Cosmic Signature

Arbitrum上のプロシージャル・オンチェーンアート・プロトコル

Taras Bobrovytsky taras@cosmicsignature.com

バージョン1.0 · 2026年8月

概要

Cosmic SignatureはArbitrum One上のプロシージャルアート・プロトコルです。時間制限のあるパフォーマンス・サイクルの連なりとして動きます。サイクルの間、参加者はETH、またはプロトコルのERC-20トークンであるCSTで一筆を入れます。すべての一筆はサイクルのカウントダウンを延ばし、サイクルの星選に対象を記録し、新しいCSTを刻印することがあります。カウントダウンが切れてサイクルが確定すると、プロトコルはETH準備金を10を超える配分トラックへ配り、新しい世代のCosmic Signature NFTを刻印し、170人以上のEthereumコア貢献者の資金支援メカニズムであるProtocol Guildへ固定の分を送ります。準備金のおよそ半分は次へ持ち越されるので、各サイクルは前より大きく始まります。

各Cosmic Signature NFTは、オンチェーンのシードから生成され、誰でもピクセル単位で再現できる、重力三体問題の決定論的なレンダリングです。ニューラルネットワークが画像に触れることはありません。本稿は仕組みとトークンの設計を完全に記述し、現在稼働中のV2アップグレードを記録し、計画されているV3アップグレードを提示し、設計が完成した後にデプロイしたアドレスからあらゆる形の特権的な管理を取り除くという約束を述べます。

目次

1. はじめに **2**

2. プロトコルの概要 **3**

3. パフォーマンス・サイクル **4**
3.1 開始とETH調律期間 4
3.2 カウントダウン 4
3.3 確定と公開確定期間 4

4. 一筆 **4**
4.1 ETH一筆 5
4.2 Random Walk NFTの添付 5
4.3 CST一筆 5
4.4 メッセージと添付されたアセット 5

5. サイクル準備金と配分トラック **5**
5.1 確定時の分配 5
5.2 持久チャンピオンと時の戦士 6
5.3 星選 6
5.4 配送、エスクロー、タイムアウト 7

6. アート：決定論的な三体シグネチャー **7**
6.1 パイプライン 7
6.2 再現性とライセンス 7

7. CSTトークン **8**
7.1 刻印のルール 8
7.2 焼却と供給量の動態 8
7.3 調整ウェイト 9

8. 係留 **9**

9. 宇宙評議会 **9**

10. 公共財 **9**

11. セキュリティ、乱数、検証可能性 **10**
11.1 独立したレビュー 10
11.2 防御的な設計 10
11.3 乱数 10
11.4 オープンな検証 10

12. デプロイの歴史と今後の道 **11**
12.1 V1：ローンチ 11
12.2 V2アップグレード、現在稼働中 11
12.3 計画されているV3アップグレード 11

13. 完全な分散化への道 **12**

14. 明確化とリスク要因 **12**
14.1 Cosmic Signatureではないもの 12
14.2 リスク要因 12

15. 結び **13**

付録A：検証済みコントラクトアドレス **13**

付録B：パラメーター一覧 **13**

参考文献 **14**

1. はじめに

Cosmic Signatureは二つの確信から始まりました。一つは、ジェネラティブアートが最も面白くなるのは、その何もが恣意的でないとき——すべての画像が物理的な過程の出力であり、シードによって固定され、誰でもその過程を再実行して結果を検証できるとき——だということです。もう一つは、参加者に代わってETHを保持するプロトコルは、すべてのweiがどこへ行くのかという問いに、機械的で読み取れる答えを負っているということです。

その結果が、時間を軸に築かれたプロトコルです。パフォーマンス・サイクルが開き、一筆で満たされ、カウントダウンが尽きると閉じます。一筆は小さなオンチェーンの行為です。ETHまたはCSTを携え、短いメッセージや添付

されたアセットを携えることもあり、サイクルの確定時刻をさらに未来へ押し出します。カウントダウンが切れたときに一筆が最後に立っている参加者——最後の一筆——がサイクルを確定します。確定は準備金を配り、サイクルのNFTを刻印し、次のサイクルを準備します。

