织格：
一种按设备摇号分配的抗量子点对点电子现金系统

Plekra

plekra.org

摘要

一个公平的电子现金系统，应当允许任何人在不预先持币、不消耗大量算力的情况下参与新币的分配。工作量证明把分配交给算力，权益证明把分配交给资本，二者都把参与者挡在门外。我们提出一种方案，将「分配」与「安全」分开处理：新币每 10 分钟以随机开奖的方式发放给一个参与者，手续费的一半平均分给未中奖的参与者；参与凭据以计算机内的实体安全芯片或持续占用的硬盘空间为代价，两类凭据各得一半分配，任何一类失守至多影响半数。账本由质押加权的拜占庭容错委员会在有向无环图上定序，作恶者的质押被罚没，攻击成本因此可以度量。开奖号码来自对预先固定的链上状态所做的串行哈希计算，能够影响输入的人来不及算出结果。账户不设单一主私钥，日常操作由限额内的设备密钥完成，恢复依靠用户口令与随机抽选的守护节点的门限验证。全部签名采用后量子算法。链上原生提供批量拍卖现货、全额备兑期权与按深度开放的永续合约，清算不依赖任何外部价格。

1 引言

比特币 [1] 证明了，互不信任的参与者可以在没有中心机构的情况下维护同一本账。它以算力决定记账权与新币归属：算力越多，分得越多。随着专用矿机的出现，记账权与新币事实上集中到拥有廉价电力与专用硬件的少数主体手中，普通计算机早已无法参与。权益证明消除了能耗，但通常按持币比例分配新币，后来者只能先购币、后参与。

除分配之外，现有系统还有三个结构性问题。其一，账户的全部控制权绑定于一把私钥，丢失即永久失去资产，泄露即被完全控制。其二，ECDSA 与 EdDSA 依赖的离散对数问题在容错量子计算机上可被 Shor 算法求解；NIST 已于 2024 年发布后量子签名与密钥封装标准 [2]，并规定量子脆弱的公钥算法在 2030 年后弃用、2035 年后禁用 [3]。其三，衍生品交易依赖中心化交易所托管资产，而链上交易又面临抢先交易与夹击 [4]。

本文提出的系统以如下思路回应这些问题：

- **分配与安全分离。** 新币按参与凭据随机分配，与持币量、算力和在线时长无关；账本安全由质押承担，作恶者被罚没。
- **以物理资源为参与代价。** 在没有身份机构的开放网络中，创建身份若无代价，一个人便可伪装成任意多人 [5]。我们以实体安全芯片与硬盘空间作为代价，二者的弱点互补。

- **规则账户**。 账户由一组授权规则而非一把私钥定义，任何单一密钥的泄露都不足以转移全部资产。
- **原生金融**。 现货、期权与永续合约在链上撮合与结算，与资产账本在同一批次内原子完成。

2 区块网

交易由一个委员会定序。委员会成员在每一轮各自提出一个区块，区块引用上一轮中累计投票权超过 2/3 的区块；引用本身即构成投票，无需额外的认证消息。由此形成的结构是一张有向无环图（图 1），我们称之为区块网。提交规则是确定性的：全体诚实成员从同一张图导出同一个交易全序。该构造取自 Mysticeti [6]，后者在由上百个验证者组成的生产网络中实现了亚秒级提交。

