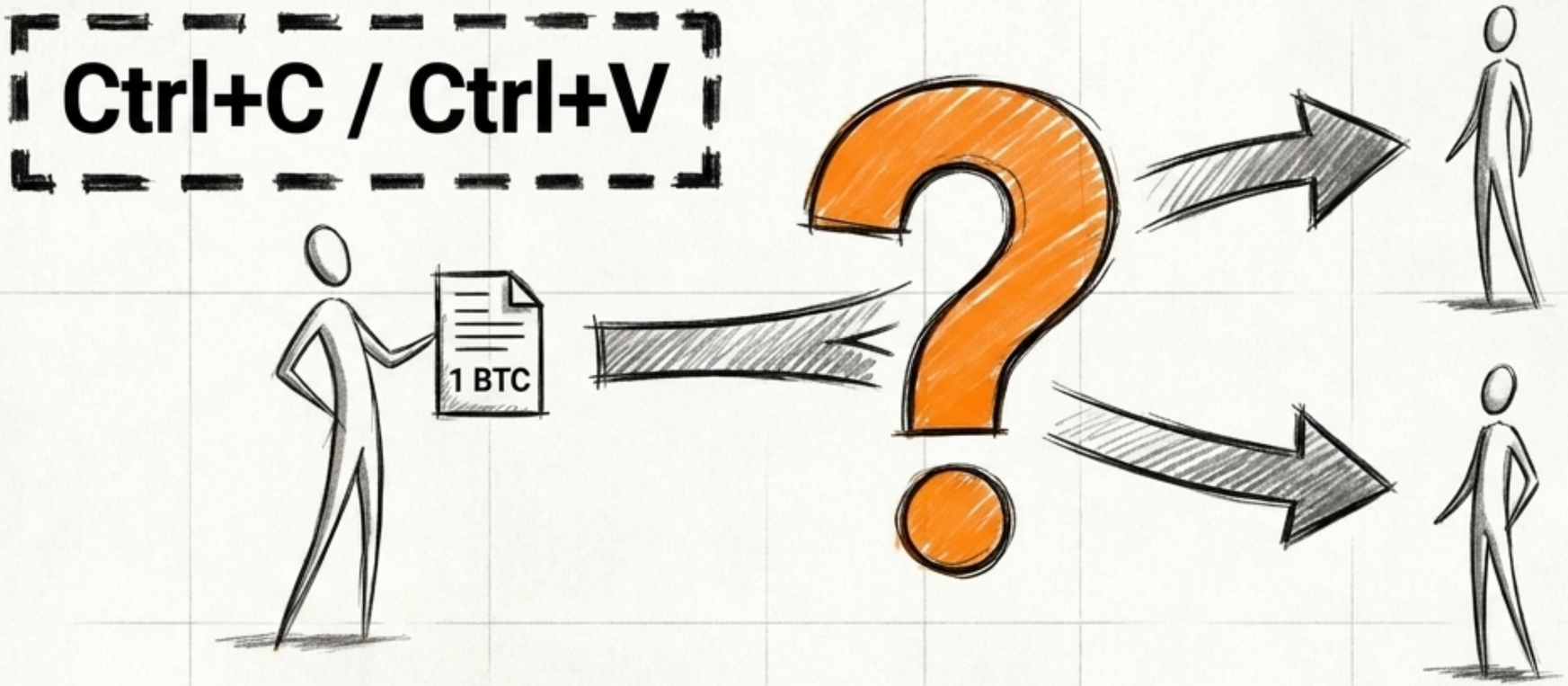
微小支付受限：高昂的交易成本直接扼杀了日常小额交易的可能性。

隐私让渡：商家必须防范客户，迫使人们提供不必要的个人信息，并默认一定比例的欺诈是“不可避免的”。

Gemini Notebook

数字货币的致命缺陷：双重支付(Double Spending)