三つの性質が設計を支えています。

- 決定論。アートワークは、刻印時にオンチェーンに記録されたシードから計算されます。レンダリングパイプラインはオープンソースで、同じシードは常に同じ画像と動画をビット単位で生みます。
- 機械的な分配。配分の割合は検証済みのコントラクトの中の定数です。参加者と分配のルールの間に裁量を持つアカウントは存在せず、一筆からETHを受け取るチームのウォレットもありません。
- チームの有限な役割。所有者の権限は狭く、サイクルの実行中はロックされ、残りのアップグレードが実現した後には完全に取り除かれる予定です。

本稿はプロトコルのリファレンスです。第2節は系の概略を描きます。第3節から第5節はサイクル、一筆、配分を規定します。第6節はアートを扱います。第7節から第10節はCST、係留、宇宙評議会、公共財を扱います。第11節はセキュリティと検証可能性を扱います。第12節と第13節はアップグレードの歴史と完全な分散化への道を記録し、第14節はプロトコルが何ではないかをはっきりと述べます。本稿で引用する数値はコントラクトの定数、またはオンチェーンのパラメーターの開始時の値です。付録Aに挙げるデプロイ済みのコントラクトが最終的な権威であり続けます。

2. プロトコルの概要

系は一つの中核コントラクトと、その周りを囲む狭く単一目的のコントラクトの環からなります。アップグレード可能なプロキシの背後にデプロイされた中核がサイクルを動かします。一筆の費用を決め、カウントダウンを追い、サイクル準備金を保持し、確定を実行します。その周りに、CSTトークン、Cosmic Signature NFTコレクション、配分のためのエスクローウォレット、二つの係留ウォレット、公共財金庫、広報準備金、そして宇宙評議会があります。

構成要素	役割
プロトコルコントラクト	パフォーマンス・サイクルを動かす：一筆の費用、カウントダウン、サイクル準備金、確定。
CST（ERC-20）	参加トークン。プロトコルだけが刻印し、一筆に使われると焼却され、委任されると調整ウェイトを表す。
Cosmic Signature NFT（ERC-721）	決定論的な三体アートワーク。確定時にだけ刻印され、シードはオンチェーンに保存される。
Random Walk NFT	同じチームによる以前のジェネラティブコレクション。一度だけの一筆の費用の引き下げと、別の係留星選トラックを与える。
配分ウォレット	二次的なETH配分と一筆に添付されたアセットのためのエスクロー。公開の受け取りタイムアウトを持つ。
係留ウォレット	Cosmic Signature NFT用（ETH係留配分）とRandom Walk NFT用（星選の対象資格）の二つ。
公共財金庫	サイクルごとの公共財配分を受け取り、送る。受け手は現在Protocol Guild。
広報準備金	コミュニティへの広報のために、サイクルごとに3,000 CSTを受け取る。
宇宙評議会	委任されたCSTが調整ウェイトを表す、オンチェーンの調整機関。

コントラクトの周りには、エコシステムが育っています。app.cosmicsignature.comのアプリ、NFTのためのAxiom Zeroマーケットプレイス、Arbitrum上のCSTのUniswap流動性、そしてサイクルの結果についての予測の場であるChaos Zero。どれも必須ではありません。本稿のすべての仕組みは、コントラクトに対して直接実行できます。

3. パフォーマンス・サイクル

サイクルとは時間の窓です。費用が下がっていく調律期間で開き、一筆で満たされ、サイクル確定時刻が切れて誰かがそれを確定すると終わります。本節は時計を扱い、第4節は一筆そのものを扱います。

3.1 開始とETH調律期間

各サイクルはETH一筆で開かなければならず、ETH調律期間がその費用を決めます。期間は、前のサイクルで実際に支払われた開始費用の2倍から始まり、その開始値の200分の1に1 weiを加えた下限へ線形に下がります。開始時のパラメーターでは、下降にはおよそ二日かかります。その長さはサイクルの時間増分に結びついているので、プロトコルが年を重ねるにつれてゆっくり伸びます。誰も一筆を入れる前に期間が完全に経過すれば、費用は単に下限に留まります。最初のサイクルは固定の0.0001 ETHで開きました。

