比特币氪

BTC 永恒**-**比特币氪

未来可持续发展，无需升级 **P2P(Peer to Peer)**电子货币系统

聪史。K satoshi.k@bitcoinkrypton.org

https://bitcoinkrypton.org

抽象。

“电子现金的纯点对点版本将允许在线支付直接从一方发送到另一方，而不经过金融机构。数字　签名提供了部分解决方案，但是如果仍然需要可信任的第三方来防止重复花费，那么主要的好处就失去了。我们提出了一种使用对等网络来解决重复花费问题的解决方案。网络通过将事务散列到正在进行的基于散列的工作证明链中来对事务进行时间戳标记，从而形成在不重做工作证明的情况下无法更改的记录。最长的链不仅证明了所见证的事件序列，还证明了它来自最大的 CPU 能力池。只要不合作攻击网络的节点控制着大部分 CPU 能力，它们就会产生最长的链，超过攻击者。网络本身需要最小的结构。消息是在尽最大努力的基础上广播的，节点可以随意离开和重新加入网络，接受最长的工作证明链作为它们离开时发生的事情的证明”。

上面提到的内容是引用自中本聪的比特币白皮书摘要。

最初的比特币在其摘要中表示，其目标是通过工作证明建立一个可信的第三方电子货币系统。截至2024 年，在最初的比特币公布 15 年后，已经确认新更新的比特币程序和原始程序之间的兼容性无法正常工作，并且由于该问题衍生的比特币已经得到确认。它提出了未来可持续性的问题，作为解决问题的替代方案，它是一种新的电子货币程序，可以在未来的任何时间点连续运行，无 需更新，无需满足比特币原始目标的可信第三方。我们想用比特币宣布氪星。

0.中本聪的比特币和现在的比特币是不同的。

比特币始于 2009 年 1 月发布源代码，是一种 P2P 金融工具。尽管最初存在疑虑，但比特币已经发展成为全球金融的重要资产，其用户数量和交易量稳步增长。每个区块的 1 兆字节固定限制允许每个区块大约进行 2,100 笔交易。在这个有限大小的分布式分类账中，引入了一种竞争机制，优先传输提供较高费用的交易，而那些费用较低的交易则存储在 Mempool 内存空间中。随着网络使用的增加，费用也相应上涨。

在众多能够大幅提高比特币交易极限的提议中，使用闪电网络的 SegWit 更新将记录大宗交易时的签名部分与数据部分分离，并将签名部分发送到闪电网络。它提出了一种双重方法，即记录数据块和在比特币网络上记录区块。然而，尽管比特币矿工网络及用户和支持者团体最初对引入 SegWit 存在阻力，随着时间的推移，其效率得到了认可，数据块记录在比特币网络上。

2017 年，随着利润视角的出现，SegWit 升级被广泛接受，因为它只不过是软分叉，原比特币来源与未来版本相互兼容，且区块链数据可以在节点之间顺利同步。最终，SegWit 升级被应用于比特币的原代码。正因为如此，比特币交易效率提升了约 2 倍。然而，尽管与当前版本相比，原始程序不兼容，但几乎无人

对此问题表示关注。

目前，比特币网络面临危机。中本聪已不再活跃，他最初的比特币程序也不再有效。这揭示了比特币区块链（不兼容性）最严重的矛盾与威胁。

比特币开发者提出了两种方法：SegWit 方法和 SegWit2X 方法，用于提高比特币的交易速度并解决 Mempool 中交易积压的问题。尽管 2017 年 SegWit 升级已经完成，但 Mempool 内积累的未处理事务问题仍未完全解决。

前者（SegWit 方法）通过软分叉方式，将签名部分与数据部分分开，而非物理上增加 1MB 的块容量，因此理论上实现了 4MB 的块容量扩展，这种方法与中本聪的原始比特币程序完美兼容。而 SegWit2X 方法则通过硬分叉将块容量提高至 2MB，改进了多个部分，但也分支成了完全不同的新区块链。大多数用户倾向于软分叉，因为它既不会破坏中本聪区块链的核心特性，又提高了速度与安全性，修复了多个 Bug，特别是将 TPS 提高了 4 倍，并降低了传输成本。这种升级被期待为完全兼容的解决方案。然而，实际上，软分叉并未完全成功（相关证据已在本文第 5 项中提供）。

