Cosmic Signature

Arbitrum 上的程序化链上艺术协议

Taras Bobrovytsky taras@cosmicsignature.com

版本 1.0 · 2026 年 8 月

摘要

Cosmic Signature 是部署在 Arbitrum One 上的程序化艺术协议，以一个个限时的演绎周期运转。周期进行中，参与者以 ETH 或协议的 ERC-20 代币 CST 落笔：每一笔都会延长收官倒计时，计入一次星选资格，还可能铭刻新的 CST。倒计时结束、周期收官后，协议将 ETH 储备分配至十余条轨道，铭刻新一代 Cosmic Signature NFT，并把固定份额转拨给 Protocol Guild，即 170 余位以太坊核心贡献者的资助机制。约一半储备滚入下一周期，储备规模还取决于各周期新加入的 ETH。

每枚 Cosmic Signature NFT 都是对引力三体问题的确定性渲染：作品由链上种子生成，任何人都能逐像素复现，全程没有神经网络参与。本文完整阐述协议机制与代币设计，记录已上线的 V2 升级，介绍规划中的 V3 升级，并阐明一项承诺：待设计定稿，部署者地址将交出全部特权控制。

目录

1. 引言

Cosmic Signature 源于两个信念。其一，生成艺术最动人的时刻，是它没有任何随意性：每幅图像都是物理过程的输出，由种子唯一确定，任何人重跑一遍流程即可验证结果。其二，一个替参与者保管 ETH 的协议，应当对"每一个 wei 去了哪里"给出机械的、可读的答案。

由此而来的，是一个围绕时间构建的协议。演绎周期开启，在一次次落笔中延展，倒计时归零后落幕。落笔是一次小小的链上行为：携带 ETH 或 CST，可附上一句短消息或一份资产，并把周期的

收官时间向后推。倒计时结束时，最后落下的那一笔就是收官之笔，其参与者可完成收官：发放储备、铭刻本周期的 NFT，并为下一周期做好准备。

三项性质贯穿整个设计。

- 确定性。作品由铭刻时记录在链上的种子计算而来。渲染管线开源，同一种子永远产出同一图像与视频，逐比特一致。
- 机械化发放。分配由已验证合约按链上规则执行。参与者与发放规则之间没有任何自由裁量的账户，也没有团队钱包从落笔中收取 ETH。
- 有限的团队角色。所有者权限范围有限，核心参数在周期运行期间锁定，并将在剩余升级完成后彻底移除。

本文是协议的权威说明。第 2 节勾勒系统全貌；第 3 至 5 节定义周期、落笔与分配；第 6 节介绍艺术；第 7 至 10 节涵盖 CST、锚定、宇宙议会与公共物品；第 11 节讨论安全与可验证性；第 12、13 节记录升级历史与全面去中心化路线；第 14 节直言协议不是什么。文中引用的数字要么是合约常量，要么是链上参数的上线初始值；附录 A 所列的已部署合约始终是最终依据。

2. 协议概览

系统由一份核心合约和环绕它的一组单一职责合约构成。核心合约部署在可升级代理之后，负责运转周期：为落笔定价、维护倒计时、持有周期储备、执行收官。环绕它的是 CST 代币、Cosmic Signature NFT 系列、分配托管钱包、两个锚定钱包、公共物品金库、推广储备与宇宙议会。

组件	职责
协议合约	运转演绎周期：落笔定价、收官倒计时、周期储备与收官执行。
CST（ERC-20）	参与代币。仅由协议铭刻，用于落笔时销毁，完成委托后表达协调权重。
Cosmic Signature NFT (ERC-721)	确定性三体艺术作品。仅在收官时铭刻，种子存储在链上。
Random Walk NFT	同一团队更早的生成艺术系列。可一次性降低落笔价格，并拥有独立的锚定星选轨道。
分配钱包	托管次级 ETH 分配与随落笔附加的资产，设有公开取回期限。
锚定钱包	一个面向 Cosmic Signature NFT（ETH 锚定派发），一个面向 Random Walk NFT（星选资格）。
公共物品金库	接收并转拨每周期的公共物品分配，受益方目前为 Protocol Guild。
推广储备	每周期接收 3,000 CST，用于社区推广。
宇宙议会	链上协调机构，完成委托的 CST 在其中表达协调权重。

