

Cosmic Signature

Arbitrum 上的程序化鏈上藝術協議

Taras Bobrovytsky taras@cosmicsignature.com

版本 1.0 · 2026 年 8 月

摘要

Cosmic Signature 是部署在 Arbitrum One 上的程序化藝術協議，以一個個限時的演繹週期運轉。週期進行中，參與者以 ETH 或協議的 ERC-20 代幣 CST 落筆：每一筆都會延長收官倒數，計入一次星選資格，還可能銘刻新的 CST。倒數結束、週期收官後，協議將 ETH 儲備分配至十餘條軌道，銘刻新一代 Cosmic Signature NFT，並把固定份額轉撥給 Protocol Guild，即 170 餘位以太坊核心貢獻者的資助機制。約一半儲備滾入下一週期，每個新週期都以更大的儲備開場。

每枚 Cosmic Signature NFT 都是對引力三體問題的確定性渲染：作品由鏈上種子生成，任何人都能逐畫素復現，全程沒有神經網路參與。本文完整闡述協議機制與代幣設計，紀錄已上線的 V2 升級，介紹規劃中的 V3 升級，並闡明一項承諾：待設計定稿，部署者地址將交出全部特權控制。

目錄

1. 引言	2
2. 協議概覽	3
3. 演繹週期	3
3.1 開場與 ETH 校準窗口	4
3.2 收官倒數	4
3.3 收官與公開收官窗口	4
4. 落筆	4
4.1 ETH 落筆	4
4.2 附加 Random Walk NFT	4
4.3 CST 落筆	5
4.4 訊息與附加資產	5
5. 週期儲備與分配軌道	5
5.1 收官時的發放	5
5.2 堅守冠軍與時之勇士	6
5.3 星選	6
5.4 發放、託管與期限	6

6. 藝術：確定性的三體簽名	6
6.1 渲染管線	7
6.2 可復現性與許可	7
7. CST 代幣	7
7.1 銘刻規則	7
7.2 銷燬與供應動態	8
7.3 協調權重	8
8. 錨定	8
9. 宇宙議會	8
10. 公共財	9
11. 安全、隨機性與可驗證性	9
11.1 獨立審查	9
11.2 防禦式設計	9
11.3 隨機性	9
11.4 公開驗證	10
12. 部署歷史與前路	10
12.1 V1：上線	10
12.2 V2 升級：現已上線	10
12.3 規劃中的 V3 升級	10
13. 全面去中心化之路	11
14. 釋疑與風險因素	11
14.1 Cosmic Signature 不是什麼	11
14.2 風險因素	11
15. 結語	12
附錄 A：已驗證合約地址	12
附錄 B：參數一覽	12
參考資料	13

1. 引言

Cosmic Signature 源於兩個信念。其一，生成藝術最動人的時刻，是它沒有任何隨意性：每幅影像都是物理過程的輸出，由種子唯一確定，任何人重跑一遍流程即可驗證結果。其二，一個替參與者保管 ETH 的協議，應當對「每一個 wei 去了哪裡」給出機械的、可讀的答案。

由此而來的，是一個圍繞時間構建的協議。演繹週期開啟，在一次次落筆中延展，倒數歸零後落幕。落筆是一次小小的鏈上行為：攜帶 ETH 或 CST，可附上一句短訊息或一份資產，並把週期

的收官時間向後推。倒數結束時，最後落下的那一筆就是收官之筆，其參與者可完成收官：發放儲備、銘刻本週期的 NFT，併為下一週期做好準備。

三項性質貫穿整個設計。

- 確定性。作品由銘刻時記錄在鏈上的種子計算而來。渲染管線開源，同一種子永遠產出同一影像與影片，逐位元一致。
- 機械化發放。分配比例是已驗證合約中的常量。參與者與發放規則之間沒有任何自由裁量的帳戶，也沒有團隊錢包從落筆中收取 ETH。
- 有限的團隊角色。所有者權限範圍很窄，在週期執行期間全部鎖定，並將在剩餘升級完成後徹底移除。

本文是協議的權威說明。第 2 節勾勒系統全貌；第 3 至 5 節定義週期、落筆與分配；第 6 節介紹藝術；第 7 至 10 節涵蓋 CST、錨定、宇宙議會與公共財；第 11 節討論安全與可驗證性；第 12、13 節紀錄升級歷史與全面去中心化路線；第 14 節直言協議不是什麼。文中引用的數字要麼是合約常量，要麼是鏈上參數的上線初始值；附錄 A 所列的已部署合約始終是最終依據。