この開始の仕組みは、注文板なしに価格の発見を行います。前のサイクルの開始が安すぎたなら、倍にすることで余地が戻ります。倍にした値が高すぎると分かれば、二日間の下降が誰かが始めてもよいと思う水準を見つけます。

3.2 カウントダウン

最初の一筆が時計を動かし、開始時のパラメーターではサイクル確定時刻をおよそ24時間先に設定します。その後のすべての一筆は、ETHであれCSTであれ、保存された確定時刻に現在の時間増分を加えます。増分はちょうど一時間から始まり、確定したサイクルごとに1%ずつ大きくなるので、サイクルは徐々に長くなり、NFTの刻印のペースは年月とともに遅くなります。一筆が届き続ける限り、サイクルの長さに固定の上限はありません。実際には、上がっていく一筆の費用が無期限の延長を高価なものにします。

延長は現在の瞬間ではなく、保存された時刻に適用されます。カウントダウンが切れた後、確定が実行される前に入れられた一筆は、保存された値に1増分を加え、最後の一筆の位置を引き継ぎます。時計をやり直すことはありません。

3.3 確定と公開確定期間

サイクル確定時刻が切れると、最後の一筆を入れた参加者が確定できるようになります。確定は一つのトランザクションです。プロトコルのETH残高を読み取り、第5節の配分トラックを配り、サイクルのNFTとCSTを刻印し、各新しいアートワークのシードを記録し、次のサイクルを予定します。

最後の一筆の参加者はこの権利を48時間、独占的に保ちます。その後、公開確定期間が始まります。誰でも確定でき、コントラクトは確定した人を、その役割が携えるすべて——シグネチャー配分のETHの分、そのCSTの刻印、そのNFT、添付されたアセットへの優先権——とともにサイクルの受領者として扱います。このルールは意図的に容赦のないものです。参加者が消えてもプロトコルを生かし続け、不注意に値段を付けます。二日以内に動かなかった受領者は、その役割を最初に呼び出す人に開け放したのです。

確定の後、次のサイクルは短い遅延——既定では30分——を経て有効になり、その調律期間が開きます。

4. 一筆

一筆はプロトコルの唯一の入力です。通貨にかかわらず、それぞれがカウントダウンを延ばし、サイクルの参加者の星選に1件の対象を記録し、第5.2節の持久の時計を更新し、第7.1節に述べるとおり参加CSTを刻印することがあります。

4.1 ETH一筆

最初の一筆の後、ETH一筆はそれぞれ次のETH一筆の費用を1%と1 weiだけ上げます。この数列は公開されていて正確です。誰でも動く前にコントラクトから現在の費用を読み取れます。ダスト閾値を超える過払いは同じトランザクションの中で返されます。その閾値より下では、返金は戻す額よりガス代のほうが高くつくので、差額は準備金に残ります。

4.2 Random Walk NFTの添付

Random Walk NFTを持つ参加者は、それを1回のETH一筆に添付して、その一筆の費用を50%引き下げられます。NFTは移転されません。コントラクトがそれを使用済みとして印を付けます。各Random Walk NFTはすべてのサイクルを通じてちょうど一度だけ添付できるので、この引き下げは消費される資源であり、固定された外部のコレクションをプロトコルの経済に結びつけます。

4.3 CST一筆

CSTは二つ目の入り口を与えます。CST調律期間は、前のCST一筆で支払われた費用の2倍——ただし200 CSTを下回らない——から始まり、期間の長さをかけてゼロへ線形に下がります。すべてのCST一筆は新しい開始値から期間をやり直し、使われたCSTは焼却され、供給量から永久に除去されます。

期間の長さそれ自体が生きたパラメーターで、プロトコルのより静かなフィードバックループの一つです。それは12時間の基準から始まりました。ETH一筆はそれぞれ約0.398%短くし、CST一筆はそれぞれ約0.4%長くします。したがって、ETHの活動が盛んならCSTの下降は速まり、CST一筆はより早く魅力的になります。CSTの活動が盛んならまた遅くなります。このループは、すべてのサイクルを二つの通貨のバランスの取れた混合へそっと押しやります。