比特币网络的设计与中本聪的“复活节彩蛋”息息相关：总量 2100 万币，每 21 万块奖励减半。一个区块允许约 2,100 笔交易。当 2021 年后奖励再减少 21 倍时，区块链奖励将趋于 0，这是设计使然。当奖励减至最小单位 Satoshi 时，比特币将不再继续减半。

80 年后，比特币减半奖励将完全停止。然而，由于比特币设计旨在通过每块的交易费用为工作量证明参与者提供额外补偿，因此比特币早期版本计划，即使减半结束后，也可以维持网络运转。因此，设定适

合时代的适当费用对于比特币网络的持续维护至关重要。如果因 SegWit 应用导致费用降低，这可能会使比特币网络面临维护危机。根据 Mempool.space 的数据，费用补偿变化范围从 0 到 0.3 BTC 不等。在某些情况下，甚至可能出现没有费用补偿的零奖励。

比特币的价值与可信度得以维持，是因为公众相信比特币总量 2100 万的不可改变性，相信区块链技术不可伪造，且比特币网络的去中心化特性使其免于外界干预。正因如此，比特币被认为是地球上最有价值的资产之一。如果未来某位开发者背弃信念，发行超过 2100 万比特币，或者以效率或创新之名修改规则，比特币的价值可能会发生不可预知的波动。

比特币已通过 SegWit 更新采用双重分布式账本系统，将现有统一分布式账本分为数据与签名部分。我们必须认识到，这是一项重大变革，其背离了公众认为比特币如黄金或钻石般具有永恒价值的信念。

1. 无需更新即可持续

比特币氪(Bitcoin Krypton)是一个项目，其目的是在没有可信第三方干预的情况下，完全继承个人之间的电子货币系统，这是中本聪比特币的设计目的。

比特币氪是作为一种 P2P 电子货币程序开发的，可以在未来继续运行，无需更新。然而，比特币 氪的原始版本是通过参考、模仿或修改开源程序而创建的，即使在程序完成后进行了充分的测试，也不应完全信任。这意味着可能会出现未知的错误。尽管任意开发者都可以通过效率流程来提高 性能、纠正错误和升级，但比特币氪的原始版本程序和更高版本程序必须兼容。

2. 比特币减半和区块循环

比特币的总货币供应量为 2100 万，设计为每 10 分钟开采 1 块。每 21 万块达到半衰期，21 万块有

4 年的周期。最初设计的是每块 50 个比特币的挖矿奖励，84 万块过去后，已经有 4 个减半，导致现在的每块奖励 3.125 个比特币。

如果块周期被设置为网络之间广播的最小必要时间，以防止工作验证的节点记录中的错误，则必须考虑几个变量。考虑互联网的允许等待时间等。，时间越长，错误越少。但是，工作证明的最短时间不应短于 3 秒。比特币将每块的验证时间设置为 10 分钟，降低了出错的可能性，但交付资产的时间设置使得它不符合人类的生活模式。人们认为，人类最舒适的时间是每块不到 1 分钟，而不是每块 10 分钟。根据经验，很明显，如果比特币的区块周期小于 10 秒，将会非常方便。然而，不需要将块周期设置为 1 秒或更少。一秒是人类在物理上感受到的最小时间单位，在人体中体现已久。单位小于一秒的区块链对人类来说不是区块链，操作它需要巨大的运营成本。出现这种情况，使得区块链不可能实现匿名和去中心化。因此，据透露，比特币氪被设计为维护 3 秒的块，并允许任何人通过一个完整节点可以在家用计算机上充分操作的环境来使用分布式账本。如果挡位周期在 3 秒左右，我有信心以人类的标准来看不会觉得慢或者不舒服。

为期四年的整体奖励减半是一个明显的因素，为维持比特币区块链提供了动力，但对于那些参与工作证明的人来说，这也是一次冒险。为了参与工作证明，必须首先考虑活动的盈利性，因此活动的参与者不会愿意参与工作证明，除非参与的盈利性至少得到保证。这将引发人们对比特币未来可持续性的质疑。比特币的高费用对于确保比特币未来的可持续性至关重要。它是该系统最重要的元素，通过燃烧中本聪比特币原始源代码中呈现的每块比特币转让费的总额来补偿工作证明中的参与者，并根据燃烧的金额奖励工作证明中的参与者。

因此，SegWit 的每块更多交易和更低转移费用的目标可能首先会破坏比特币单一区块链的可靠性，他们提出的低费用可能会影响未来比特币区块链能否维持下去。这引起了怀疑。

