量子货币与信任经济学：从比特币到量子闪电

XXX, XXX, XXX

Abstract

本文探讨了数字货币从比特币到量子货币的演化，聚焦信任与稀缺性的底层机制。比特币通过计算共识与密码安全开创了去中心化价值转移，但其依赖的经典假设使其在量子攻击与可扩展性问题面前显得脆弱。量子货币借助不可克隆定理，提供了一种截然不同的路径：不可伪造性植根于物理定律本身。报告回顾了集中式与去中心化量子货币架构，重点介绍作为公钥、自稀缺系统的量子闪电。同时分析了在量子货币体系中抑制无控制发行和通胀的策略，如计算难度、状态空间限制以及链式验证。最后，讨论了量子货币成为一种可行、抗通胀交换媒介所需克服的实践与理论挑战，并强调其重塑数字信任与经济价值的潜力。

关键词：比特币，量子货币，量子闪电，通胀。

1 从比特币到量子货币

2009 年比特币的出现[1]标志着第一个大规模去中心化数字货币系统的实现。它引入了一个突破性的理念：货币价值可以在没有任何集中式权威的情况下被维护并安全转移。这一理念通过区块链得以实现——区块链是一个由被称为矿工的参与者网络共同维护的分布式、仅追加的账本。每笔交易都会作为区块的一部分被记录，而新块则通过称为工作量证明（Proof of Work, PoW）的高耗能计算过程被添加到链上。

因此，比特币的稀缺性是计算的函数：每一个新的货币单位都作为解出密码难题的奖励而产生，需要大量计算和能源资源。系统的完整性并非源自对某个个体的信任，而是来自数以千计的独立节点对每笔交易的全球共识验证。

然而，比特币的安全性根本上建立在经典密码假设之上。整数分解、椭圆曲线离散对数以及哈希原像问题的困难性阻止了伪造与双花。像 Shor 算法[2]和 Grover 算法[3]这样的量子算法理论上能够破坏这些假设，使比特币的公钥基础设施在后量子世界中变得脆弱。此外，比特币架构还遭遇可扩展性限制与极高的能源消耗，使其难以成为一种通用的交换媒介。

量子货币提出了完全不同的范式。它不依赖计算难度，而是依托量子力学不可违背的物理定律。依据不可克隆定理，[4]无法对未知量子态制作完全相同的副本。利用这一性质，可以设计让每一张量子” 钞票” 由唯一且不可复制的量子态表示的货币体系。因此，伪造不仅在计算上几乎不可能，而且在物理上被禁止。不过代价是实用性：量子态脆弱、对环境噪声敏感，并且需要专用的量子存储与测量设备。因而，量子货币系统目前仍主要停留在理论层面——但在概念上，它们代表了超越比特币等经典密码货币的一大飞跃。

2 量子货币的架构：集中式方案与量子闪电

现有研究通常将量子货币划分为两大设计范式：集中式量子货币，以及以量子闪电为代表的去中心化或公钥量子货币。

1. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Bitcoin.org*, 2008, https://bitcoin.org/bitcoin.pdf.

2. Peter W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal on Computing* 26, no. 5 (1997): 1484–1509, https://doi.org/10.1137/S0097539795293172.

3. Lov K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search,” *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, 212–219, https://doi.org/10.1145/237814.237866.

4. Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010), https://doi.org/10.1017/CBO9780511976667.

2.1 集中式量子货币

20 世纪 70 年代，Stephen Wiesner 提出了最早的量子货币方案,[5]如今被视为量子密码学的奠基性工作。在 Wiesner 的模型中，受信任的银行充当量子钞票的发行者。每张钞票由两部分组成：一个经典序列号，以及用随机选择的非正交基编码的相应量子态。银行维护一个私有数据库，将每个序列号与其特定的量子态相对应。

当持有人请求验证钞票时，银行会在相应基上对给定量子态进行测量。如果测量结果与数据库记录一致，该钞票即被判定为真。由于对未知量子态的任何测量或复制尝试都会不可逆地扰动该状态，伪造在物理上被禁止。