下降はゼロに達しうるので、長い静かな時間はCST一筆をほぼ無償にすることがあります。それは意図的です。わずかなCST残高でも持っている誰かによってサイクルが常に延ばせることを保証し、すべてのCST一筆での焼却がトークンの供給量を実際の使用に結びつけます。CST一筆を送信する参加者は受け入れる最大の費用を指定するので、想定より遅れて届いた一筆が承認された額より多く使うことはありません。

すべてのサイクルの最初の一筆はETHでなければなりません。CST一筆は二つ目の一筆から使えます。

4.4 メッセージと添付されたアセット

一筆は、それとともにオンチェーンに記録される最大280バイトのメッセージを携えることができます。一筆はERC-20トークンやERC-721 NFTを添付することもできます。添付されたアセットはETH準備金には加わりません。配分ウォレットが保管し、確定後はサイクルの受領者がそれらを受け取る優先権を持ちます。第5.4節の公開の受け取りタイムアウトに従います。

5. サイクル準備金と配分トラック

一筆に支払われたすべてのETHは、前のすべてのサイクルの準備金のおよそ半分とともに、プロトコルのコントラクトに積み重なります。この残高がサイクル準備金です。確定はそれを一度読み取り、その固定の割合を配ります。

5.1 確定時の分配

ETHトラック	サイクル準備金の割合	受領者
シグネチャー配分	25%	サイクルの受領者。通常は最後の一筆の参加者。
時の戦士配分	8%	最も長く在位した持久チャンピオン（第5.2節）。
公共財配分	7%	公共財金庫を通じてProtocol Guildへ。
係留配分	6%	係留中のCosmic Signature NFTへ、比例して。
ETH星選	4%	サイクルの一筆のプールから選ばれた3件の対象が、金額を等しく分け合う。
累積準備金	約50%（残り）	次のサイクルへ持ち越される。

割合は、確定の瞬間のプロトコルの*ETH*残高に対して読み取られます。

配られる五つのトラックの合計は準備金の半分です。残りは累積します。プロトコルは引き出すのではなく蓄えていき、各サイクルは前より大きな準備金で開きます。Cosmic Signature NFTが一つも係留されていない状態でサイクルが確定すれば、そのサイクルの係留配分は飛ばされ、その分も累積します。

CSTとNFTのトラック	分配	受領者
シグネチャー配分	1,000 CSTとNFT 1点	サイクルの受領者。
時の戦士	1,000 CSTとNFT 1点	時の戦士。
持久チャンピオン	1,000 CSTとNFT 1点	持久チャンピオン。
最後のCST一筆	1,000 CSTとNFT 1点	サイクルの最後のCST一筆を入れた参加者。
NFT星選	1,000 CSTとNFT 1点、10回	一筆のプールから選ばれた10件の対象。
係留NFT星選	1,000 CSTとNFT 1点、10回	係留中のRandom Walk NFTにわたる10回の選定。
広報準備金	3,000 CST	コミュニティへの広報（第7.1節）。

したがって標準的なサイクルは、固定の分配として24点のCosmic Signature NFTと27,000 CSTを刻印し、それに加えて、個々の一筆が途中で刻印した参加CSTがあります。CST一筆のないサイクルは最後のCST一筆のトラックを飛ばし、係留中のRandom Walk NFTのないサイクルは係留星選を飛ばします。

5.2 持久チャンピオンと時の戦士

二つのトラックは位置ではなく持続を測ります。持久チャンピオンは、サイクルの間に最新の一筆の主として最も長く途切れずに留まった参加者です。一つの一筆が持ちこたえた、最も長い静かな間隔です。時の戦士は一段上にあります。持久チャンピオンの称号そのものを最も長く途切れずに保った参加者です。

この区別は微妙ですが、本物です。静かな午後に一筆を入れ、十時間追い落とされなかった参加者は、強い持久の間隔を打ち立てます。その参加者がサイクルをその時の戦士として終えるかどうかは、別の参加者がそれを上回るまでにその記録がどれだけ長く立っているかによります。持久は自分が作った間隔を測り、時の戦士のトラックは自分の記録がどれだけ長く持ちこたえたかを測ります。どちらも確定時にだけ決着します。