为了解决这些疑问，确保比特币氪在未来是可持续的，并激励持续的工作证明参与，考虑了各种因素，如块周期、半衰期和总报酬，并将其应用于该计划。

为此，它被设计为最多能够表示 11 位小数(11 位小数位)，并且传输费用相对于补偿的范围被降低，使得费用每三个半衰期减少十分之一。

这可以比比特币的 8 个小数位小 1000 倍，但通过使用比特币的数据类型 unit64，每块数据的效率得到了提高。

(作为参考，1 个Satoshi 产生 1 个额外单位的 1000 氪。)

比特币氪快速测试，从 1 块到 1,100,000 3 秒的块周期。第 1，100，001 块后，将发布源代码和程 序，块周期为 63 秒，最长持续 210 万块。从第 1 块到 210 万块，每块奖励 5 个币。之后，每 210 万个块，块周期将减少 3 秒，在第 21 个减半时，块周期将减少到 3 秒。

比特币氪的总货币与 2100 万个个体比特币相同，但以太坊地址规则它被设计成与以太坊的 Dapps 兼容。

比特币氪使用现有的比特币方式 Mempool，不引入基于高额费用的竞争方式，并计划根据每笔交易使用的实际使用量，使用与数据权重一样多的费用，210 万块。它旨在将每 630 万块的费率降低 1/10，这是其使用限制的 3 倍，但设计为每 2100 万块增加 100kb。

3.区块链节点的数据增长率和分散性

比特币节点每三年大约使用 100GB 的完整节点存储空间，截至 2024 年 6 月 5 日，完整节点需要 577GB 的存储空间。

另一方面，以太坊 mainnet 截至 2024 年6 月5 日的全节点存储空间为 18.195TB，每年必须向节点添加 5TB 以上

以太坊 2 的更新被命名为 2022 年 9 月的“合并”更新，这标志着从现有的工作量证明 (POW) 方法向权益证明 (POS) 方法的过渡，这将引发以太坊网络的快速变化和使用量的增加。

随着以太坊在 2024 年 3 月 13 日进行 Denkun 升级（EIP-4844），以太坊的交易手续费最多降低了 1/60，平均降低了 75% 以上。这显著减轻了智能合约和 DAPP 开发与使用给用户带来的财务负担。

然而，以太坊最大的挑战在于节点物理硬盘需求的增加。为缓解这一问题，实施了 Verkle 树升级以更高效地管理存储状态数据所需的磁盘空间。尽管努力减少存储需求的增长，但由于数据需求的增，用于存储的磁盘空间预计仍将持续增长。

随着时间推移，预计以太坊相关开发者直接操作完整节点的难度会越来越大，节点数量将不可避免地减少。这表明区块链在长期运行中可能面临结构性问题，并可能从分布式账本逐渐转变为集中式账本。

比特币氪的每块大小从 100kb 开始，一个完整节点占用的存储空间也在逐步增加。预计每年的磁盘需求为 30GB 至 50GB，其设计能够应对区块数据每年平均增加 5% 的情况而不会产生问题。相比之下，当前技术使每 GB 存储设备的价格每年下降 10% 以上，同时考虑到维护成本，以确保未来的可持续性。

4. 比特币氪的用途

比特币氪(Bitcoin Krypton)的目的是为未来的工作证明参与者维持一个有效的补偿体系，作为一个追求完全匿名、没有第三方干预的点对点金融程序，并确保未来的改进版本与已经发布的原始程序兼容。完成了。

即使 2024 比特币氪是由特定的团体和开发者开发的，但在公布后的一定时间内，初始开发者和最初指定的Satoshikei 的职责将被终止，所有权利将转移给一个新的 Satoshikei，一个匿名的替代者。域管理、开源管理、邮件管理、初期矿业资产管理下放，2024 年 12 月 31 日前解散初期开发者小组。

比特币氪不仅没有任何资产价值的保证，而且也没有对其未来的生存、上市、愿景或有计划社区的运营进行规划。

比特币氪网官方并不存在，也不属于任何个人或团体。如果有人愿意，有可能把比特币氪上市，任何人都可以随心所欲地使用这个名字。但使用时不得主张任何权利，不得使用任何官方称谓或名称。为了满足上市条件，不得随意写入一般交易所要求的基本文件中所要求的关于官方主体、成员、机构和社区的内容。