2. 協議概覽

系統由一份核心合約和環繞它的一組單一職責合約構成。核心合約部署在可升級代理之後，負責運轉週期：為落筆定價、維護倒數、持有週期儲備、執行收官。環繞它的是 CST 代幣、Cosmic Signature NFT 系列、分配託管錢包、兩個錨定錢包、公共財金庫、推廣儲備與宇宙議會。

元件	職責
協議合約 CST (ERC-20) Cosmic Signature NFT (ERC-721) Random Walk NFT	運轉演繹週期：落筆定價、收官倒數、週期儲備與收官執行。 參與代幣。僅由協議銘刻，用於落筆時銷燬，完成委託後表達協調權重。 確定性三體藝術作品。僅在收官時銘刻，種子儲存在鏈上。 同一團隊更早的生成藝術系列。可一次性降低落筆價格，並擁有獨立的錨定星選軌道。
分配錢包 錨定錢包	託管次級 ETH 分配與隨落筆附加的資產，設有公開取回期限。 一個面向 Cosmic Signature NFT (ETH 錨定配發)，一個面向 Random Walk NFT (星選資格)。
公共財金庫 推廣儲備 宇宙議會	接收並轉撥每週期的公共財分配，受益方目前為 Protocol Guild。 每週期接收 3,000 CST，用於社群推廣。 鏈上協調機構，完成委託的 CST 在其中表達協調權重。

合約之外，一個生態正在生長：應用程式位於 app.cosmicsignature.com，NFT 在 Axiom Zero 市場流通，CST 在 Arbitrum 上有 Uniswap 流動性，Chaos Zero 則為每個週期提供預測場所。它們都不是必需的：本文所述的每項機制，都可以直接呼叫合約完成。

3. 演繹週期

週期是一段時間之窗：以價格遞減的校準窗口開啟，在落筆中延展，倒數結束並有人收官後落幕。本節講清這座時鐘；落筆本身見第 4 節。

3.1 開場與 ETH 校準窗口

每個週期的首筆落筆必須使用 ETH，其價格由 ETH 校準窗口決定。窗口起始價為上一週期開場實付價格的 2 倍，隨後線性下行，直至起始價的兩百分之一加 1 wei。按上線參數，整段下行約需兩天；時長與週期時間增量掛鉤，會隨協議年歲緩慢拉長。若窗口走完仍無人落筆，價格便停在底價等待。第一個週期以固定的 0.0001 ETH 開場。

這套開場機制不依賴訂單簿：上一週期若開得太便宜，翻倍會先恢復上行空間；翻倍後若顯得偏高，兩天的緩慢下行總會停在有人願意開場的位置。

3.2 收官倒數

首筆落筆啟動時鐘，按上線參數將週期收官時間設在約 24 小時之後。此後每筆 ETH 或 CST 落筆，都會把目前時間增量加到鏈上收官時間上。增量上線時恰為 1 小時，並在每個週期收官後增長 1%，週期因此逐漸變長，NFT 的銘刻節奏也隨歲月放緩。只要落筆不斷，週期長度沒有硬性上限；但落筆價格持續上行，無限延長在實踐中代價高昂。

延長作用於鏈上儲存的收官時間，而非當下時刻。倒數已過、收官尚未執行時，落筆依然有效：它把儲存值再推一個增量，並接任收官之筆，但不會讓時鐘從頭再來。

3.3 收官與公開收官窗口

週期收官時間一到，收官之筆參與者即可收官。收官是一筆交易：讀取協議的 ETH 餘額，按第 5 節的軌道發放，銘刻本週期的 NFT 與 CST，為每件新作品紀錄種子，並排定下一週期。

這項權利在 48 小時內專屬於收官之筆參與者。窗口過後進入公開收官：任何人都可收官，合約會把實際收官者視為週期受益方，該角色的一切隨之歸屬，包括簽名分配的 ETH 份額、CST 銘刻、NFT，以及對已附加資產的優先權。這條規則刻意不留情面：即使參與者消失，協議照樣前行；疏忽也有價格，受益方兩天內不出手，角色就向第一位來者敞開。

收官之後，下一週期經過一段短暫延遲啟用（預設 30 分鐘），校準窗口隨之開啟。

4. 落筆

落筆是協議唯一的輸入。無論使用哪種貨幣，每一筆都會延長倒數、在參與者星選池中計入一次資格、更新第 5.2 節的堅守時鐘，還可能按第 7.1 節銘刻參與 CST。

4.1 ETH 落筆

開場之後，每筆 ETH 落筆都會把下一筆的 ETH 落筆價格抬高 1%，再加 1 wei。這條序列公開而精確，落筆前隨時可以從合約讀到目前價格。超付的金額會在同一筆交易中退回；只有當退款連 gas 都不夠抵時，差額才留在儲備中。