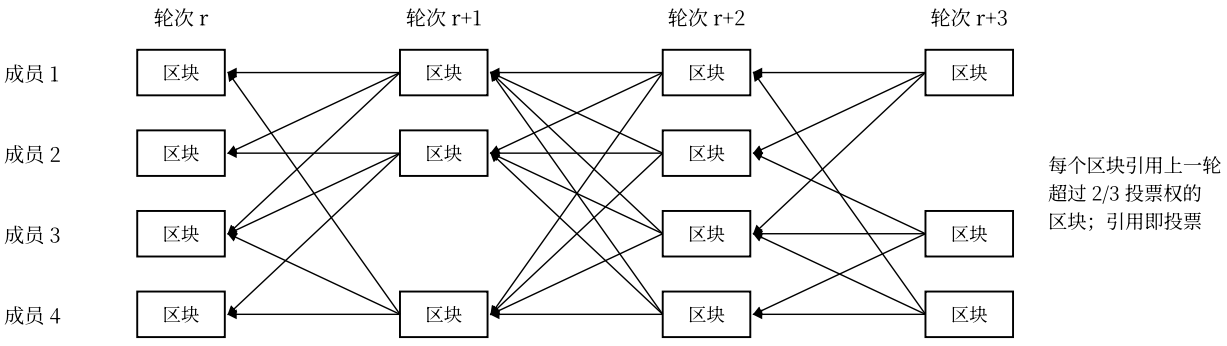


图 1　区块网。成员在每一轮并行出块，不需要排队等待同一个出块者。

区块与投票以 ML-DSA-44 [2] 签名。任何决定须获得超过委员会总投票权 2/3 的签名。在部分同步网络 [7] 与敌手投票权低于 1/3 的假设下，协议同时满足安全性与活性。交易所在的区块一经提交，其顺序即不可更改，稳态下普通转账的确认目标为 0.5 至 1 秒。

3 双车道账本

全序交易由两条执行车道处理：A 车道负责资产与分配，包括余额、账户、参与凭据、开奖、分红、质押与治理；B 车道负责金融与合约，包括现货、期权、杠杆、永续合约与第三方 WebAssembly 合约。

每 1.5 至 2 秒为一个批次。每个批次由确定性的执行规则产生一对状态根 $(\mathrm{StateRoot}_A, \mathrm{StateRoot}_B)$，随后续区块一同确认。B 车道中涉及资金划转的操作，即成交、行权、强制平仓，与其在 A 车道的对应划转属于同一原子事务，任一步骤失败则两条车道同时回滚。两条车道共享同一共识骨架，跨车道操作不需要跨链桥，其安全性不依赖额外假设（图 2）。

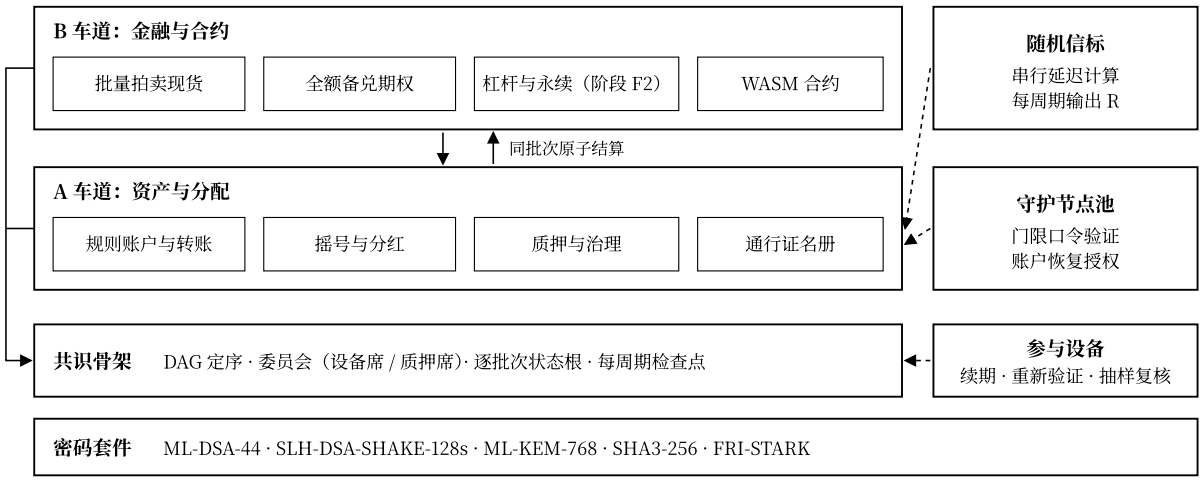


图 2　双车道账本。实线箭头表示状态依赖，虚线箭头表示向账本提交的输入。

每个批次的执行容量分为三类，分别是系统操作、原生金融与第三方合约，各自拥有独立的费用市场。第三方合约造成的拥堵只抬高其自身类别的费率，不影响转账与强制平仓的执行。