如果去掉中间机构，我们如何防止同一笔钱被花两次？



互联网能完美复制信息，但这对于传递价值是灾难。在铸币厂模型中，中央机构知晓所有交易并决定先后顺序。去掉机构后，谁来给历史定调？

Gemini Notebook

范式转移：从依赖信任到密码学证明

中本聪的破局思路：用分布式算力代替中心化权威。

过去（基于信任的银行模型）	破局（基于密码学的比特币模型）
☐ 验证核心：可信任的第三方（Trusted Third Party）	☐ 验证核心：密码学证明（Crypto-proof）
☐ 网络架构：中心化服务器（易被单点控制）	☐ 网络架构：点对点分布式网络（节点可随时加入/离开）
☐ 决策机制：基于权威仲裁	☐ 决策机制：CPU算力投票（共识机制）
☐ 交易状态：可撤销，需承担信用摩擦	☐ 交易状态：计算上的不可撤销，保护卖方免受欺诈

Gemini Notebook

零件一：数字签名（证明所有权）

将电子货币定义为一条由数字签名构成的链条。

公钥是你的透明收款箱，私钥是唯一能打开它的钥匙。收款人可通过验证签签名证实所有权，但这依然无法防止他把同一把锁开两次（双重支付）。

Gemini Notebook

零件二：时间戳与区块（固定历史顺序）

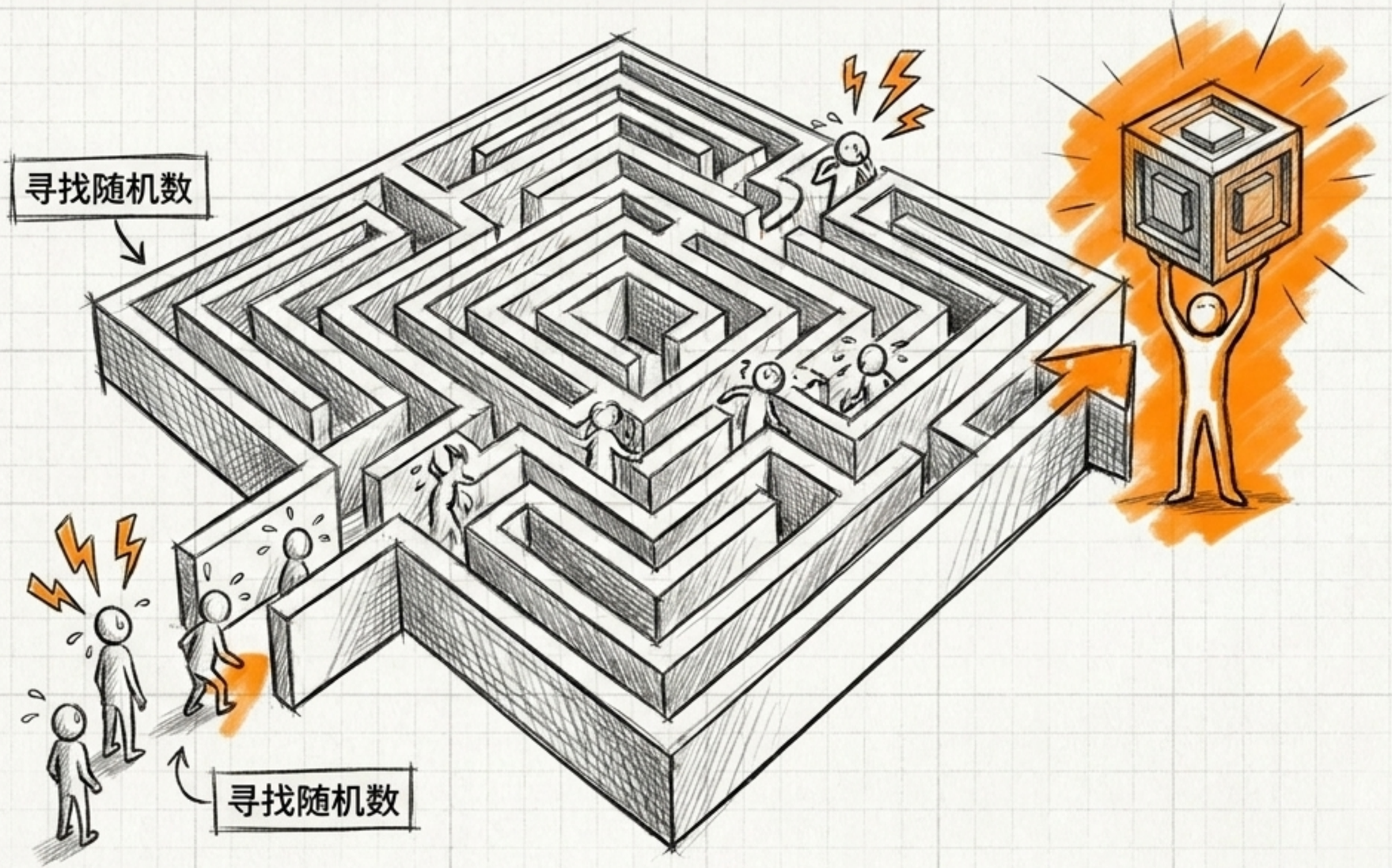
给交易盖上时间戳，用“数字指纹”将它们死死锁在一起。

哈希（Hash）即数据的数字指纹。每个时间戳都纳入了上一个时间戳的哈希值。一旦有人试图篡改中间某一页的一笔交易，该页的指纹就会改变，导致后面所有被锁链连接的页面全部作废。