合约之外，一个生态正在生长：应用位于 app.cosmicsignature.com，NFT 在 Axiom Zero 市场流通，CST 在 Arbitrum 上有 Uniswap 流动性，Chaos Zero 则为每个周期提供预测场所。它们都不是必需的：本文所述的每项机制，都可以直接调用合约完成。

3. 演绎周期

周期是一段时间之窗：以价格递减的校准窗口开启，在落笔中延展，倒计时结束并有人收官后落幕。本节讲清这座时钟；落笔本身见第 4 节。

3.1 开场与 ETH 校准窗口

每个周期的首笔落笔必须使用 ETH，其价格由 ETH 校准窗口决定。窗口起始价为上一周期开场实付价格的 2 倍，随后线性下行，直至起始价的两百分之一加 1 wei。按上线参数，整段下行约需两天；时长与周期时间增量挂钩，会随协议年岁缓慢拉长。若窗口走完仍无人落笔，价格便停在底价等待。第一个周期以固定的 0.0001 ETH 开场。

这套开场机制不依赖订单簿：上一周期若开得太便宜，翻倍会先恢复上行空间；翻倍后若显得偏高，两天的缓慢下行总会停在有人愿意开场的位置。

3.2 收官倒计时

首笔落笔启动时钟，按上线参数将周期收官时间设在约 24 小时之后。此后每笔 ETH 或 CST 落笔，都会把当前时间增量加到链上收官时间上。增量上线时恰为 1 小时，并在每个周期收官后增长 1%，周期因此逐渐变长，NFT 的铭刻节奏也随岁月放缓。只要落笔不断，周期长度没有硬性上限；但落笔价格持续上行，无限延长在实践中代价高昂。

延长作用于链上存储的收官时间，而非当下时刻。倒计时已过、收官尚未执行时，落笔依然有效：它把存储值再推一个增量，并接任收官之笔，但不会让时钟从头再来。

3.3 收官与公开收官窗口

周期收官时间一到，收官之笔参与者即可收官。收官是一笔交易：读取协议的 ETH 余额，按第 5 节的轨道发放，铭刻本周期的 NFT 与 CST，为每件新作品记录种子，并排定下一周期。

这项权利在 48 小时内专属于收官之笔参与者。窗口过后进入公开收官：任何人都可收官，合约会把实际收官者视为周期受益方，该角色的一切随之归属，包括签名分配的 ETH 份额、CST 铭刻、NFT，以及对已附加资产的优先权。这项期限让协议能够继续运作：受益方若未在专属窗口内收官，其他人即可接手并获得该角色对应的分配。

收官之后，下一周期经过一段短暂延迟启用（默认 30 分钟），校准窗口随之开启。

4. 落笔

落笔推动演绎周期。无论使用哪种货币，每一笔都会延长倒计时、在参与者星选池中计入一次资格、更新第 5.2 节的坚守时钟，还可能按第 7.1 节铭刻参与 CST。

4.1 ETH 落笔

开场之后，每笔 ETH 落笔都会把下一笔的 ETH 落笔价格抬高 1%，再加 1 wei。这条序列公开而精确，落笔前随时可以从合约读到当前价格。超付的金额会在同一笔交易中退回；只有当退款连 gas 都不够抵时，差额才留在储备中。

4.2 附加 Random Walk NFT

持有 Random Walk NFT 的参与者，可将其附加到一笔 ETH 落笔上，使该笔价格降低 50%。NFT 不会转移，合约只是将其标记为已使用。每枚 Random Walk NFT 在所有周期中仅可附加一次：降价因此成了一种消耗品，一个数量固定的外部系列也由此融入协议经济。

4.3 CST 落笔

CST 提供第二条入口。CST 校准窗口的起始价为上一笔 CST 实付价格的 2 倍，且不低于 200 CST，随后在窗口时长内线性降至零。每笔 CST 落笔都会以新的起始价重启窗口，所付 CST 全数销毁，永久移出供应量。

窗口时长本身也是链上的活参数，是协议里一条安静的反馈回路。它从 12 小时的基准出发：每笔 ETH 落笔使其缩短约 0.398%，每笔 CST 落笔使其延长约 0.4%。ETH 落笔越密集，CST 价格降得越快，CST 落笔越早变得划算；CST 落笔多了，下行又会放慢。这条回路把每个周期推向两种货币的均衡组合。