4 参与凭据

参与开奖与分红的凭据称为通行证，分为两轨。

芯片轨。 计算机内的可信平台模块（TPM 2.0）在出厂时由厂商写入背书密钥证书。设备在本地生成秘密 ς，并派生

$$c = H(\varsigma \,\|\, 0), \qquad \mathrm{tag} = H(\varsigma \,\|\, 1)$$

设备以证书、芯片内生成的证明密钥与承诺 c 登记芯片，由随机指派的委员会成员质询芯片后见证。芯片去重标识为背书公钥的哈希，同一芯片只能登记一次。领取通行证时，设备提交 tag 与一份零知识证明，表明自己知道某个已登记芯片的 ς，并持有该芯片对最新随机数的签名，但不透露是哪一枚芯片。链上拒绝重复的 tag。芯片的登记是公开的，芯片与通行证之间的对应关系则不公开。通行证每 30 天须重新出示一次芯片签名。

芯片轨只接受实体芯片。云服务商为虚拟机提供的虚拟 TPM，其证书可以按需签发，且关机后几乎不产生费用，因此不予接受。为限制单一厂商密钥泄露的影响，每张签发证书名下的有效份额设有上限 θ。

硬盘轨。 持有者以通行证公钥的哈希 PassID 为种子，按空间证明的构造 [8][9] 生成一份大小为 256 GiB 的数据。给定挑战，持有者只需从数据中查找即可在数秒内作答；未存储数据者须重做大部分生成计算。续期时，持有者提交一笔带签名的请求，请求入块所在的批次 b 决定挑战

$$ch_j = H\big(\mathrm{StateRoot}_A(\mathsf{b}+1) \,\|\, \mathrm{PassID} \,\|\, j\big), \qquad j = 1, \ldots, 4$$

响应须在约 30 秒内入块。硬盘轨只依赖哈希函数，不依赖任何厂商，也不受量子计算影响。

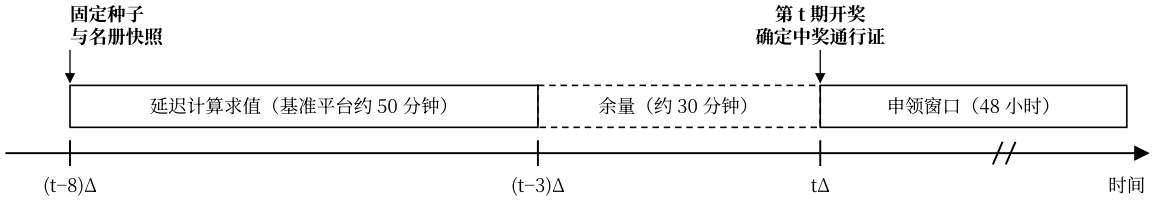
两轨的互补。芯片轨使一台普通计算机取得与规模化运营者同等的单位份额，因为每增加一份就须增加一台实体机器，但它依赖芯片厂商的出厂签名。硬盘轨不依赖任何商业主体，但存储有规模经济，有利于大型运营者。开奖期数在两轨之间轮替，分红池两轨各半，这一比例不可由治理更改。厂商密钥泄露只影响芯片轨，存储的集中只影响硬盘轨，任何一方失守至多波及分配总量的一半。硬盘通行证容易被单一运营者堆积，因此不进入委员会，也不参与治理表决。

5 随机信标

开奖要求任何能够影响输入的人都无法预知结果。令 b_t 为共识时间早于第 t 期开奖 8 个周期的最后一个批次，种子与开奖号码为

$$\mathrm{Seed}_t = H\big(t \,\|\, \mathrm{StateRoot}_A(\mathsf{b}_t) \,\|\, \mathrm{StateRoot}_B(\mathsf{b}_t)\big), \qquad R_t = H^{(n)}(\mathrm{Seed}_t)$$