4.2 附加 Random Walk NFT

持有 Random Walk NFT 的參與者，可將其附加到一筆 ETH 落筆上，使該筆價格降低 50%。NFT 不會轉移，合約只是將其標記為已使用。每枚 Random Walk NFT 在所有週期中僅可附加一次：降價因此成了一種消耗品，一個數量固定的外部系列也由此融入協議經濟。

4.3 CST 落筆

CST 提供第二條入口。CST 校準窗口的起始價為上一筆 CST 實付價格的 2 倍，且不低於 200 CST，隨後在窗口時長內線性降至零。每筆 CST 落筆都會以新的起始價重啟窗口，所付 CST 全數銷燬，永久移出供應量。

窗口時長本身也是鏈上的活參數，是協議裡一條安靜的回饋迴路。它從 12 小時的基準出發：每筆 ETH 落筆使其縮短約 0.398%，每筆 CST 落筆使其延長約 0.4%。ETH 落筆越密集，CST 價格降得越快，CST 落筆越早變得划算；CST 落筆多了，下行又會放慢。這條迴路把每個週期推向兩種貨幣的均衡組合。

價格既然能降到零，足夠長的沉寂就能讓一筆 CST 落筆近乎免費。這是有意為之：只要有人持有哪怕一點 CST，週期就總能延續；而每筆 CST 落筆的銷燬，又把代幣供應量與真實使用綁在一起。提交 CST 落筆時需指定可接受的最高價格，交易落地晚於預期也不會多花一分。

每個週期的首筆落筆必須使用 ETH；從第二筆起即可使用 CST。

4.4 訊息與附加資產

落筆可攜帶最長 280 位元組的訊息，與落筆一同記錄在鏈上；也可附加 ERC-20 代幣或一枚 ERC-721 NFT。附加資產不進入 ETH 儲備，而由分配錢包託管；週期收官後，受益方享有優先取回權，並受第 5.4 節的公開取回期限約束。

5. 週期儲備與分配軌道

所有落筆支付的 ETH 都匯入協議合約，連同上一週期約一半的儲備，共同構成週期儲備。收官時讀取一次餘額，按固定比例發放。

5.1 收官時的發放

ETH 軌道	佔週期儲備份額	獲配者
簽名分配	25%	週期受益方，通常為收官之筆參與者。
時之勇士分配	8%	在位最久的堅守冠軍（見第 5.2 節）。
公共財分配	7%	Protocol Guild，經公共財金庫轉撥。
錨定配發	6%	已錨定的 Cosmic Signature NFT，按比例分攤。
ETH 星選	4%	從本週期落筆資格池中選出 3 次，均分該份額。
滾動儲備	約 50%（其餘部分）	滾入下一週期。

各比例均按收官那一刻協議的 ETH 餘額計算。

五條發放軌道合計正好一半，其餘滾動累積：協議滾動累積，而非抽取，每個週期都以比上一週期更大的儲備開場。若收官時沒有任何已錨定的 Cosmic Signature NFT，該週期的錨定配發將跳過，這部分份額同樣滾入下一週期。

CST 與 NFT 軌道	發放內容	獲配者
簽名分配	1,000 CST 與 1 枚 NFT	週期受益方。
時之勇士	1,000 CST 與 1 枚 NFT	時之勇士。
堅守冠軍	1,000 CST 與 1 枚 NFT	堅守冠軍。

CST 與 NFT 軌道	發放內容	獲配者
CST 收官之筆	1,000 CST 與 1 枚 NFT	本週期最後一筆 CST 落筆的參與者。
參與者 NFT 星選	1,000 CST 與 1 枚 NFT，共 10 次	從落筆資格池中選出。
錨定 NFT 星選	1,000 CST 與 1 枚 NFT，共 10 次	在已錨定的 Random Walk NFT 中選出。
推廣儲備	3,000 CST	社群推廣（見第 7.1 節）。

因此，典型週期共銘刻 24 枚 Cosmic Signature NFT，外加 27,000 CST 的固定發放；各筆落筆沿途銘刻的參與 CST 另計。沒有 CST 落筆的週期跳過 CST 收官之筆軌道；沒有已錨定 Random Walk NFT 的週期跳過錨定星選。