Gemini Notebook

零件三：工作量证明 PoW（防作弊核心）

按CPU算力投票：用消耗物理能量的解谜游戏代替IP地址投票。



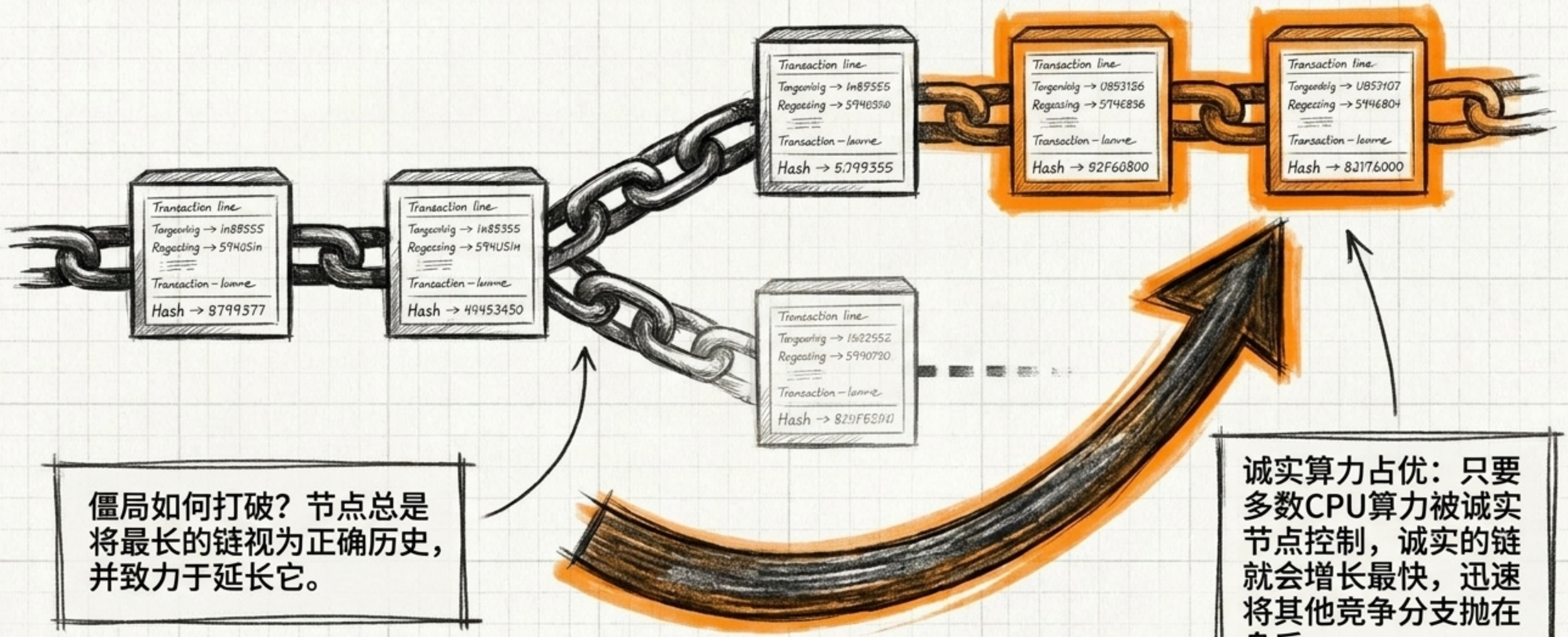
解题极难，验证极简：平均所需工作量呈指数级增长，但全网验证只需执行一次哈希。

物理屏障：由于后面的区块链接在此区块之后，篡改这一个页，必须重新消耗同等电力重做该区块及其后所有的工作量。

Gemini Notebook

零件四：最长链原则（达成全网共识）

最大算力所在，即为不容置疑的事实。