尽管理念优雅，这一设计存在明显局限。所有验证都必须经过发行银行，这重新引入了中心化与对单一可信实体的依赖。此外，银行必须维护并访问所有合法量子态的秘密记录，这带来了可扩展性与隐私方面的顾虑。因此，尽管 Wiesner 的构想展示了量子货币的基本可行性，却并不适用于大规模、去中心化的经济体。

2.2 量子闪电与公钥验证

为克服上述限制，研究者试图设计可以公开验证的量子货币——任何参与者都能在无需联系中心权威的情况下验证真伪。在这类方案中，由 Mark Zhandry 提出的量子闪电[6]是最先进且概念上最优雅的方法之一。

在量子闪电中，每一个货币单位是一道独一无二的” 闪电”——一种连生成该闪电的算法也无法再次复制的特殊量子态。系统依赖抗碰撞的量子哈希函数以及确保不存在两份相同闪电的特定密码假设。验证过程是公开的：任何人都可以运行一个多项式时间的量子算法来判定给定量子态是否为有效闪电，这与验证数字签名类似。

其创新之处在于系统的自稀缺性：无需中央发行者，却保证复制在物理与算法层面都不可能。这让量子闪电成为比特币等去中心化加密货币的量子对应物，但具有一个关键差异——稀缺性直接源自量子力学结构，而非经济成本或计算努力。

3 防止无限铸币与通胀

尽管去中心化量子货币解决了伪造问题，但新的挑战随之而来：如何防止无节制的货币创造。如果任何参与者都能随意生成有效的量子闪电，货币供给将无限膨胀，从而摧毁其价值。因此，量子货币必须包含调节发行的机制——类似于比特币的挖矿难度或法币的货币政策。

为此，研究者提出了若干策略，每种策略都有独特的技术实现方式。

3.1 计算难度调节

一种直接方法是将生成有效量子态与求解困难的计算问题绑定。在 Zhandry 的设计中,[7]一道闪电只有在满足特定的公开哈希条件时才有效——也就是说，它是一种测量结果对应某个密码哈希值原像的量子态。由于寻找这类状态在计算上很困难，自然限制了新货币的产生速度。难度也可以动态调整，类似比特币中的挖矿难度，从而维持稳定的发行速率。

技术实现：考虑这样一种量子货币方案，其中有效状态 $|\psi\rangle$ 必须满足 $H(|\psi\rangle) < D$，其中 H 是量子可访问哈希函数，D 是难度阈值。铸币过程包括：

1. 量子态制备：使用带随机输入的参数化量子电路生成试验量子态 $|\psi_{\text{trial}}\rangle$。
2. 哈希验证：应用量子哈希算符 $\hat{H}$ 并测量输出。如果结果低于目标难度 D，该状态被接受为有效货币。
3. 动态调整：难度参数 D 在每 N 个区块后根据实际发行速率与目标速率更新：$D_{n+1} = D_n \times \frac{T_{\text{target}}}{T_{\text{actual}}}$，其中 T 表示时间间隔。

5. Stephen Wiesner, “Conjugate Coding,” Original manuscript written circa 1970, *ACM SIGACT News* 15, no. 1 (1983): 78–88, https://doi.org/10.1145/1008908.1008920.

6. Mark Zhandry, “Quantum Lightning Never Strikes the Same State Twice. Or Does It?,” *Journal of Cryptology* 34, no. 4 (2021): 37, https://doi.org/10.1007/s00145-021-09405-0.

7. Zhandry.

该机制类似比特币的减半机制，但在量子层面运作。关键优势在于量子哈希函数可被设计为即使对抗量子对手也具备抗碰撞性，使用量子密码学技术如量子安全单向函数或可提取见证加密。寻找有效状态的计算成本随难度参数指数增长，确保货币供给以可控、可预测的速率扩张，不受量子计算能力进步的影响。

3.2 限制量子状态空间

另一种方法是限制可接受的量子态集合。如果系统的哈希函数或验证算符仅定义有限数量的有效状态，那么总货币供给天生受到上限约束。这一方法在希尔伯特空间的层面直接引入稀缺性——只有有限个正交态满足验证条件，通过物理限制而非协议控制来防止通胀。

技术实现：将货币状态空间定义为完整希尔伯特空间的有限维子空间 $\mathcal{H}_{\text{money}} \subset \mathcal{H}$。具体而言：