5.2 堅守冠軍與時之勇士

有兩條軌道衡量的是堅持，而非位置。堅守冠軍，是本週期內以最近落筆者身份堅守最久的參與者，也就是單筆落筆擄過的最長靜默間隔。時之勇士再上一層：誰連續在位堅守冠軍的時間最長，誰就是時之勇士。

兩者的差別細微而真實。慵懶的午後落下一筆、十個小時無人打破，就立下了一段漂亮的堅守間隔；但能否以時之勇士的身份走完週期，取決於這項紀錄在他人刷新之前又存續了多久。堅守衡量你創造的間隔，時之勇士衡量紀錄存活的時長。兩者都要到收官那一刻才塵埃落定。

5.3 星選

每筆落筆都在本週期的參與者星選池中計入一次資格。收官時，合約為 ETH 星選選出 3 次資格，均分儲備的 4%；再為 NFT 星選選出 10 次。選擇採用放回方式，同一參與者可能被選中多次；資格隨落筆累積，入選頻次與參與程度成正比。

另有一條獨立的錨定 NFT 星選，在已錨定的 Random Walk NFT 中選出 10 次，權重按各錨定者錨定的 NFT 數量計。這條軌道只發放 CST 與 Cosmic Signature NFT，不含 ETH。

這些選擇背後的隨機性在收官時於鏈上構造，其來源與邊界見第 11.3 節。

5.4 發放、託管與期限

發放刻意分成兩類：主動送達與自行取回。簽名分配的 ETH 在收官時直接送達受益方，公共財轉撥亦然；時之勇士的 ETH 與三份 ETH 星選份額則存入分配錢包託管，獲配者隨時取回。CST 與 NFT 在收官時直接銘刻到各自獲配者名下。

託管中的分配與附加資產會等待 5 週。期限一過，合約允許任何人為自己取回仍未取回的分配。這條規則與公開收官窗口一脈相承：協議不為缺席者無限期停留，每份發放終會到達想要它的人手中。請及時取回。

6. 藝術：確定性的三體簽名

每枚 Cosmic Signature NFT 都是對引力三體問題的一次渲染：三個質量相近的天體在牛頓引力下互繞。三體問題沒有一般解析解，軌跡天然混沌，初始條件的毫釐之差會演成完全不同的舞步。這種混沌正是整個系列的引擎：種子決定初始條件，物理完成其餘一切，沒有兩幅簽名會重樣。

任何階段都沒有生成式模型參與。沒有訓練資料，沒有採樣，也沒有提示詞。管線就是一段物理模擬加一個渲染器，以 Rust 寫成，完全開源，徹底確定。

6.1 渲染管線

- 種子。銘刻時，合約從鏈上資料匯出 32 位元組種子（見第 11.3 節），並與 NFT 一同儲存。種子初始化一個 SHA3-256 隨機數生成器，此後的一切都是它的純函式。
- 模擬。十萬組候選構型分別透過四階 Yoshida 辛積分器演算，每組推進 1,000,000 個物理步；這種積分器能在長時間尺度上保持系統的能量行為。
- 遴選。Borda 排序聚合按混沌程度與三角形的等邊程度為候選打分，選出視覺上最意味的一條軌道。
- 鏡頭。緩慢的橢圓鏡頭漂移穿行於軌道之間，賦予每幅簽名電影般的視差。
- 色彩。色彩在 OKLab 感知色彩空間中混合，各天體色相相隔 120°，並由漂移與正弦波調變。
- 光譜渲染。從 380 至 700 奈米劃分 64 個波長區間，以隨速度變化的線寬和景深渲染軌跡。
- 收尾。AgX 色調對映、輝光、OpenSimplex 星雲層與色彩分級共同完成畫面。

每枚 NFT 的最終輸出，是一張 16 位元 PNG 與一段 30 秒 H.265 影片。

6.2 可復現性與許可

確定性靠機制保證，而非口頭承諾。同一種子在任何機器上都產出逐畫素一致的影像，生成幀的 SHA-256 雜湊在持續整合中逐一斷言。種子全部在鏈上，管線完全公開，這個系列因此不依賴任何伺服器：哪怕明天所有伺服器都消失，每幅簽名都能從鏈上重生。

所有者可在鏈上為 NFT 命名，最長 32 位元組。專案自有的合約、著色器與渲染管線均以 CC0 1.0 獻入公有領域，不保留任何權利；第三方依賴保留各自的授權。