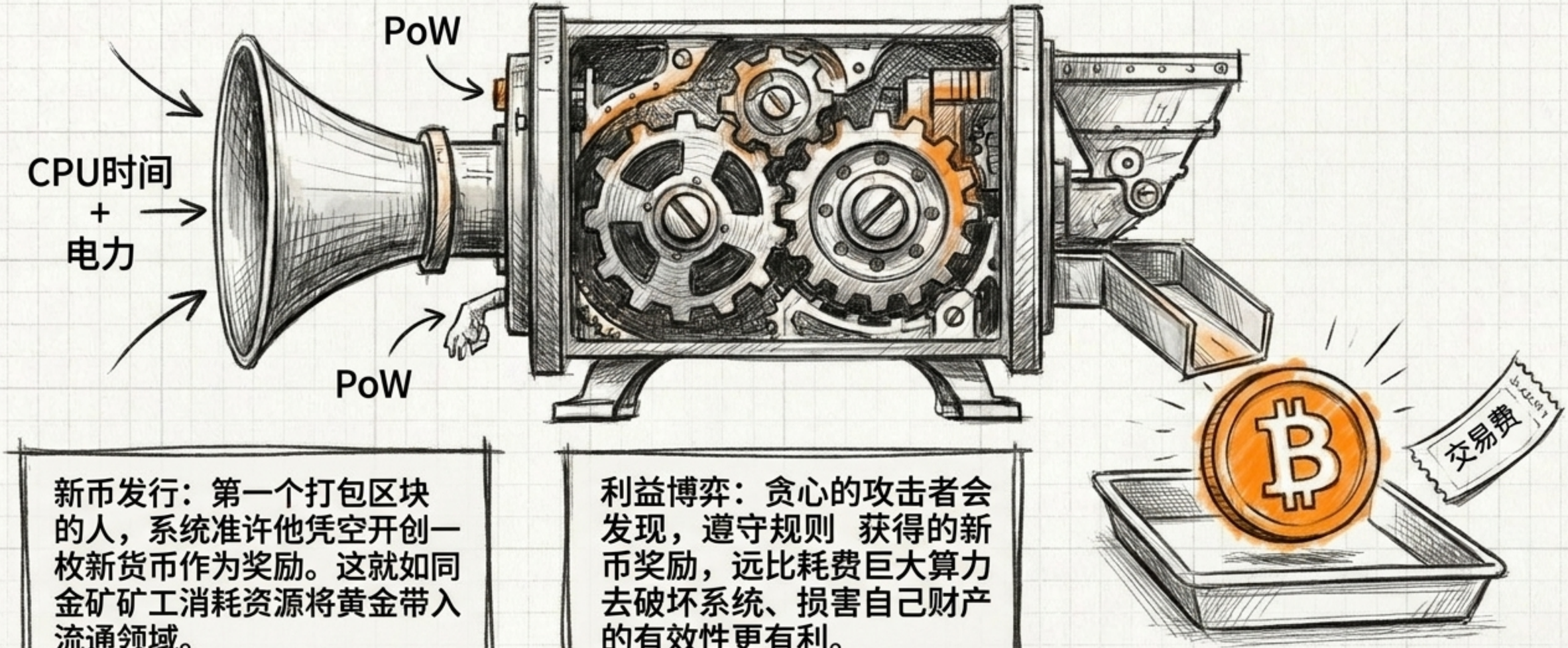
僵局如何打破？节点总是将最长的链视为正确历史，并致力于延长它。

诚实算力占优：只要多数CPU算力被诚实节点控制，诚实的链就会增长最快，迅速将其他竞争分支抛在身后。

Gemini Notebook

永动引擎：精妙的经济激励闭环

没有中央机构发行货币，如何让人们心甘情愿地提供算力维护安全？



新币发行：第一个打包区块的人，系统准许他凭空开创一枚新货币作为奖励。这就如同金矿矿工消耗资源将黄金带入流通领域。

利益博弈：贪心的攻击者会发现，遵守规则 获得的新币奖励，远比耗费巨大算力去破坏系统、损害自己财产的有效性更有利。