1. 正交基构造：选择有限的 N 个相互正交量子态集合 $\{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_N\rangle\}$，它们构成 $\mathcal{H}_{\text{money}}$ 的完备基。这些状态被选择为专门设计的验证算符 $\hat{V}$ 的本征态，具有不同本征值。
2. 叠加态编码：每个有效量子货币令牌是该子空间内的相干叠加：$|\psi_{\text{valid}}\rangle = \sum_{i=1}^{N} \alpha_i |\phi_i\rangle$，其中系数 α_i 通过量子指纹编码唯一序列号。
3. 硬上限执行：由于维度固定为 N，可区分（近似正交）货币状态的最大数量被 N 限制。任何创建额外状态的尝试要么落在 $\mathcal{H}_{\text{money}}$ 之外（验证失败），要么与现有令牌非正交（违反唯一性）。

该方案可使用拓扑量子码或稳定子码实现，[8]其中码空间本身充当 $\mathcal{H}_{\text{money}}$。例如，使用参数为 $[[n, k, d]]$ 的量子纠错码，逻辑码空间维度为 2^k，精确提供 2^k 个正交货币状态。验证过程通过测量稳定子生成元检查给定状态是否位于码空间内。[9]这种方法自然防止通胀：一旦所有 2^k 个令牌被发行，就无法创建新的有效令牌而不违反正交性约束或码结构。

3.3 基于链式或签名的验证

更复杂的策略是通过量子签名链将每一个有效状态与之前的状态关联起来。[10]在这样的" 量子区块链" 中，每个新铸造的闪电都包含从早期闪电测量结果导出的编码信息。这既强制了发行的时间顺序，也让货币供给具备公共可追溯性。尽管仍处于理论阶段，这类链式验证机制有望通过量子定律与密码一致性来建立完全去中心化的货币政策。

技术实现：构造量子区块链，其中链中位置 n 的每个货币状态 $|\psi_n\rangle$ 满足：

$$|\psi_n\rangle = U_n(\vec{m}_{n-1}) |\phi_{\text{seed}}\rangle \tag{1}$$

其中 U_n 是由前一状态 $|\psi_{n-1}\rangle$ 的测量结果 $\vec{m}_{n-1}$ 参数化的幺正算符，$|\phi_{\text{seed}}\rangle$ 是固定的初始种子状态。实现过程如下：

1. 创世状态：区块链以通过分布式随机性协议（如创始参与者间的量子抛硬币）选择的公开可验证创世状态 $|\psi_0\rangle$ 开始。
2. 链式铸币：要铸造新令牌，参与者必须：
   - 从网络获取最新有效状态 $|\psi_{n-1}\rangle$
   - 在特定基上执行预定测量集，得到经典结果 $\vec{m}_{n-1}$
   - 使用这些结果参数化量子电路 $U_n(\vec{m}_{n-1})$
   - 应用该电路生成下一状态：$|\psi_n\rangle = U_n(\vec{m}_{n-1}) |\phi_{\text{seed}}\rangle$
3. 公开验证：任何方可通过以下方式验证链：

8. Daniel Gottesman and Isaac L. Chuang, "Quantum Digital Signatures," *arXiv preprint quant-ph/0105032*, 2001, https://arxiv.org/abs/quant-ph/0105032.

9. Nielsen and Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*.

10. Gottesman and Chuang, "Quantum Digital Signatures"; Shalev Ben-David and Or Sattath, "Quantum Tokens for Digital Signatures," *Quantum Information and Computation* 17, nos. 9-10 (2017): 811–831, https://doi.org/10.26421/QIC17.9-10.

- 从创世状态 $|\psi_0\rangle$ 开始
- 使用公布的测量结果顺序验证每个后续状态是否正确导出
- 检查每个状态是否通过抗碰撞量子哈希测试

4. 通胀控制：通过使测量和电路构造过程在计算上昂贵来控制发行速率。例如，可选择测量基使得找到产生有效下一状态（通过哈希测试）的结果需要解决计算困难问题，类似比特币中的工作量证明。

该方法具有多项优势：提供所有货币创造的不可变审计轨迹，通过强制顺序依赖防止任意铸造，并允许通过量子电路构造的难度调整实现算法化货币政策。然而，它需要在整个区块链上维持量子相干性，这对当前技术提出重大实践挑战。