7. CST 代幣

CST 是協議的 ERC-20 代幣。供應量從零起步，代幣合約只接受協議合約的銘刻與銷燬指令。流通中的每一枚 CST，都能追溯到某個週期裡的一次參與。

7.1 銘刻規則

CST 經三條途徑進入流通。參與 CST 在落筆時按下方公式銘刻。表彰 CST 在收官時銘刻：本週期每份 NFT 發放都伴隨 1,000 CST，典型週期共 24 份。此外，每週期還有 3,000 CST 進入推廣儲備，由團隊用於社群推廣；這是團隊經手的唯一一條固定 CST 流，且不附帶任何特殊權限。

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

一筆落筆銘刻的參與 CST。經過時間自上一筆起算，並按目前週期時間增量歸一化。

直白地說，數量隨距上一筆時間的平方根增長。上一筆落下一秒後就跟進，幾乎什麼也銘刻不到；終結一整天沉默的一筆，能銘刻數百 CST。

距上一筆的時間	參與 CST
0 秒	0
1 秒	1.73
60 秒	13.4
1 小時	104
1 天	509

按上線時恰為 1 小時的時間增量計算。增量逐週期增長後，實際數額會略低於表中值；即時預覽與合約本身才是最終依據。

7.2 銷燬與供應動態

CST 一經使用即離開流通：每筆 CST 落筆支付的全部價格都會銷燬。供應量因此由行為塑造：沉寂的週期銘刻的參與 CST 不多，活躍的 CST 使用又把供應量燒回去，固定的表彰與推廣兩條流則為每個典型週期穩定注入 27,000 CST。沒有上限，沒有預留份額，也沒有團隊分配。

平方根公式本身就是一道供應閘門，由 V2 升級引入（見第 12.2 節）。最初的設計是每筆固定銘刻 100 CST，機器速度的連續落筆由此成了源源不斷的新 CST 來源。改用現行規則後，一串急促的落筆幾乎什麼都銘刻不到；創造供應的，是耐心的參與。

7.3 協調權重

CST 同時是宇宙議會（第 9 節）的權重代幣。權重在委託後生效：持有者把權重委託給自己或其他地址，此後每枚 CST 表達一個單位的協調權重。代幣採用基於時間戳的檢查點，提案快照對應的是鐘錶時間，而非區塊高度。

8. 錨定

錨定是協議的長期對齊方式。所有者可將 Cosmic Signature NFT 錨定至協議；錨定期間，它按比例累積每週期 6% 的錨定配發，累積的 ETH 在解錨時取回。錨定沒有固定期限，也沒有任何罰則，但它是每枚 NFT 一次性的決定：每枚 NFT 一生僅可錨定一次，解錨即永久失去錨定資格。

一生一次的規則，用一個不可逆的抉擇取代了常見的鎖定時間表，也讓已錨定的集合有了真實的退出成本。要不要繼續錨定，是每個週期都可以重新掂量的活問題；要不要解錨，則是永久的決定。

Random Walk NFT 的錨定自成一線，目的也不同：已錨定的 Random Walk NFT 參與錨定 NFT 星選（見第 5.3 節），每週期 10 次，每次攜帶 1,000 CST 與一枚 Cosmic Signature NFT。Random Walk 錨定不含 ETH 配發。一生一次的規則同樣適用。

9. 宇宙議會

宇宙議會是協議的鏈上協調機構，基於經過審計的 OpenZeppelin Governor 框架構建，以 CST 為權重代幣。任何持有至少 100 CST 委託權重的地址都可提交協調提案。提案先經過 2 天協調延遲，再進入 2 週的協調期。

提案通過需同時滿足兩個條件：支持權重高於反對權重，且支持與棄權權重之和達到 CST 總供應量 3% 的協調法定權重。反對權重不計入法定權重。表達權重是一次密碼學行為，不是股份或權益工具；委託隨時可以更改。

今天，議會與團隊範圍有限的所有者角色並行運作。待第 13 節的去中心化步驟完成，它就是協議僅存的協調層。

10. 公共財

每個週期都將週期儲備的 7% 轉撥給公共財金庫，其受益方目前是 Protocol Guild，即 170 餘位以太坊核心協議貢獻者的集體資助機制。轉撥作為收官的一部分在鏈上強制執行，沒有人逐週期決定是否兌現。協議使用得越多，流向以太坊賴以運轉的基礎設施的也就越多。

道理並不複雜：Cosmic Signature 因以太坊基礎層持續運轉而存在，一個活在公共基礎設施之上的協議，就該用它做其他一切事情的方式來資助這層設施：機械地、按節奏地、公開地。金庫也接受週期之外的自願 ETH 貢獻。