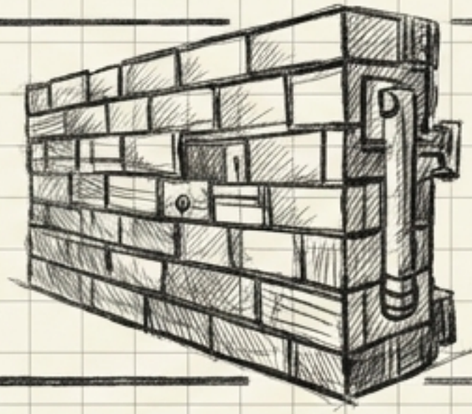
Gemini Notebook

隐私保护的范式转移

账本全网公开，但身份依然可以隐匿。

传统隐私模型

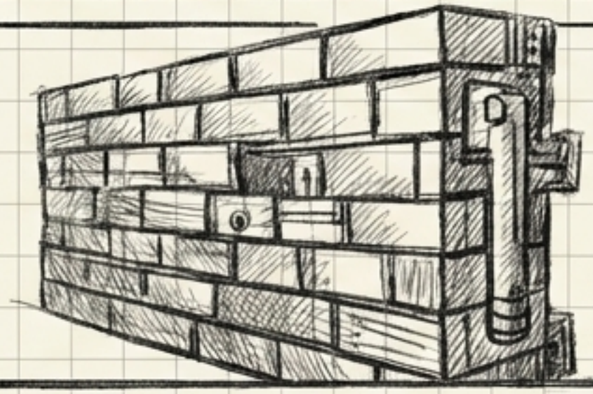
身份信息 → 交易 → 可信任第三方



公众

新隐私模型

身份信息



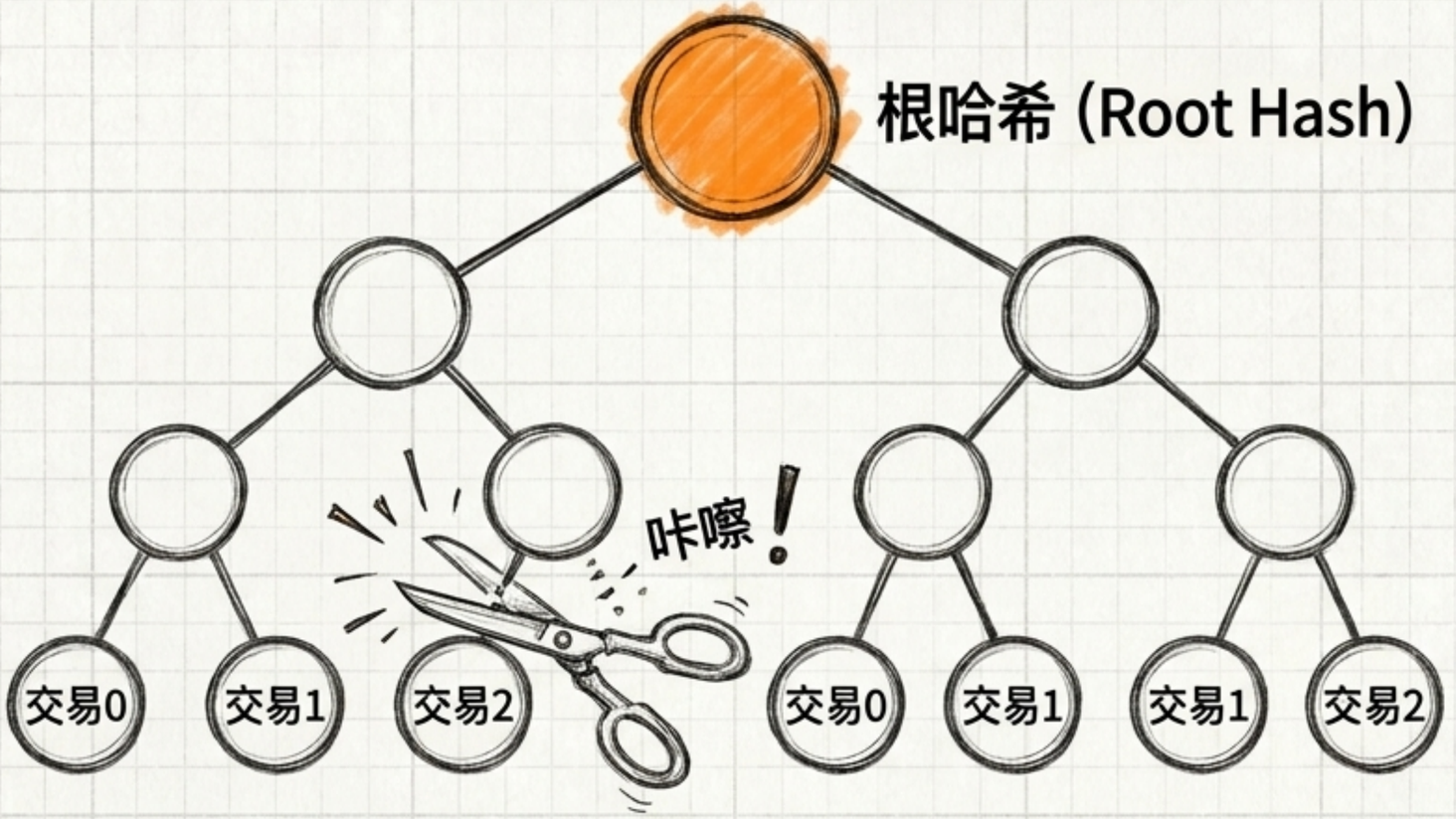
交易 → 公众

公众能看到有人正发送一定量货币给他人，但无法将交易关联到特定的人（公钥匿名）。作为额外防火墙，建议每笔交易使用新密钥对。