5.3 星選

各一筆は、サイクルの参加者の選定プールに1件の対象を記録します。確定時、コントラクトはETH星選のために3件の対象を選び、それらが準備金の4%を等しく分け合います。またNFT星選のために10件の対象を選びます。選定は復元抽出で行われるので、同じ参加者が複数回選ばれることがあり、対象は入れた一筆の数に応じて増えます。選ばれる頻度は参加に比例します。

別の係留NFT星選が、係留中のRandom Walk NFTにわたって行われます。10回の選定で、各保有者が係留したNFTの数で重み付けされます。このトラックはCSTとCosmic Signature NFTだけを配り、ETHは携えません。

これらの選定の背後にある乱数は、確定時にオンチェーンで構成されます。第11.3節がその源と限界を述べます。

5.4 配送、エスクロー、タイムアウト

分配は意図的にプッシュとプルに分けられています。シグネチャー配分のETHは確定の間に受領者へ直接送られ、公共財への送付も同様です。時の戦士のETHとETH星選の分け前はエスクローコントラクトである配分ウォレットに置かれ、各受領者が都合のよいときに受け取ります。CSTとNFTは確定の間に受領者へ直接刻印されます。

エスクローされた配分と添付されたアセットは5週間待ちます。その後、コントラクトは未受け取りの配分を誰でも自分のものとして受け取ることを許します。このルールは公開確定期間と対になっています。プロトコルの中に不在の参加者を永遠に待つものはなく、すべての分配はいずれそれを望む手に届きます。早めに受け取ってください。

6. アート：決定論的な三体シグネチャー

すべてのCosmic Signature NFTは重力三体問題のレンダリングです。同程度の質量を持つ三つの天体が、ニュートン重力のもとで軌道を描きます。三体問題には一般的な閉形式の解がなく、その軌跡はカオスです。初期条件の知覚できないほどの違いが、まったく異なる舞を生みます。そのカオスがコレクションの原動力です。シードが初期条件を決め、残りは物理が行い、二つのシグネチャーが同じになることはありません。

どの段階にも生成モデルは関わっていません。学習データも、サンプリングも、プロンプトもありません。パイプラインは物理シミュレーションとそれに続くレンダラーで、Rustで書かれ、オープンソースとして公開され、完全に決定論的です。

6.1 パイプライン

- シード。刻印時に、コントラクトはオンチェーンのデータ（第11.3節）から32バイトのシードを導き、NFTとともに保存します。シードはSHA3-256乱数生成器を初期化し、下流のすべてはその純粋な関数です。
- シミュレーション。10万通りの候補配置が、4次ヨシダ・シンプレクティック積分器を使ってそれぞれ100万の物理ステップで積分されます。この積分器は長い時間にわたって系のエネルギーの振る舞いを保ちます。
- 選抜。ボルダ集計が、カオスと天体が作る三角形の正三角形度で候補を採点し、プールから最も視覚的に興味深い軌道を選びます。
- カメラ。ゆっくりとした楕円軌道のカメラの揺らぎが視点を軌道の中で動かし、各シグネチャーに映画のような視差を与えます。
- 色。色は知覚的なOKLab空間で、天体ごとに120度の色相差を持って混ぜられ、揺らぎと正弦波で変調されます。
- スペクトルレンダリング。380から700ナノメートルにわたる64の波長ビンが、速度に応じた太さと被写界深度で軌道の軌跡を描きます。
- 仕上げ。AgXトーンマッピング、ブルーム、OpenSimplexの星雲レイヤー、カラーグレーディングがフレームを完成させます。

すべてのNFTの出力は、16ビットPNGと30秒のH.265動画です。

6.2 再現性とライセンス

決定論は前提ではなく、強制されています。同じシードは、どのマシンでもピクセル単位で同じ画像を生み、生成されたフレームのSHA-256ハッシュは継続的インテグレーションで検証されます。すべてのシードがオンチェーンに保存され、パイプラインが公開されているので、コレクションはどのサーバーにも依存しません。すべてのサーバーが明日消えても、すべてのシグネチャーはチェーンから再生成できます。