其中 H 为 SHA3-256，n 的取值使基准平台上的串行计算约需 50 分钟。参与者名册与种子同时固定（图 3）。能够影响种子的最后一个委员会成员只有数秒的决策时间；若要有方向地选择区块内容，它须在这段时间内完成一次求值，所需的顺序加速比在 300 倍以上。哈希链没有已知的并行加速方法，我们假设敌手的顺序加速比不超过 100 倍。基于未知阶群的可验证延迟函数 [10] 具有简短证明，但依赖在量子计算下不成立的假设，故不采用；哈希链的正确性由委员会成员分段重算验证。



Δ = 600 秒；种子与名册在求值开始前即已固定。分段重算与求值并行进行，求值期间不接受任何输入。

图 3　随机信标的时间线（申领窗口未按比例绘制）。

6 开奖与分红

偶数期从芯片轨开奖，奇数期从硬盘轨开奖。名册按 PassID 排序存放，由 R_t 派生 $u_1 = H(R_t \,\|\, 0)$ 与 $u_2 = H(R_t \,\|\, 1)$。硬盘轨的中奖者为名册中第 $\lfloor u_1 N / 2^{256} \rfloor$ 个通行证。芯片轨先以 u_1 按有效数量 $\tilde{n}_g$ 加权选出一张签发证书 g，再以 u_2 在其名下的 n_g 个通行证中均匀选出一个。通行证中奖的概率因此为

$$\Pr[\,i \text{ 中奖}\,] = \frac{\tilde{n}_g}{\tilde{N}} \cdot \frac{1}{n_g}$$

各签发证书均未触及份额上限时，它就是 $1/N$。整个过程只需一次加权选择与一次按序号的检索，不需要遍历名册。

中奖者须在 48 小时内以通行证密钥申领，奖励一半即时到账，另一半在此后 30 天内逐日解锁。中奖者在至多 90 天的冷却期内不参与分红。

手续费的 50% 进入分红池，两轨各半。每个纪元（24 小时）释放池余额的 1/7，在该轨未处于冷却期的通行证之间等额分配：

$$f_e = \frac{P_e/7}{\sum_{i \in \mathcal{A}_e} w_i}$$

其中 P_e 为该轨分红池余额，$\mathcal{A}_e$ 为在册且不在冷却期的通行证，w_i 为签发证书份额上限所决定的权重，未触及上限时为 1。分红与在线时长无关，自动记账，不需要任何申领交易。

7 激励

发行。 PLK 的总量上限为 10^9 枚，创世时为零，没有任何预分配。发行按档进行：

$$E_j = 10^8 \times 0.9^{\,j-1}, \qquad \rho_j = 2000 \times 0.9^{\,j-1}, \qquad \sum_{j=1}^{\infty} E_j = 10^9$$

其中 E_j 为第 j 档的额度，ρ_j 为满额单次奖励。每档包含 5 万次开奖，约 347 天；档末累计发行在第 1 档为 10%，第 7 档为 52%，第 22 档为 90%。某一轨参与者较少时，单次奖励按 $\rho_j \cdot \min(1,\ \tilde{N}/10^5)$ 缩小，早期少数参与者无法在短时间内取得不成比例的份额。

手续费。 手续费不销毁：50% 进入分红池，20% 归委员会，5% 归守护节点，20% 进入本金不可提取的协议储备，5% 进入经投票支出的公共金库。一个主体即使控制全部通行证与全部质押，通过自成交支付的手续费也至多收回 75%，自成交因而无利可图。

安全补贴。 早期手续费不足以吸引足够的质押。每期开奖奖励中的比例

$$s_e = \min\!\Big(15\%,\ \frac{\max\!\big(0,\ B_e - \tfrac{1}{2}F_{e-1}\big)}{I_{e-1}}\Big), \qquad B_e = \frac{5\%}{365} \cdot \frac{2}{3} \cdot Q_e$$

计入质押者，其中 Q_e 为已发行量，F_{e-1} 与 I_{e-1} 分别为上一纪元质押者所得的手续费与开奖奖励总额。它将质押者的收入补足到「三分之二的代币质押时年化 5%」的水平；手续费按一半抵扣，达到目标的两倍时补贴归零。已发行 10^8 枚时，补贴约为当年发行量的 3%。