价格既然能降到零，足够长的沉寂就能让一笔 CST 落笔近乎免费。这是有意为之：只要有人持有哪怕一点 CST，周期就总能延续；而每笔 CST 落笔的销毁，又把代币供应量与真实使用绑在一起。提交 CST 落笔时需指定可接受的最高价格，交易落地晚于预期也不会多花一分。

每个周期的首笔落笔必须使用 ETH；从第二笔起即可使用 CST。

4.4 消息与附加资产

落笔可携带最长 280 字节的消息，与落笔一同记录在链上；也可附加 ERC-20 代币或一枚 ERC-721 NFT。附加资产不进入 ETH 储备，而由分配钱包托管；周期收官后，受益方享有优先取回权，并受第 5.4 节的公开取回期限约束。

5. 周期储备与分配轨道

所有落笔支付的 ETH 都汇入协议合约，连同上一周期约一半的储备，共同构成周期储备。收官时读取一次余额，按固定比例发放。

5.1 收官时的发放

ETH 轨道	占周期储备份额	获配者
签名分配	25%	周期受益方，通常为收官之笔参与者。
时之勇士分配	8%	在位最久的坚守冠军（见第 5.2 节）。
公共物品分配	7%	Protocol Guild，经公共物品金库转拨。
锚定派发	6%	已锚定的 Cosmic Signature NFT，按比例分摊。
ETH 星选	4%	从本周期落笔资格池中选出 3 次，均分该份额。
滚动储备	约 50%（其余部分）	滚入下一周期。

各比例均按收官那一刻协议的 *ETH* 余额计算。

五条发放轨道合计正好一半，其余滚动累积：协议滚动累积，而非抽取，下一周期的起始储备来自这笔留存，其规模不保证逐周期增长。若收官时没有任何已锚定的 Cosmic Signature NFT，该周期的锚定派发将跳过，这部分份额同样滚入下一周期。

CST 与 NFT 轨道	发放内容	获配者
签名分配	1,000 CST 与 1 枚 NFT	周期受益方。
时之勇士	1,000 CST 与 1 枚 NFT	时之勇士。
坚守冠军	1,000 CST 与 1 枚 NFT	坚守冠军。

CST 与 NFT 轨道	发放内容	获配者
CST 收官之笔	1,000 CST 与 1 枚 NFT	本周期最后一笔 CST 落笔的参与者。
参与者 NFT 星选	1,000 CST 与 1 枚 NFT，共 10 次	从落笔资格池中选出。
锚定 NFT 星选	1,000 CST 与 1 枚 NFT，共 10 次	在已锚定的 Random Walk NFT 中选出。
推广储备	3,000 CST	社区推广（见第 7.1 节）。

因此，典型周期共铭刻 24 枚 Cosmic Signature NFT，外加 27,000 CST 的固定发放；各笔落笔沿途铭刻的参与 CST 另计。没有 CST 落笔的周期跳过 CST 收官之笔轨道；没有已锚定 Random Walk NFT 的周期跳过锚定星选。

5.2 坚守冠军与时之勇士

有两条轨道衡量的是坚持，而非位置。坚守冠军，是本周期内以最近落笔者身份坚守最久的参与者，也就是单笔落笔撑过的最长静默间隔。时之勇士再上一层：谁连续在位坚守冠军的时间最长，谁就是时之勇士。

两者的差别细微而真实。慵懒的午后落下一笔、十个小时无人打破，就立下了一段漂亮的坚守间隔；但能否以时之勇士的身份走完周期，取决于这项纪录在他人刷新之前又存续了多久。坚守衡量你创造的间隔，时之勇士衡量纪录存活的时长。两者都要到收官那一刻才尘埃落定。

5.3 星选

每笔落笔都在本周期的参与者星选池中计入一次资格。收官时，合约为 ETH 星选选出 3 次资格，均分储备的 4%；再为 NFT 星选选出 10 次。选择采用放回方式，同一参与者可能被选中多次；资格随落笔累积，入选频次与参与程度成正比。