Gemini Notebook

空间回收：极简存储与快速验证

无需下载完整账本，老旧历史可以像修剪树枝一样被压缩。



每个区块头仅 80 bytes。

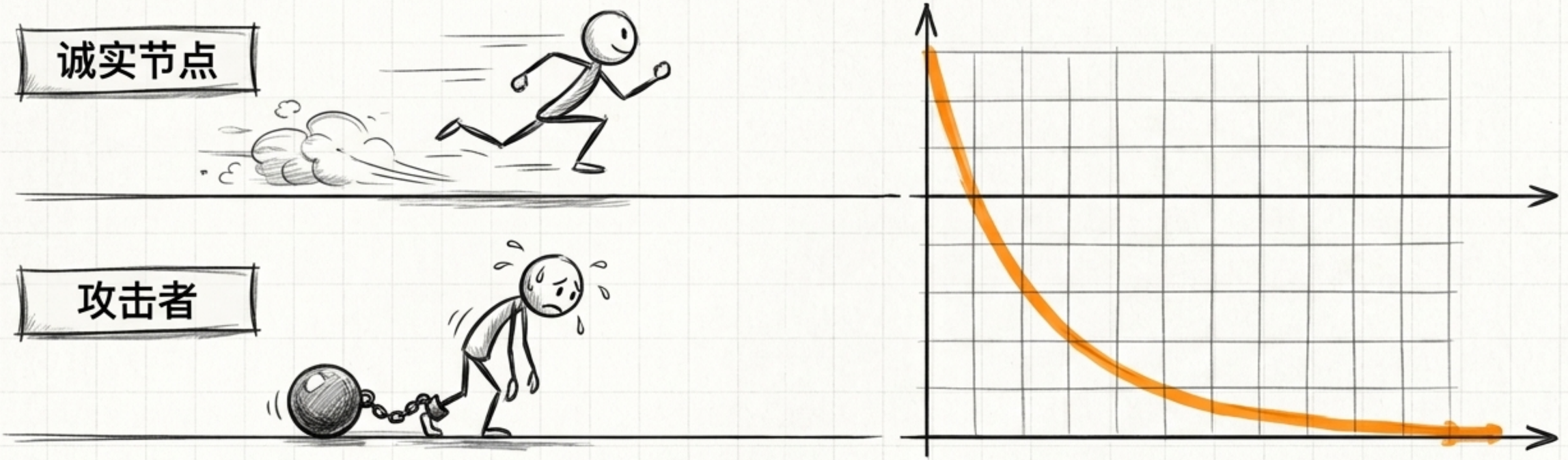
哪怕每年生成 4.2 MB 区块头，即便保存在内存里，存储也绝不是问题。

简化支付验证（SPV）：普通用户只需保留最长链的“区块头目录”，即即可安全验证支付，无需运行完整节点。

Gemini Notebook

攻击者的徒劳：安全性的数学保障

为什么计算上的篡改在物理层面不可行?