8 共识安全

任何地址均可质押 PLK 成为候选节点，其他持币者可委托质押。计票质押位列前 128 的节点组成委员会，投票权与计票质押成正比。在同一纪元内重复签名的节点被罚没，比例为

$$\max\big(5\%,\ \min(100\%,\ 3\varphi)\big)$$

其中 φ 为重复签名的投票权占比。$\varphi < 1/10$ 时视为个别故障，只罚节点自有质押；造成分叉须 $\varphi \geq 1/3$，届时自有与委托质押全额罚没。重复签名可由任何人凭两份签名举证，破坏安全性的代价因此不低于委员会计票质押总额的约三分之一。

创世时无币可押，网络因此分三个阶段过渡。引导期由芯片轨的设备节点组成至多 256 席的委员会；发行满 10^7 枚且质押达到已发行量的 25% 后进入混合期，任何决定须同时获得设备席与质押

席各自超过 2/3 的签名，只要二者之一诚实，账本即不分叉；发行满 10^8 枚且计票质押连续 180 天不低于已发行量的 2/3 后，经双重表决进入质押稳态。质押大幅回落时，网络自动退回混合期。

9 账户

账户由一组授权规则定义，承认三类相互独立的授权因素：设备（芯片内保存的限额会话密钥）、口令（经守护集群验证）与冷密钥（离线保存的 SLH-DSA 密钥）。限额内转账只需设备；超出限额的转出与规则修改须任意两类因素，并经过 24 至 72 小时的等待期。等待期内的操作可被出示不少于同等类数因素的一方撤销。所有者只要比敌手多掌握一类因素，即可撤销敌手的一切操作；单独泄露一台设备，损失以限额为界。

失去全部设备的用户，凭恢复名与口令向守护集群申请恢复。集群由 41 个以随机信标抽选的守护节点组成，每 90 天整体重抽。客户端将口令验证密钥 v 以门限为 21 的 Shamir 方案 [11] 分享给集群成员，任意 20 个成员的份额不泄露关于 v 的任何信息。验证时，集群以诚实多数下的可验证多方计算 [12][13] 公开 $r(v - v')$，其中 r 为任何成员都不知晓的随机数：结果为零当且仅当口令正确，否则为不携带信息的随机值。每次尝试须缴纳押金，失败则押金翻倍并归账户所有者，离线穷举因此不可行。验证通过后，至少 21 个成员签署授权，链上核对尝试记录、恢复记录承诺与集群成员身份，新设备在 72 小时等待期后生效。

10 原生金融

现货。 现货采用频繁批量拍卖 [14]：每个批次内的订单以单一清算价统一成交，订单之间不分先后，抢先交易因此失去对象。订单在清算前以承诺提交，随后揭示。

期权。 卖方须在卖出前全额锁定履约资产，买方可在到期前随时行权，交割在同一批次内原子完成，不存在违约。

杠杆与永续合约。 永续合约杠杆上限为 20 倍，现货杠杆上限为 3 倍，按交易对的订单簿深度逐个开放。可在价格变动 δ_L 内被强制平仓的未平仓总量，不超过同一区间内稳健深度与当前深度中较小者的四分之一；稳健深度取过去 30 天挂单量的第 10 百分位数。强平价格取链上现货清算价的 5 分钟时间加权均价，逐批次限幅。永续合约与借贷各设隔离的保险金库，永续合约的穿仓由保险金库与自动减仓消化，不动用协议储备。所有清算只使用链上价格，不依赖外部预言机。

11 计算

设备委员会。 引导期的委员会有 256 席，设任一席位由敌手控制的概率为 p，失守须敌手占据至少 86 席：

$$\Pr(X \ge 86) = \sum_{x=86}^{256} \binom{256}{x} p^{x} (1-p)^{256-x}$$

p	10%	15%	20%	25%
单个纪元	1.0×10^{-24}	1.0×10^{-13}	2.4×10^{-7}	1.3×10^{-3}
一年（365 纪元）	3.8×10^{-22}	3.8×10^{-11}	8.9×10^{-5}	37%