此處是將 ETH 轉撥至公共財地址（目前為 Protocol Guild）的行為，不構成美國稅法意義上的慈善捐贈，Cosmic Signature 亦不對其在任何司法轄區的稅務處理作出任何陳述。

11. 安全、隨機性與可驗證性

11.1 獨立審查

2025 年末，Hacken 對 Cosmic Signature 合約完成了獨立安全審查，範圍覆蓋核心協議、CST 代幣、兩個 NFT 整合、錨定錢包，以及配套的錢包與系統管理合約。最終報告於 2026 年 1 月發布，共列出 23 項發現：無嚴重級，無高危級，中危 3 項、低危 8 項、資訊級 12 項，其中多數是團隊已審閱並附書面理由接受的設計取舍。

人工審查之外，Hacken 還對 14 項系統不變數做了模糊測試，例如協議持有的 ETH 總額必須始終等於存入減去發放。全部 14 項在 10,000 次執行中均保持成立。報告全文公開，連結見參考資料。

外部審查之外，程式碼儲存庫還帶有 Certora 形式化驗證規範、Solidity SMTChecker 配置、Slither 靜態分析，以及一套以 Solidity 原始碼全覆蓋為目標的測試。

11.2 防禦式設計

- 重入防護覆蓋核心合約的每個外部入口。
- 取回優先於送達：次級 ETH 分配與附加資產存入托管，而非在收官時直接傳送，任何獲配方合約都無法藉此阻塞週期落幕。
- 容錯轉撥：公共財轉帳若無法完成，收官照常進行，事件記錄在案，留待後續處理。
- 週期間鎖定：週期執行期間，核心參數不可更改，合約不可升級（見第 13 節）。

11.3 隨機性

協議在兩處需要隨機性：收官時的星選，以及每枚新 NFT 的種子。它在鏈上把上一區塊雜湊、目前基礎費，以及來自 ArbSys 與 ArbGasInfo 預編譯合約的 Arbitrum 專屬熵（上一 Arbitrum 區塊雜湊、gas 積壓量與 L1 計價計數器）摺疊成一個種子，再以 keccak256 從中逐個匯出隨機值。預編譯呼叫具備容錯性，某一來源不可用時，構造會退回其餘來源。

這是有意的極簡：不引入預言機，不依賴外部委員會，也沒有任何可能讓週期擱淺的回撥。取舍擺在明處：排序器理論上可以影響區塊級輸入，而設計限定了這種影響所能觸及的範圍。隨機性的消費者只有星選與藝術種子；倒數、落筆價格序列和第 5 節的每一個百分比都是確定性的。整個構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開交易。

11.4 公開驗證

全部合約都已在 Sourcify 上以精確匹配狀態完成原始碼驗證（鏈 ID 42161），地址固定於附錄 A。藝術管線的確定性由持續整合斷言：生成幀的 SHA-256 雜湊逐一核對。專案自有程式碼均為 CC0：任何人都可以復刻合約、渲染器或網站，也可以用種子重新生成任何一幅簽名來驗證。

12. 部署歷史與前路

Cosmic Signature 的設計目標是「完工」。可升級性之所以存在，是為了在協議早期能對照真實行為修正機制；設計定稿之日，就是它謝幕之時。本節紀錄已經發生的與尚待發生的。

12.1 V1：上線

V1 將協議部署上 Arbitrum One，置於 UUPS 可升級代理之後：週期、落筆、分配軌道、錨定、議會與藝術管線，與本文所述基本一致。升級需由所有者發起，且只能在週期間進行。協議刻意不設任何在週期進行中修改合約的機制，無論情形如何。

12.2 V2 升級：現已上線

V2 是目前部署的實現，共有五項改動，每一項都回應了已觀察到或可預見的行為。

- 動態參與 CST。每筆固定 100 CST 改為第 7.1 節的平方根公式。固定銘刻曾讓高頻連續落筆淪為憑空生成 CST 的手段；新規則按耐心銘刻，而非按頻次。
- 最低銘刻保護。每個落筆方法新增一項參數，用於指定參與者可接受的最低參與 CST 數額，避免簽名與執行之間的時間差造成損失。
- 活的 CST 校準窗口。窗口時長改為鏈上儲存值，隨落筆構成變化（見第 4.3 節），讓 ETH 與 CST 兩條路徑互相制衡。
- 更長的專屬窗口。收官之筆參與者的專屬收官窗口由 24 小時延長至 48 小時。
- 時序與算術加固。倒數延長一律作用於鏈上儲存的收官時間，堵住了到期後用近乎免費的 CST 落筆反覆外推截止時間的漏洞；排定下一週期的算術同樣加固，任何參數組合，無論多麼極端，都無法阻止週期收官。