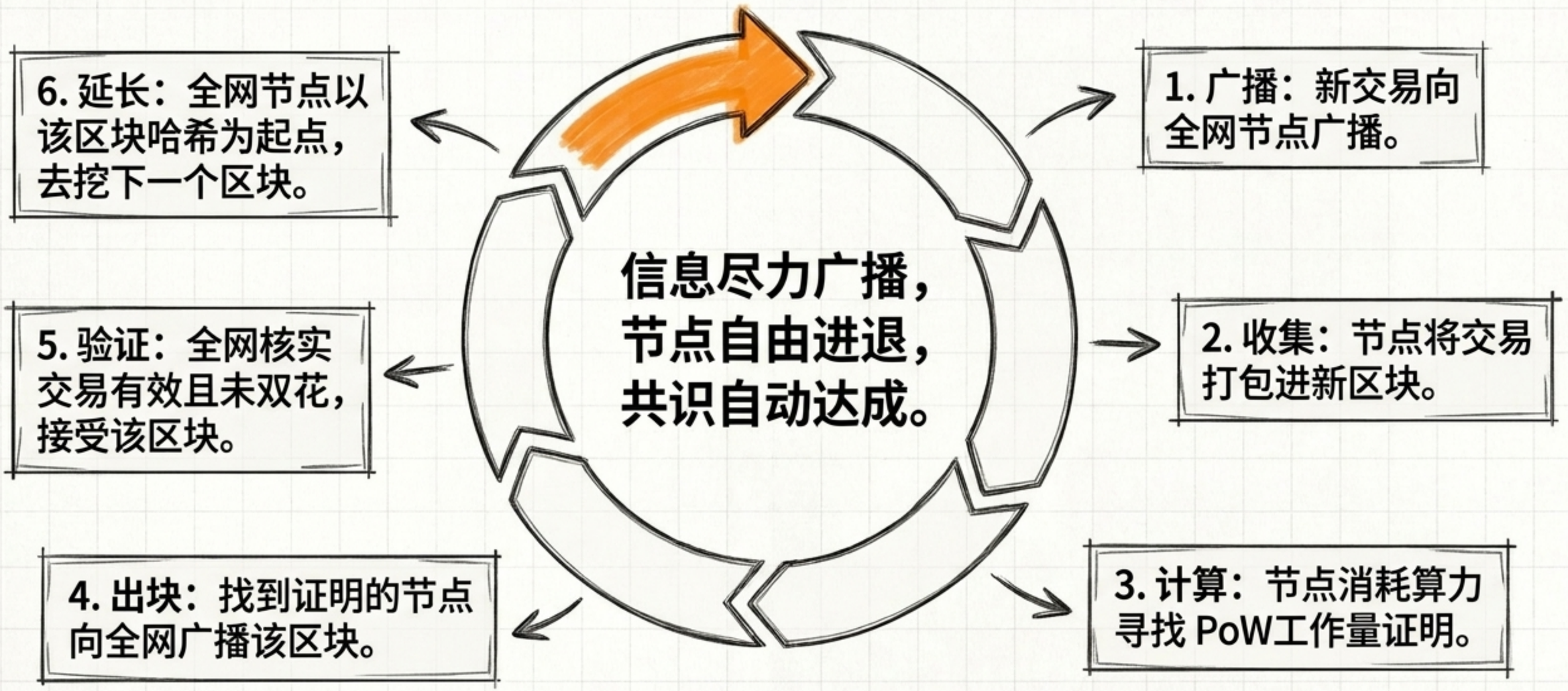
这是一场二项随机漫步的赛跑。诚实链延长一步，差距加1；攻击者延长一步，差距减1。