另有一条独立的锚定 NFT 星选，在已锚定的 Random Walk NFT 中选出 10 次，权重按各锚定者锚定的 NFT 数量计。这条轨道只发放 CST 与 Cosmic Signature NFT，不含 ETH。

这些选择背后的随机性在收官时于链上构造，其来源与边界见第 11.3 节。

5.4 发放、托管与期限

发放刻意分成两类：主动送达与自行取回。签名分配的 ETH 在收官时直接送达受益方，公共物品转拨亦然；时之勇士的 ETH 与三份 ETH 星选份额则存入分配钱包托管，获配者随时取回。CST 与 NFT 在收官时直接铭刻到各自获配者名下。

托管中的分配与附加资产会等待 5 周。期限一过，合约允许任何人为自己取回仍未取回的分配。这条规则与公开收官窗口一脉相承：协议不为缺席者无限期停留，每份发放终会到达想要它的人手中。请及时取回。

6. 艺术：确定性的三体签名

每枚 Cosmic Signature NFT 都是对引力三体问题的一次渲染：三个质量相近的天体在牛顿引力下互绕。三体问题没有一般解析解，轨迹天然混沌，初始条件的毫厘之差会演成完全不同的舞步。这种混沌正是整个系列的引擎：种子决定初始条件，物理完成其余一切，没有两幅签名会重样。

任何阶段都没有生成式模型参与。没有训练数据，没有采样，也没有提示词。管线就是一段物理模拟加一个渲染器，以 Rust 写成，完全开源，彻底确定。

6.1 渲染管线

- 种子。铭刻时，合约从链上数据导出 32 字节种子（见第 11.3 节），并与 NFT 一同存储。种子初始化一个 SHA3-256 随机数生成器，此后的一切都是它的纯函数。
- 模拟。十万组候选构型分别通过四阶 Yoshida 辛积分器演算，每组推进 1,000,000 个物理步；这种积分器能在长时间尺度上保持系统的能量行为。
- 遴选。Borda 排序聚合按混沌程度与三角形的等边程度为候选打分，选出视觉上最有意味的一条轨道。
- 镜头。缓慢的椭圆镜头漂移穿行于轨道之间，赋予每幅签名电影般的视差。
- 色彩。色彩在 OKLab 感知色彩空间中混合，各天体色相相隔 120°，并由漂移与正弦波调制。
- 光谱渲染。从 380 至 700 纳米划分 64 个波长区间，以随速度变化的线宽和景深渲染轨迹。
- 收尾。AgX 色调映射、辉光、OpenSimplex 星云层与色彩分级共同完成画面。

每枚 NFT 的最终输出，是一张 16 位 PNG 与一段 30 秒 H.265 视频。

6.2 可复现性与许可

确定性靠机制保证，而非口头承诺。同一种子在任何机器上都产出逐像素一致的图像，生成帧的 SHA-256 哈希在持续集成中逐一断言。种子全部在链上，管线完全公开，这个系列因此不依赖任何服务器：哪怕明天所有服务器都消失，每幅签名都能从链上重生。

所有者可在链上为 NFT 命名，最长 32 字节。项目自有的合约、着色器与渲染管线均以 CC0 1.0 献入公有领域，不保留任何权利；第三方依赖保留各自的许可。

7. CST 代币

CST 是协议的 ERC-20 代币。供应量从零起步，代币合约只接受协议合约的铭刻与销毁指令。流通中的每一枚 CST，都能追溯到某个周期里的一次参与。

7.1 铭刻规则

CST 经三条途径进入流通。参与 CST 在落笔时按下方公式铭刻。表彰 CST 在收官时铭刻：本周期每份 NFT 发放都伴随 1,000 CST，典型周期共 24 份。此外，每周期还有 3,000 CST 进入推广储备，由团队用于社区推广；这是团队经手的唯一一条固定 CST 流，且不附带任何特殊权限。

```
floor(sqrt(elapsedSinceLastGesture * bidCstRewardAmountMultiplier
    / mainPrizeTimeIncrementInMicroSeconds))
```