12.3 規劃中的 V3 升級

正在公開儲存庫中開發的 V3 只改一件事：晚出手的代價。週期收官時間前的最後 20 分鐘內，一切落筆價格（ETH、附加 Random Walk NFT 的 ETH、CST）都會乘上一個溢價係數，從 1 倍按多項式攀升至 10 倍：到點即達 10 倍，超時落筆同樣按 10 倍計。

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

臨近收官的價格溢價； t 為最後 20 分鐘窗口內已經過的時間。

指數是關鍵。八次方的曲線讓溢價在窗口的大部分時間裡幾乎無感，只在最後陡然直立：距收官 10 分鐘約 1.04 倍，5 分鐘約 1.9 倍，1 分鐘約 7 倍，到點 10 倍。

意圖是改寫終局。V2 之下，拖到最後幾秒落筆近乎零成本，週期可能在一陣低訊號的卡點操作中收場。V3 之下，壓哨一筆成了昂貴的表態，貫穿週期的持續參與相對便宜，想在第 5.2 節的堅守軌道上偷襲得手，也難得多。參數在部署前仍可能微調，機制則如上所述。

13. 全面去中心化之路

協議目前有一位所有者，即部署它的地址。這一角色真實存在，本文無意淡化；但它天生範圍有限，並且註定是臨時的。

週期執行期間，核心參數全部鎖定：所有者不能在週期中途更改比例、增量或價格，也不能升級合約；所有者的操作只存在於週期與週期之間的縫隙裡。另有三項範圍更窄的權限隨時可用：把下一週期的啟用時間向後推（僅限其首筆落筆到來之前）、調整下一週期前的延遲，以及管理外圍合約，即公共財金庫受益方、NFT 後設資料 URI 與託管取回期限。任何所有者權限都觸不到託管中的分配、已銘刻的 NFT、已紀錄的種子或任何人的 CST 餘額；也沒有任何團隊錢包從落筆中收取 ETH。

這些權限之所以存在，是因為機制是全新的。V2 的每一項改動都來自線上真實行為的教訓，V3 亦然；一段有邊界、全公開的調整期，是設計走向完工的方式。清單裡最強的權限是升級本身，而它同樣公開：新實現上鏈即可見、可驗證，且必須趕在下一週期開始之前完成。

終點是這樣約定的：待以 V3 為首的剩餘升級完成、機制與代幣設計定稿，部署者地址將交出全部特權控制。所有者角色將永久離開部署者，或轉交宇宙議會，或直接放棄所有權，具體方式會提前公佈。自那時起，任何私人主體都無法再升級協議或更改參數，部署者地址所擁有的，與其他任何地址再無不同。留下來的，是按部署形態執行的協議、作為協調層的議會，以及藝術本身。

這一程序的每一步都在鏈上公開可見，包括最後一步。

14. 釋疑與風險因素

14.1 Cosmic Signature 不是什麼

Cosmic Signature 不是彩票，不是賭場，也不是賭博產品。這裡沒有莊家，沒有荷官，也沒有賭注。參與者以價值換取參與本身：每一筆都是塑造作品、延長週期並永久記錄在鏈上的表達行為。協議不留任何運營方抽成；第 5 節的每條分配軌道，流向的都是參與者、已錨定的 NFT、滾動儲備或公共財。

Cosmic Signature 也不是投資產品，本文的任何內容都不構成投資建議或證券要約。CST 與 Cosmic Signature NFT 是參與憑據與藝術物件，協議不對其價格、流動性或未來價值作任何承諾；任何人都不應帶著「憑他人努力獲利」的預期取得它們。

14.2 風險因素

- 智慧合約風險。合約經過審查、形式化分析與原始碼驗證，但這些都不構成保證；任何持有價值的軟體都可能存在未知缺陷。
- 隨機性邊界。星選使用區塊衍生熵（見第 11.3 節），排序器理論上可施加影響；設計限定了後果的範圍，但無法徹底消除。
- 時限責任。48 小時收官窗口與 5 週託管期限是真實的截止時間；逾期未取回的分配將向他人開放，這正是設計使然。
- 參數變更。去中心化步驟完成之前，參數仍可能按第 13 節所述在週期間調整；每次變更都會在下一週期開始前公開。
- 資產波動。ETH、CST 與 NFT 的價值都會波動。參與需要花費真金白銀，應把落筆當作為參與和藝術付出的花費，而非取得金錢的途徑。
- 監管不確定性。數字資產的法律定性因司法轄區而異，且仍在演變。