所有者は最大32バイトの名前をNFTにオンチェーンで付けられます。プロジェクト所有のコントラクト、シェーダー、レンダリングパイプラインはCC0 1.0で提供され、権利は一切留保しません。第三者の依存関係はそれぞれのライセンスを保持します。

7. CSTトークン

CSTはプロトコルのERC-20トークンです。供給量はゼロから始まり、トークンコントラクトは刻印と焼却の指示をプロトコルのコントラクトからだけ受け付けます。流通しているすべてのCSTは、サイクルへの参加にさかのぼれます。

7.1 刻印のルール

CSTは三つの流れを通じて流通に入ります。参加CSTは、下の式によって一筆の時に刻印されます。功労CSTは確定時に刻印されます。1,000 CSTがサイクルのNFTの分配のそれぞれ——標準的なサイクルでは24件——に伴います。最後に、サイクルごとに3,000 CSTが広報準備金へ行き、チームがコミュニティへの広報に使います。これはチームが振り向ける唯一の繰り返しのCSTの流れで、特別な権限は伴いません。

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

一筆が刻印する参加*CST*。経過時間は前の一筆から測り、現在のサイクルの時間増分に対して尺度化されます。

平たく言えば、量は前の一筆からの時間の平方根とともに増えます。最後の一筆の1秒後に届く一筆はほとんど何も刻印しません。一日の沈黙を終わらせる一筆は数百のCSTを刻印します。

前の一筆からの時間	参加CST
0 seconds	0
1 second	1.73
60 seconds	13.4
1 hour	104
1 day	509

開始時の時間増分であるちょうど*1*時間で計算しています。増分が大きくなるにつれて量はわずかに下がります。アプリのライブプレビューとコントラクトが基準です。

7.2 焼却と供給量の動態

CSTは使われるたびに流通から離れます。すべてのCST一筆の費用の全額が焼却されます。したがって供給量は振る舞いによって形づくられます。静かなサイクルはわずかな参加CSTしか刻印せず、活発なCSTの使用は供給量を焼き戻し、固定の功労と広報の流れは標準的なサイクルごとに予測できる27,000 CSTを加えます。上限も、事前刻印も、チームへの配分もありません。

平方根の式はそれ自体が供給の制御で、V2アップグレード（第12.2節）で導入されました。元の設計は一筆あたり一律100 CSTを刻印し、機械の速さの一筆の連続を新しいCSTの無限の源にしてしまいました。現在のルールのもとでは、連続する一筆の一斉射はおよそゼロを刻印し、忍耐強い参加が供給を生みます。

7.3 調整ウェイト

CSTは宇宙評議会（第9節）のウェイトトークンでもあります。ウェイトは委任によって有効になります。保有者は自分または別のアドレスへ委任し、それから各CSTは1単位の調整ウェイトを表します。トークンはタイムスタンプに基づくチェックポイントを使うので、提案のスナップショットはブロック番号ではなく実時間を参照します。

8. 係留

係留は、プロトコルにおける長期的な結びつきの形です。所有者はCosmic Signature NFTをプロトコルに係留できます。係留されている間、それは各サイクルの6%の係留配分の比例した分け前を積み上げます。積み上がったETHは係留を解除したときに受け取ります。固定期間もペナルティもありませんが、係留はNFTごとに一度だけの判断です。各NFTを係留できるのは生涯で一度だけなので、解除するとそのNFTの係留資格は永久に終わります。

「一度だけ」のルールは、通常のロックのスケジュールを一回限りの取り消せない選択に置き換え、係留された集合に本物の退出コストを与えます。NFTを係留し続けるかどうかはサイクルごとの生きた判断であり、解除するかどうかは永久の判断です。

Random Walk NFTは別に、別の目的で係留されます。係留中のRandom Walk NFTは係留NFT星選（第5.3節）で選定を受け、サイクルごとに10回、それぞれが1,000 CSTとCosmic Signature NFTを携えます。Random Walkの係留はETHの配分を携えません。同じ「一度だけ」のルールが当てはまります。

9. 宇宙評議会

宇宙評議会はプロトコルのオンチェーンの調整機関で、監査済みのOpenZeppelin Governorフレームワークの上に、CSTをウェイトトークンとして築かれています。委任されたウェイトが100 CST以上あるアドレスは誰でも調整提案を提出できます。提案は2日間の調整の遅延を待ち、その後2週間の調整の期間の間、開かれたままになります。