一笔落笔铭刻的参与 *CST*。经过时间自上一笔起算，并按当前周期时间增量归一化。

直白地说，数量随距上一笔时间的平方根增长。上一笔落下一秒后就跟进，几乎什么也铭刻不到；终结一整天沉默的一笔，能铭刻数百 CST。

距上一笔的时间	参与 CST
0 秒	0
1 秒	1.73
60 秒	13.4
1 小时	104
1 天	509

按上线时恰为 *1* 小时的时间增量计算。增量逐周期增长后，实际数额会略低于表中值；实时预览与合约本身才是最终依据。

7.2 销毁与供应动态

CST 一经使用即离开流通：每笔 CST 落笔支付的全部价格都会销毁。供应量因此由行为塑造：沉寂的周期铭刻的参与 CST 不多，活跃的 CST 使用又把供应量烧回去，固定的表彰与推广两条流则为每个典型周期稳定注入 27,000 CST。没有硬性供应上限，也没有上线预留份额；推广储备则按上述规则逐周期铭刻。

平方根公式本身就是一道供应闸门，由 V2 升级引入（见第 12.2 节）。最初的设计是每笔固定铭刻 100 CST，机器速度的连续落笔由此成了源源不断的新 CST 来源。改用现行规则后，一串急促的落笔几乎什么都铭刻不到；创造供应的，是耐心的参与。

7.3 协调权重

CST 同时是宇宙议会（第 9 节）的权重代币。权重在委托后生效：持有者把权重委托给自己或其他地址，此后每枚 CST 表达一个单位的协调权重。代币采用基于时间戳的检查点，提案快照对应的是钟表时间，而非区块高度。

8. 锚定

锚定是协议的长期对齐方式。所有者可将 Cosmic Signature NFT 锚定至协议；锚定期间，它按比例累积每周期 6% 的锚定派发，累积的 ETH 在解锚时取回。锚定没有固定期限，也没有任何罚则，但它是每枚 NFT 一次性的决定：每枚 NFT 一生仅可锚定一次，解锚即永久失去锚定资格。

锚定没有固定锁定期，持有者可以自行决定何时解锚。不过，解锚会永久用尽这枚 NFT 的锚定资格，因此每次决定都需要同时考虑当前派发与今后的参与方式。

Random Walk NFT 的锚定自成一线，目的也不同：已锚定的 Random Walk NFT 参与锚定 NFT 星选（见第 5.3 节），每周期 10 次，每次携带 1,000 CST 与一枚 Cosmic Signature NFT。Random Walk 锚定不含 ETH 派发。一生一次的规则同样适用。

9. 宇宙议会

宇宙议会是协议的链上协调机构，基于经过审计的 OpenZeppelin Governor 框架构建，以 CST 为权重代币。任何持有至少 100 CST 委托权重的地址都可提交协调提案。提案先经过 2 天协调延迟，再进入 2 周的协调期。

提案通过需同时满足两个条件：支持权重高于反对权重，且支持与弃权权重之和达到 CST 总供应量 3% 的协调法定权重。反对权重不计入法定权重。表达权重是一次密码学行为，不是股份或权益工具；委托随时可以更改。

今天，议会与团队范围有限的所有者角色并行运作。待第 13 节的去中心化步骤完成，它就是协议仅存的协调层。

10. 公共物品

每个周期都将周期储备的 7% 转拨给公共物品金库，其受益方目前是 Protocol Guild，即 170 余位以太坊核心协议贡献者的集体资助机制。转拨作为收官的一部分在链上强制执行，没有人逐周期决定是否兑现。协议使用得越多，流向以太坊赖以运转的基础设施的也就越多。

道理并不复杂：Cosmic Signature 因以太坊基础层持续运转而存在，一个活在公共基础设施之上的协议，就该用它做其他一切事情的方式来资助这层设施：机械地、按节奏地、公开地。金库也接受周期之外的自愿 ETH 贡献。

> 此处是将 ETH 转拨至公共物品地址（目前为 Protocol Guild）的行为，不构成美国税法意义上的慈善捐赠，Cosmic Signature 亦不对其在任何司法辖区的税务处理作出任何陈述。

11. 安全、随机性与可验证性

11.1 独立审查

2025 年末，Hacken 对 Cosmic Signature 合约完成了独立安全审查，范围覆盖核心协议、CST 代币、两个 NFT 集成、锚定钱包，以及配套的钱包与系统管理合约。最终报告于 2026 年 1 月发布，共列出 23 项发现：无严重级，无高危级，中危 3 项、低危 8 项、信息级 12 项，其中多数是团队已审阅并附书面理由接受的设计取舍。