15. 結語

Cosmic Signature 想要建成這樣一個生成藝術協議：不需要任何人的許可，最終也不需要任何人的照看。機制小到可以完整寫清：價格遞減的窗口、落筆不斷延長的倒數、固定的分配比例、滾動累積的儲備，以及一門只由物理和種子決定的藝術。剩下的升級屈指可數，且全部公開。待它們完成，所有者角色退場，留下的正是本文所寫的一切：一座時鐘、一份儲備、一枚代幣、一個議會，以及一幅接一幅、記錄著每雙塑造之手的簽名。

附錄 A：已驗證合約地址

合約	地址 (Arbitrum One)
協議合約 (代理)	0x6a714Ae7B5b6eA520F6BCA23d2E609C4Fd5863F2
協議實現 (V2)	0x50eB3d05d2C463949DE9238D419385594f7AdB97
CST 代幣	0xAD91843e6A58Ba560F577E676986AFb1dba6FBA0
Cosmic Signature NFT	0xbb84Be3500A63581d3F2d5AC3bdf8685AAedad25
Random Walk NFT	0x895a6F444BE4ba9d124F61DF736605792B35D66b
宇宙議會	0xF3D52E1c681949be7E624778dB13DaD7F8c729db
公共財金庫	0x96bB0ADB414d5350f435E52f94946B6C7A0760a9
推廣儲備	0xa3802c799f5e3D3D3562A9B513a41C6aAF92e25e
分配錢包	0xE1b619e9B39ea4109D2F429Ea5eAA307759b0011
錨定錢包 (Cosmic Signature NFT)	0x6308A405B4FF1eA890870Efe2a6D036750B81F7C
錨定錢包 (Random Walk NFT)	0x5EB3396092841E6c5b0b51141699F6711E830529

全部合約均已在 *Sourcify* 上完成精確匹配驗證 (鏈 ID 42161)。代理地址是協議的永久地址；實現只會經由第 12、13 節所述的公開升級流程更替。

附錄 B：參數一覽

參數	數值
首個週期開場價格	0.0001 ETH (固定)
ETH 校準窗口上限	上一週期開場實付價格的 2 倍
ETH 校準窗口下限	上限 ÷ 200，再加 1 wei
ETH 落筆價格步進	每筆 ETH 落筆上調 1%，再加 1 wei
Random Walk NFT 降價	50%，每枚一生一次
CST 校準窗口上限	max(上一筆 CST 實付價格的 2 倍，200 CST)
CST 校準窗口下限	0 CST
CST 校準窗口時長	初始基準 12 小時；每筆 ETH 落筆約 -0.398%，每筆 CST 落筆約 +0.4%
開場後的初始倒數	上線時約 24 小時
每筆落筆的時間增量	上線時 1 小時，每週期增長 1%
專屬收官窗口	48 小時
託管取回期限	5 週，隨後公開取回
落筆訊息長度上限	280 位元組
ETH 分配軌道	簽名 25%、時之勇士 8%、公共財 7%、錨定配發 6%、ETH 星選 4%
滾動儲備	約 50% 滾入下一週期
每份 NFT 發放的表彰 CST	1,000 CST
每週期推廣儲備	3,000 CST
典型週期銘刻量	24 枚 NFT，27,000 CST 固定發放

參數	數值
議會參數	提案門檻 100 CST，延遲 2 天，協調期 2 週，法定權重 3%
下一週期前延遲	預設 30 分鐘，所有者可調整

會演變或可調整的參數以上線值列出；即時數值以合約為準。

參考資料

1. Cosmic Signature 合約儲存庫（原始碼、測試與驗證工具）。<https://github.com/PredictionExplorer/Cosmic-Signature>
2. Cosmic Signature 應用程式。<https://app.cosmicsignature.com/zh>
3. Cosmic Signature 協議站點。<https://cosmicsignature.com/zh>
4. Hacken 對 Cosmic Signature 合約的安全審查（2026 年 1 月）。<https://hacken.io/audits/cosmic-signature/sca-cosmic-signature-cosmicsignature-contracts-oct2025/>
5. Protocol Guild 文件。<https://protocol-guild.readthedocs.io>
6. OpenZeppelin Governor 文件。<https://docs.openzeppelin.com/contracts/5.x/governance>
7. Arbitrum One。<https://arbitrum.io>

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

本文與 Cosmic Signature 全部專案自有材料一樣，依 CC0 1.0 獻入公有領域。