提案は二つの条件が成り立つときに成立します。支持が反対を上回ること、そして支持と棄権のウェイトの合計が総CST供給量の3%という調整定足数に達することです。反対のウェイトは定足数に数えられません。ウェイトの表明は暗号学的な行為であり、株式や持分の証書ではなく、委任はいつでも変えられます。

現在、評議会はチームの限定された所有者の役割と並んで調整を行っています。第13節の分散化のステップの後は、それがプロトコルの持つ唯一の調整の層になります。

10. 公共財

すべてのサイクルはサイクル準備金の7%を公共財金庫へ送ります。その受け手は現在Protocol Guild——170人以上のEthereumコアプロトコル貢献者の共同資金支援メカニズム——です。送付は確定の一部としてオンチェーンで強制されます。それを守るかどうかをサイクルごとに誰かが決めることはありません。プロトコルが使われるほど、Ethereum自身が依存するインフラへ多くが流れます。

理由は単純です。Cosmic Signatureが存在するのはEthereumのベースレイヤーが動き続けているからであり、公開のインフラの上で生きるプロトコルは、他のすべてと同じやり方でそれを支えるべきです：機械的に、予定どおりに、公開の場で。金庫はまた、どのサイクルの外でも、自発的なETHの拠出を直接受け付けます。

> これは公共財のアドレス（現在はProtocol Guild）へのETHの送付です。米国の税法上の慈善寄付や寄付ではなく、Cosmic Signatureはいかなる法域においてもその税務上の扱いについて何も表明

しません。

11. セキュリティ、乱数、検証可能性

11.1 独立したレビュー

2025年後半、HackenはCosmic Signatureのコントラクトの独立したセキュリティレビューを実施しました。対象は中核プロトコル、CSTトークン、二つのNFTの統合、係留ウォレット、そして支えるウォレットとシステム管理のコントラクトです。2026年1月に公開された最終報告書には23件の所見が挙げられています。重大なし、高い深刻度なし、中程度3件、低8件、情報提供12件で、ほとんどは書面の理由づけとともに検討され受け入れられた設計上のトレードオフです。

手動のレビューに加えて、Hackenは14のシステム不変条件をファジングテストしました。たとえば、プロトコルのETH残高が常に受け入れた額から配った額を引いたものに等しいという性質などです。14件すべてが10,000回の実行にわたって成立しました。報告書の全文は公開されており、参考文献にリンクしています。

外部のレビューのほかに、リポジトリはCertoraの形式検証仕様、Solidity SMTCheckerの構成、Slitherの静的解析、そしてSolidityソースの完全なカバレッジを目指すテストスイートを備えています。

11.2 防御的な設計

- 再入防止ガードが中核コントラクトのすべての外部エントリーポイントを守ります。
- プッシュよりプル：二次的なETH配分と添付されたアセットは、確定の間に送られるのではなくエスクローに置かれるので、どの受領者のコントラクトもサイクルの閉鎖を妨げられません。
- 失敗に寛容な送付：公共財への送金が完了できなくても、確定はそのまま進み、イベントは後の処理のために記録されます。
- サイクル間のロック：サイクルの実行中は、中核パラメーターの変更とコントラクトのアップグレードは不可能です（第13節）。

11.3 乱数

プロトコルは乱数を二度必要とします。確定時の星選の選定と、各新しいNFTのシードです。前のブロックハッシュ、現在のベースフィー、そしてArbSysとArbGasInfoプリコンパイルからのArbitrum固有のエントロピー——前のArbitrumブロックハッシュ、ガスのバックログ、L1価格のカウンター——を折り合わせて、オンチェーンでシードを組み立てます。個々の値は、そのシードからkeccak256で引き出されます。プリコンパイルの呼び出しは失敗に寛容で、一つが利用できなければ、構成は残りの源にフォールバックします。