人工审查之外，Hacken 还对 14 项系统不变量做了模糊测试，例如协议持有的 ETH 总额必须始终等于存入减去发放。全部 14 项在 10,000 次运行中均保持成立。报告全文公开，链接见参考资料。

外部审查之外，代码仓库还带有 Certora 形式化验证规范、Solidity SMTChecker 配置、Slither 静态分析，以及一套以 Solidity 源码全覆盖为目标的测试。

11.2 防御式设计

- 重入防护覆盖核心合约的每个外部入口。
- 取回优先于送达：次级 ETH 分配与附加资产存入托管，而非在收官时直接发送，任何获配方合约都无法借此阻塞周期落幕。
- 容错转拨：公共物品转账若无法完成，收官照常进行，事件记录在案，留待后续处理。
- 周期间锁定：周期运行期间，核心参数不可更改，合约不可升级（见第 13 节）。

11.3 随机性

协议在两处需要随机性：收官时的星选，以及每枚新 NFT 的种子。它在链上把上一区块哈希、当前基础费，以及来自 ArbSys 与 ArbGasInfo 预编译合约的 Arbitrum 专属熵（上一 Arbitrum 区块哈希、gas 积压量与 L1 计价计数器）折叠成一个种子，再以 keccak256 从中逐个导出随机值。预编译调用具备容错性，某一来源不可用时，构造会退回其余来源。

这是有意的极简：不引入预言机，不依赖外部委员会，也没有任何可能让周期搁浅的回调。取舍摆在明处：排序器理论上可以影响区块级输入，而设计限定了这种影响所能触及的范围。只有星选与艺术种子使用这套随机性；倒计时、落笔价格序列和第 5 节的每一个百分比都是确定性的。整个构造每次收官只使用一次，而收官本身是任何人都能提交的公开交易。

11.4 公开验证

全部合约都已在 Sourcify 上以精确匹配状态完成源码验证（链 ID 42161），地址固定于附录 A。艺术管线的确定性由持续集成断言：生成帧的 SHA-256 哈希逐一核对。项目自有代码均为 CC0：任何人都可以复刻合约、渲染器或网站，也可以用种子重新生成任何一幅签名来核验。

12. 部署历史与前路

Cosmic Signature 的设计目标是"完工"。可升级性之所以存在，是为了在协议早期能对照真实行为修正机制；设计定稿之日，就是它谢幕之时。本节记录已经发生的与尚待发生的。

12.1 V1：上线

V1 将协议部署上 Arbitrum One，置于 UUPS 可升级代理之后：周期、落笔、分配轨道、锚定、议会与艺术管线，与本文所述基本一致。升级需由所有者发起，且只能在周期间进行。协议刻意不设任何在周期进行中修改合约的机制，无论情形如何。

12.2 V2 升级：现已上线

V2 是当前部署的实现，共有五项改动，每一项都回应了已观察到或可预见的行为。

- 动态参与 CST。每笔固定 100 CST 改为第 7.1 节的平方根公式。固定铭刻曾让高频连续落笔沦为凭空生成 CST 的手段；新规则按耐心铭刻，而非按频次。
- 最低铭刻保护。每个落笔方法新增一项参数，用于指定参与者可接受的最低参与 CST 数额，避免签名与执行之间的时间差造成损失。
- 活的 CST 校准窗口。窗口时长改为链上存储值，随落笔构成变化（见第 4.3 节），让 ETH 与 CST 两条路径互相制衡。
- 更长的专属窗口。收官之笔参与者的专属收官窗口由 24 小时延长至 48 小时。
- 时序与算术加固。倒计时延长一律作用于链上存储的收官时间，堵住了到期后用近乎免费的 CST 落笔反复外推截止时间的漏洞；排定下一周期的算术同样加固，任何参数组合，无论多么极端，都无法阻止周期收官。

12.3 规划中的 V3 升级

正在公开仓库中开发的 V3 只改一件事：晚出手的代价。周期收官时间前的最后 20 分钟内，一切落笔价格（ETH、附加 Random Walk NFT 的 ETH、CST）都会乘上一个溢价系数，从 1 倍按多项式攀升至 10 倍：到点即达 10 倍，超时落笔同样按 10 倍计。