比特币氪的原始开发者以及在其发展中发挥作用的人，对未来比特币氪产生的任何后果不承担任何法律或经济责任。

但是， 您可以讨论新的想法、建议、新开发的讨论、新源代码的验证和认证等。通过给 satoshi.k@bitcoinkrypton.org 发邮件。我们不能保证得到回复，但只要消息是友好和礼貌的，而不是辱骂，垃圾邮件或欺诈性的，任何建议都将被听取和考虑。在某些情况下，比特币氪在各交易所自愿上市

的补偿等。可以充分讨论。

5. 中本聪的比特币源代码实验。

比特币的原始源代码 Bitcoin-V0.1 基于中本聪于 2008 年 11 月 1 日(周六)撰写的比特币白皮书(bitcoin.pdf(m D5 sum d 56d 71 ecadf 2137 be 09d 8 B1 d 35 c 6 c 042)，发表于 2009 年 1 月 8 日 14:27。正式公开版发布时间:40(美国东部时间)，私有版在此之前发布时间为 2008 年 11 月 16 日。

该版本不在比特币当前的源代码公开地址(https://github.com/bitcoin/bitcoin)，但地址不同(https://www．Metz Dowd．com/piper mail/cryptography/2009-January/014994.html)。关于 SegWit，我们进行了一个直接实验来反驳当前开发团队关于软分叉的错误主张。 首先，由于编译和执行从 metzdowd.com 获得的源代码，无法找到用于广播的最新节点，也无法与 节点同，因此该实验没有意义。执行后，只报告了“未连接”错误。我们通过各种测试发现， 用于连接多个节点的广播地址目前不起作用，并且用于此的 IRC 地址已不存在。

由于某种原因，比特币的官方 GitHub 账户有 24.x 作为最老的版本，最新版本是 27.x。接下来测试的源代码是 bitcoinv0.3。

在块 124、276，节点同步不再可能，输出消息如下。

```
ERROR: ConnectInputs() : fb0a1d8d34 VerifySignature failed
InvalidChainFound: invalid block=0000000000004939267f
height=124276  work=66138705631989025O8
```

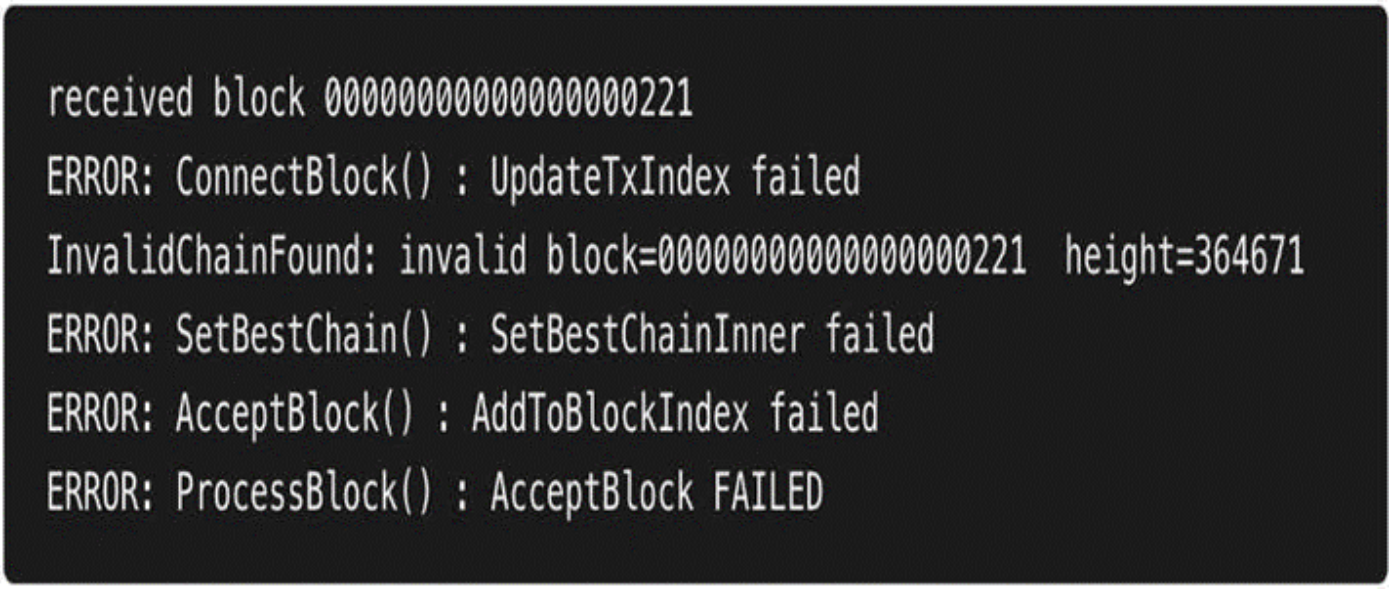
在V0.4 和v0.5 中，在块 258、354 处无法同步，并显示以下消息。

```
EXCEPTION: 11DbException
Db::put: Cannot allocate memory
bitcoin in ProcessMessage()

ProcessMessage(block, 901212 bytes) FAILED
received block 0000000000000023e872
REORGANIZE
```