3.4 混合方法与经济机制

现实的量子货币系统很可能结合多种抗通胀策略。例如，可实现双层系统：

1. 第一层（基础层）：使用状态空间限制对" 主要" 量子令牌总数施加硬上限。这些令牌存在于固定维度的码空间中，不能超过预定最大供给。
2. 第二层（交易层）：对促进日常交易的" 次要" 令牌实施计算难度调整。这些令牌可更自由地创建但需要工作量证明，且必须定期兑换或针对主要令牌验证以维持价值。

此外，传统货币政策中熟悉的经济机制也可适配：

- 量子令牌销毁：实现协议，允许通过以不可逆方式坍缩其叠加态的测量来故意销毁令牌，有效将其从流通中移除
- 基于权益的发行：限制铸币权给持有并锁定现有令牌的参与者，创造自然调节供给的经济激励结构
- 时间锁定释放：将新铸造的令牌编码为需要最少量子操作数（因而需要时间）才能验证和使用的量子态，防止突然的供给冲击

综合来看，即便在以物理为基础的货币系统中，经济稳定仍需要调节机制——无论是通过难度调节、状态空间限制、链式验证，还是混合经济机制。量子货币因此把物理层面的不可伪造性与算法化的治理灵活性结合在一起，有望为安全、抗通胀的价值交换提供全新范式。

4 结论

量子货币在货币与信任的基础上带来了深刻的概念转变。比特币与经典加密货币依赖计算假设与网络共识来维持稀缺与真实性，而量子货币则直接将这些属性扎根在自然规律中。对未知量子态不可克隆的事实从最根本的物理层面保证了不可伪造性。

本报告概述的技术方案——计算难度调整、量子状态空间限制、基于链的验证以及混合经济机制——展示了量子货币系统中的通胀控制可通过多种互补方法实现。每种策略利用量子力学的不同方面：量子问题的计算困难性、希尔伯特空间的维度约束、量子测量强制的顺序依赖性，以及量子态坍缩的不可逆性。

然而，在这种体系得以实现之前仍有大量障碍。可靠的量子存储、低噪声的量子通信信道以及可扩展的量子验证协议仍在研发之中。此外，如何在没有中央控制的情况下设计确保公平、稀缺并抵御操纵的货币政策仍是开放问题。特别是基于链的量子系统的实际实现需要在扩展时期和分布式网络中维持量子相干性——这一挑战推动了当前量子技术的边界。

本质上，比特币通过计算构建信任；量子货币则通过物理构建信任。如果未来的技术能够在大规模上存储、传输与操纵量子信息，量子闪电等系统可能会重塑数字金融以及稀缺性的概念。在那样的情景中，货币不仅是数学或经济学的产物，更是量子力学基本原理的具现——真正意义上的" 自然之币"。

References

Ben-David, Shalev, and Or Sattath. “Quantum Tokens for Digital Signatures.” *Quantum Information and Computation* 17, nos. 9-10 (2017): 811–831. https://doi.org/10.26421/QIC17.9-10.

Gottesman, Daniel, and Isaac L. Chuang. “Quantum Digital Signatures.” *arXiv preprint quant-ph/0105032*, 2001. https://arxiv.org/abs/quant-ph/0105032.

Grover, Lov K. “A Fast Quantum Mechanical Algorithm for Database Search.” *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, 212–219. https://doi.org/10.1145/237814.237866.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Bitcoin.org*, 2008. https://bitcoin.org/bitcoin.pdf.

Nielsen, Michael A., and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. https://doi.org/10.1017/CBO9780511976667.

Shor, Peter W. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.” *SIAM Journal on Computing* 26, no. 5 (1997): 1484–1509. https://doi.org/10.1137/S0097539795293172.

Wiesner, Stephen. “Conjugate Coding.” Original manuscript written circa 1970, *ACM SIGACT News* 15, no. 1 (1983): 78–88. https://doi.org/10.1145/1008908.1008920.

Zhandry, Mark. “Quantum Lightning Never Strikes the Same State Twice. Or Does It?” *Journal of Cryptology* 34, no. 4 (2021): 37. https://doi.org/10.1007/s00145-021-09405-0.