$m(t) = 1 + 9 \cdot (t / T)^8$，其中 $T = 20$ 分钟

临近收官的价格溢价；t 为最后 *20* 分钟窗口内已经过的时间。

指数是关键。八次方的曲线让溢价在窗口的大部分时间里几乎无感，只在最后陡然直立：距收官 10 分钟约 1.04 倍，5 分钟约 1.9 倍，1 分钟约 7 倍，到点 10 倍。

意图是改写终局。V2 之下，拖到最后几秒落笔近乎零成本，周期可能在一阵低信号的卡点操作中收场。V3 之下，压哨一笔成了昂贵的表态，贯穿周期的持续参与相对便宜，想在第 5.2 节的坚守轨道上偷袭得手，也难得多。参数在部署前仍可能微调，机制则如上所述。

13. 全面去中心化之路

协议目前有一位所有者，即部署它的地址。这一角色真实存在，本文无意淡化；但它天生范围有限，并且注定是临时的。

周期运行期间，核心参数全部锁定：所有者不能在周期中途更改比例、增量或价格，也不能升级合约；所有者的操作只存在于周期与周期之间的缝隙里。另有三项范围更窄的权限随时可用：把下一周期的启用时间向后推（仅限其首笔落笔到来之前）、调整下一周期前的延迟，以及管理外围合约，即公共物品金库受益方、NFT 元数据 URI 与托管取回期限。任何所有者权限都触不到托管中的分配、已铭刻的 NFT、已记录的种子或任何人的 CST 余额；也没有任何团队钱包从落笔中收取 ETH。

这些权限之所以存在，是因为机制是全新的。V2 的每一项改动都来自线上真实行为的教训，V3 亦然；一段有边界、全公开的调整期，是设计走向完工的方式。清单里最强的权限是升级本身，而它同样公开：新实现上链即可见、可验证，且必须赶在下一周期开始之前完成。

终点是这样约定的：待以 V3 为首的剩余升级完成、机制与代币设计定稿，部署者地址将交出全部特权控制。所有者角色将永久离开部署者，或转交宇宙议会，或直接放弃所有权，具体方式会提前公布。自那时起，任何私人主体都无法再升级协议或更改参数，部署者地址所拥有的，与其他任何地址再无不同。留下来的，是按部署形态运行的协议、作为协调层的议会，以及艺术本身。

这一进程的每一步都在链上公开可见，包括最后一步。

14. 释疑与风险因素

14.1 Cosmic Signature 不是什么

Cosmic Signature 不是彩票，不是赌场，也不是赌博产品。这里没有庄家，没有荷官，也没有赌注。参与者以价值换取参与本身：每一笔都是塑造作品、延长周期并永久记录在链上的表达行为。协议不留任何运营方抽成；第 5 节的每条分配轨道，流向的都是参与者、已锚定的 NFT、滚动储备或公共物品。

Cosmic Signature 也不是投资产品，本文的任何内容都不构成投资建议或证券要约。CST 与 Cosmic Signature NFT 是参与凭据与艺术对象，协议不对其价格、流动性或未来价值作任何承诺；任何人都不应带着“凭他人努力获利”的预期取得它们。

14.2 风险因素

- 智能合约风险。合约经过审查、形式化分析与源码验证，但这些都不构成保证；任何持有价值的软件都可能存在未知缺陷。
- 随机性边界。星选使用区块衍生熵（见第 11.3 节），排序器理论上可施加影响；设计限定了后果的范围，但无法彻底消除。
- 时限责任。48 小时收官窗口与 5 周托管期限是真实的截止时间；逾期未取回的分配将向他人开放，这正是设计使然。
- 参数变更。去中心化步骤完成之前，参数仍可能按第 13 节所述在周期间调整；每次变更都会在下一周期开始前公开。
- 资产波动。ETH、CST 与 NFT 的价值都会波动。参与需要花费真金白银，应把落笔当作为参与和艺术付出的花费，而非获取金钱的途径。
- 监管不确定性。数字资产的法律定性因司法辖区而异，且仍在演变。