V0.6 版在 364，670 块不能再同步，输出如下消息。

```
EXCEPTION: 11DbException
Db::put: Cannot allocate memory
bitcoin in ProcessMessages()

ProcessMessage(block, 999787 bytes) FAILED
received block 00000000000000001d3
```

V0.7 版不能再从块 364，671 同步，输出下面的消息。



所有错误的原因被认为是相同的。通过将块分成数据和签名部分，可以怀疑应用 SegWit 的最新节点和过去的节点由于各种未知原因而冲突。换句话说，很明显，软分叉有效地打破了过去和现在的程序相互兼容的主张。

6. 氪

氪是一种化学元素，符号 Kr，原子序数 36。它是一种无色、无嗅、无味的惰性气体，在大气中以微量存在，通过液态空气的分馏获得。它于 1898 年由英国的威廉·拉姆赛首先发现。

发现氦和氩的拉姆齐开始寻找原子量在 4 到 40 之间的稀有气体。1898.他们通过烧红的铜和镁蒸馏出少量液态空气，发现了一种新的绿色元素。因为这种绿色元素比其他稀有气体更难发现，所以被命名为“氪”，在希腊语中是“隐藏的东西”的意思。

与惰性气体氦不同，它具有将高能物质的分子改变为较慢移动速度的特性。当吸入氪气时，它会产生一种带有低音声波的声音，这与吸入氦气相反。

看电影《超人》的时候，氪石这种想象中的物质被用作超人的弱点。这是一种虚构的物质，以氪命名。

比特币氪在削弱 ASIC 芯片等非正常途径在挖矿(工作证明)的意义上，倡导基于 CPU 的挖矿，并推出了基于 web 的一键挖矿方式，让任何人都可以轻松参与工作证明。

此外，最初比特币程序的最小单位——Satoshi(8 位小数)位数被进一步细分和扩展为氪(11 位小数)位数。换句话说，1kr(氪)是 0.00000000001BTCK，1,000kr 是 1 satoshi。换句话说，1BTCK可以表示为 1 亿个 satoshi 或者 1000 亿个氪。

比特币氪经历了 21 次减半和 7 次费用削减，要求费用低于Satoshi，为了顺利运行这一点，比特币网络中引入了一个名为氪的单位。

如果比特币氪的可执行程序的数据类型设置为 unit64，则可以进行最多 2100 万的总货币量和最多 11 位小数的计算。因此，与使用 unit128 数据类型相比，可以更有效地减少块大小。

7. 管理实体的消失:比特币氪金的去中心化之路

比特币氪金的目标是实现彻底的去中心化，而去中心化的最终实现意味着管理比特币氪金的实体将不再存在。主题围绕比特币氪金的命运及其独特的证明过程展开。比特币氪金的节点从源代码中的 Seed 节点连接和探索开始。

Seed 节点的连接过程如同蜘蛛网般，将比特币氪金的世界观连接起来。而 Seed 节点必须不断添加和更新，这直接影响着比特币氪金网络的生命力。

为了增强这种生命力，比特币氪金设计了一个特殊的程序，使其能够像病毒一样广泛传播。由于任何节点都可以成为 Seed 节点，最初的 Seed 节点通过向提供节点信息的参与者提供特殊奖励来实现传播。

补偿的方式是量化作为信息提供的 Seed 节点状态(即服务器的维护能力)，然后根据评分每月进行差异化补偿。

随着比特币氪金网络中 Seed 节点的供应逐渐充足，我相信这些节点将能够维持一个稳定的去中心化网络。

BITCOIN KRYPTON