只要诚实算力占优（p > q），攻击者落后越多，追赶上诚实链的概率（z）就呈指数级崩溃。如果没有在早期极其幸运地快速赶上，他的篡改企图注定失败。

Gemini Notebook

终极蓝图：系统闭环运行图

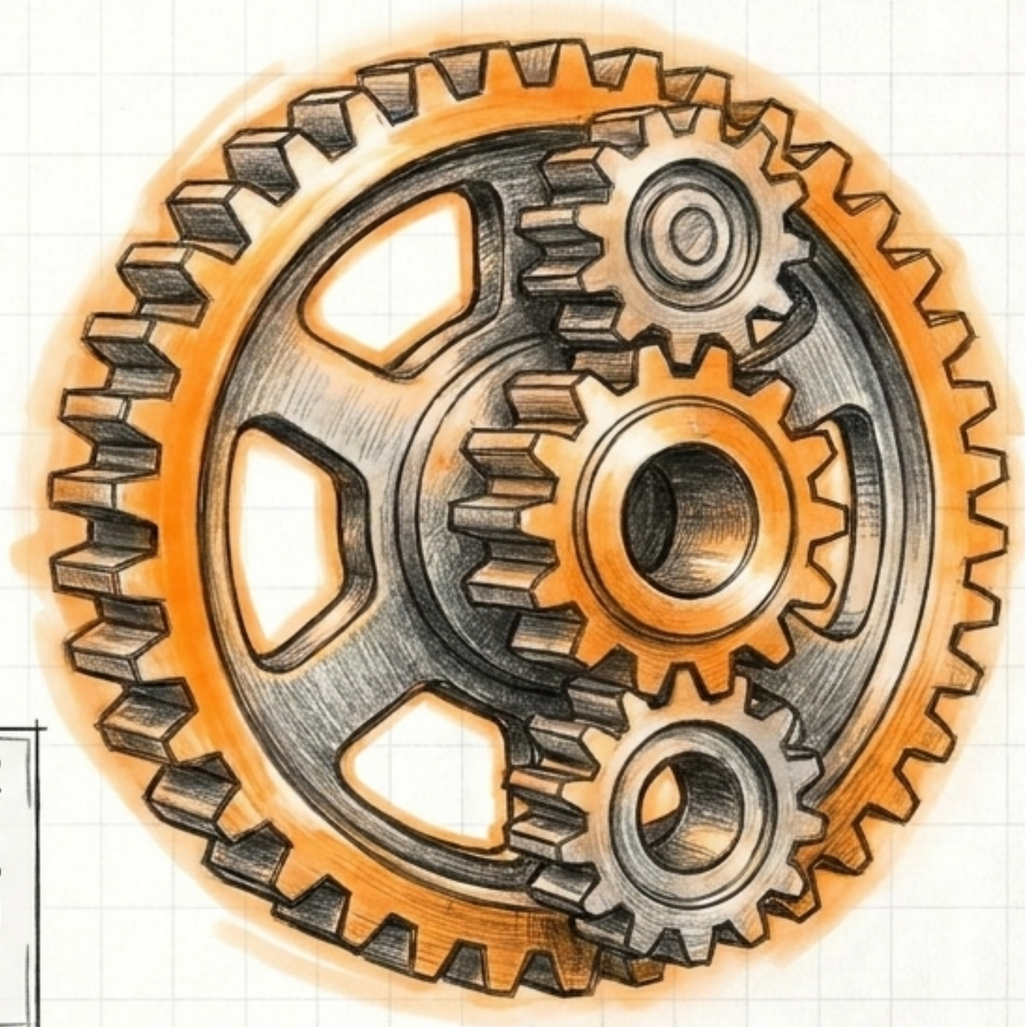
一套无需人工干预、靠数学和人性自我运转的极简飞轮。



Gemini Notebook

大道至简的架构，坚不可摧的共识

代码即法律：用极简的点对点架构，消除了对中心化信任的依赖。



算力即共识：工作量证明让篡改历史在物理和计算上变得完全不可能。

密码学取代信任：在互不相识的陌生人之间，建立起人类历史上第一个去中中心化的价值传输网络。

Satoshi Nakamoto, 2008

Gemini Notebook

Q & A

Satoshi Nakamoto, 2008

Gemini Notebook