15. 结语

Cosmic Signature 想要建成这样一个生成艺术协议：不需要任何人的许可，最终也不需要任何人的照看。机制小到可以完整写清：价格递减的窗口、落笔不断延长的倒计时、固定的分配比例、滚动累积的储备，以及一门只由物理和种子决定的艺术。剩下的升级屈指可数，且全部公开。待它们完成，所有者角色退场，留下的正是本文所写的一切：一座时钟、一份储备、一枚代币、一个议会，以及一幅接一幅、记录着每双塑造之手的签名。

附录 A：已验证合约地址

合约	地址（Arbitrum One）
协议合约（代理）	`0x6a714Ae7B5b6eA520F6BCA23d2E609C4Fd5863F2`
协议实现（V2）	`0x50eB3d05d2C463949DE9238D419385594f7AdB97`
CST 代币	`0xAD91843e6A58Ba560F577E676986AFb1dba6FBA0`
Cosmic Signature NFT	`0xbb84Be3500A63581d3F2d5AC3bdF8685AAedad25`
Random Walk NFT	`0x895a6F444BE4ba9d124F61DF736605792B35D66b`
宇宙议会	`0xF3D52E1c681949be7E624778dB13DaD7F8c729db`
公共物品金库	`0x96bB0ADB414d5350f435E52f94946B6C7A0760a9`
推广储备	`0xa3802c799f5e3D3D3562A9B513a41C6aAF92e25e`
分配钱包	`0xE1b619e9B39ea4109D2F429Ea5eAA307759b0011`
锚定钱包（Cosmic Signature NFT）	`0x6308A405B4FF1eA890870Efe2a6D036750B81F7C`
锚定钱包（Random Walk NFT）	`0x5EB3396092841E6c5b0b51141699F6711E830529`

全部合约均已在 *Sourcify* 上完成精确匹配验证（链 *ID 42161*）。代理地址是协议的永久地址；实现只会经由第 *12*、*13* 节所述的公开升级流程更替。

附录 B：参数一览

参数	数值
首个周期开场价格	0.0001 ETH（固定）
ETH 校准窗口上限	上一周期开场实付价格的 2 倍
ETH 校准窗口下限	上限 ÷ 200，再加 1 wei
ETH 落笔价格步进	每笔 ETH 落笔上调 1%，再加 1 wei
Random Walk NFT 降价	50%，每枚一生一次
CST 校准窗口上限	max(上一笔 CST 实付价格的 2 倍，200 CST)
CST 校准窗口下限	0 CST
CST 校准窗口时长	初始基准 12 小时；每笔 ETH 落笔约 -0.398%，每笔 CST 落笔约 +0.4%
开场后的初始倒计时	上线时约 24 小时
每笔落笔的时间增量	上线时 1 小时，每周期增长 1%
专属收官窗口	48 小时
托管取回期限	5 周，随后公开取回
落笔消息长度上限	280 字节
ETH 分配轨道	签名 25%、时之勇士 8%、公共物品 7%、锚定派发 6%、ETH 星选 4%
滚动储备	约 50% 滚入下一周期
每份 NFT 发放的表彰 CST	1,000 CST
每周期推广储备	3,000 CST
典型周期铭刻量	24 枚 NFT，27,000 CST 固定发放

参数	数值
议会参数	提案门槛 100 CST，延迟 2 天，协调期 2 周，法定权重 3%
下一周期前延迟	默认 30 分钟，所有者可调整

会演变或可调整的参数以上线值列出；实时数值以合约为准。

参考资料

1. Cosmic Signature 合约仓库（源码、测试与验证工具）. https://github.com/PredictionExplorer/Cosmic-Signature
2. Cosmic Signature 应用. https://app.cosmicsignature.com/zh
3. Cosmic Signature 协议站点. https://cosmicsignature.com/zh
4. Hacken 对 Cosmic Signature 合约的安全审查（2026 年 1 月）. https://hacken.io/audits/cosmic-signature/sca-cosmic-signature-cosmicsignature-contracts-oct2025/
5. Protocol Guild 文档. https://protocol-guild.readthedocs.io
6. OpenZeppelin Governor 文档. https://docs.openzeppelin.com/contracts/5.x/governance
7. Arbitrum One. https://arbitrum.io

Bobrovytsky, T. (2026). Cosmic Signature: A Procedural On-Chain Art Protocol. Version 1.0.