结果对 p 十分敏感，引导期因此是全生命周期中最弱的阶段，须尽快过渡到质押委员会。

部分存储。 只存储比例为 s 的硬盘数据者，每次续期通过 4 个挑战的概率为 s^4；续期有效期覆盖两个窗口，其处于名册之内的时间比例约为 $1-(1-s^4)^2$：

s	50%	80%	90%	95%
处于名册之内的比例	12%	65%	88%	97%
相对足额存储的单位成本收益	0.24	0.81	0.98	1.02

少存数据得不偿失，接近足额时的优势不超过约 2%。

开奖收益。 某一轨第 1 档、N 个活跃通行证时，单个通行证的期望收益为：

N	单次奖励	日期望收益	平均中奖间隔	一年内至少中奖一次
10^4	200	1.44	139 天	92.8%
10^5	2,000	1.44	3.8 年	23.1%
10^6	2,000	0.144	38 年	2.6%

规模增大后，开奖收益的方差迅速变大，分红为未中奖者提供低方差的持续收益。

守护集群。 设敌手在守护节点池中的占比为 q，单个集群中敌手不少于 21 名的概率在 $q=10\%$ 时为 3.6×10^{-11}，在 $q=20\%$ 时为 8.4×10^{-6}。即使集群被攻破，敌手发起的恢复仍须经过 72 小时等待期，并可被所有者以其余因素撤销。

12 结论

我们提出了一个不依赖挖矿与预先持币的电子现金系统。新币以随机开奖的方式分配给参与者，参与的代价是实体芯片或硬盘空间；两轨各得一半，任何一类代价的失守都不能夺走全部分配。账本安全由可罚没的质押提供，并经由设备委员会、混合委员会到质押委员会的三阶段过渡建立起来。开奖号码来自预先固定输入的串行哈希计算，账户不存在单一主私钥，全部签名采用后量子算法，金融交易与资产结算在同一批次内原子完成。

这一设计有其边界。分配的单位是设备而非自然人，控制更多设备者取得更多份额；芯片轨依赖芯片厂商的出厂签名；硬盘轨可能向大型存储运营者集中，并由此影响质押的分布；引导期的安全弱于质押稳态；不依赖外部价格的杠杆市场在剧烈行情中可能出现穿仓。这些取舍及其完整分析，连同全部参数，载于《织格技术规范》。

参考文献

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
2. NIST, *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard*; *FIPS 204: Module-Lattice-Based Digital Signature Standard*; *FIPS 205: Stateless Hash-Based Digital Signature Standard*, Aug. 2024.
3. NIST, "Transition to Post-Quantum Cryptography Standards," *NIST IR 8547*, Oct. 2026.
4. P. Daian et al., "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability," in *Proc. IEEE S&P*, 2020.
5. J. R. Douceur, "The Sybil Attack," in *Proc. IPTPS*, 2002.
6. K. Babel et al., "Mysticeti: Reaching the Latency Limits with Uncertified DAGs," in *Proc. NDSS*, 2025.
7. C. Dwork, N. Lynch, and L. Stockmeyer, "Consensus in the Presence of Partial Synchrony," *Journal of the ACM*, vol. 35, no. 2, 1988.
8. S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of Space," in *Proc. CRYPTO*, 2015.
9. H. Abusalah, J. Alwen, B. Cohen, D. Khilko, K. Pietrzak, and L. Reyzin, "Beyond Hellman's Time-Memory Trade-Offs with Applications to Proofs of Space," in *Proc. ASIACRYPT*, 2017.
10. D. Boneh, J. Bonneau, B. Bünz, and B. Fisch, "Verifiable Delay Functions," in *Proc. CRYPTO*, 2018.
11. A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, 1979.
12. T. Rabin and M. Ben-Or, "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority," in *Proc. STOC*, 1989.
13. E. Ben-Sasson, S. Fehr, and R. Ostrovsky, "Near-Linear Unconditionally-Secure Multiparty Computation with a Dishonest Minority," in *Proc. CRYPTO*, 2012.
14. E. Budish, P. Cramton, and J. Shim, "The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response," *Quarterly Journal of Economics*, vol. 130, no. 4, 2015.