これは意図的な最小主義です。オラクルも、外部の委員会も、サイクルを立ち往生させかねないコールバックもありません。トレードオフははっきりと述べられています。シーケンサーは原理的にブロックレベルの入力に影響しうるもので、設計はその影響が届きうる範囲を限ります。星選の選定とアートのシードだけが乱数の消費者であり、カウントダウン、一筆の費用の数列、第5節のすべての割合は決定論的です。構成は確定ごとに一度だけ消費され、確定は誰でも送信できる公開のトランザクションです。

11.4 オープンな検証

すべてのコントラクトは、付録Aに固定されたアドレスで、Arbitrum One（チェーン42161）についてSourcifyで完全一致のソース検証済みです。アートパイプラインの決定論は、レンダリングされたフレームのSHA-256ハッシュによって継続的インテグレーションで検証されます。プロジェクト所有のコードはCC0です。誰でもコントラクト、レンダラー、サイトをフォークでき、誰でもシードから再生成することでどのシグネチャーも確認できます。

12. デプロイの歴史と今後の道

Cosmic Signatureは完成するように設計されています。アップグレード可能性があるのは、プロトコルの初期に観察された振る舞いに対して仕組みを修正できるようにするためで、設計が終わるときにそれも終わります。本節は、何が出荷され、何が残っているかを記録します。

12.1 V1：ローンチ

V1はUUPSアップグレード可能プロキシの背後で、プロトコルをArbitrum Oneにローンチしました。サイクル、一筆、配分トラック、係留、評議会、アートパイプライン——本質的には本稿に述べるとおりです。アップグレードには所有者が必要で、サイクルの間にだけ可能です。どんな状況であっても、サイクルの途中でコントラクトを変える仕組みは意図的に存在しません。

12.2 V2アップグレード、現在稼働中

V2は現在デプロイされている実装です。五つの変更を行い、それぞれが観察された、または予期された振る舞いへの応答です。

- 動的な参加CST。一筆あたり一律100 CSTは、第7.1節の平方根の式になりました。一律の刻印は連続する一筆を無償のCSTに変えていました。新しいルールは頻度ではなく忍耐によって刻印します。
- 最小刻印の保護。すべての一筆の方法に、参加者が受け入れる最小の参加CSTの量のパラメーターが加わり、署名と実行の間のタイミングのずれから参加者を守ります。
- 生きたCST調律期間。期間の長さは一筆の混合に反応する保存された値になり（第4.3節）、ETHとCSTの道筋が互いにバランスを保ちます。
- より長い優先期間。最後の一筆の参加者の優先確定期間は24時間から48時間に延びました。
- タイミングと算術の強化。カウントダウンの延長はいまでは常に保存された確定時刻に適用され、期限切れ後のほぼ無償のCST一筆が期限を繰り返し外へ押し出せた抜け穴を閉じました。次のサイクルを予定する算術も強化され、どれほど極端なパラメーターの構成であってもサイクルの確定を妨げられないようになりました。

12.3 計画されているV3アップグレード

公開リポジトリで現在開発中のV3は、ちょうど一つのことを変えます。遅れて動くことの費用です。サイクル確定時刻の前の最後の20分の間、すべての一筆の費用——ETH、Random Walk NFT付きのETH、CSTのいずれであっても——に、1倍から10倍へ多項式的に上がる割増が掛けられます。割増は期限で10倍に達し、延長時間に入れられたどの一筆に対してもそのまま留まります。

`m(t) = 1 + 9 · (t / T)^8、 こ こ でT = 20分`

サイクル終盤の費用の割増。*t*は最後の*20*分の期間の中で経過した時間。

指数が重要です。勾配が8次なので、割増は期間のほとんどでほぼ見えず、最後の最後でだけ急になります。期限の10分前でおよそ1.04倍、5分前でおよそ1.9倍、1分前でおよそ7倍、ゼロで10倍です。

狙いは終盤を変えることです。V2のもとでは、最後の数秒まで待って一筆を入れることはほぼ無償なので、サイクルは中身の薄いタイミングの応酬で終わることがあります。V3のもとでは、最後の瞬間の一筆は高価な意思表示であり、サイクルを通じた持続的な参加は相対的に安く、第5.2節の持久のトラックは奇襲がはるかに難しくなります。正確なパラメーターはデプロイ前に調整されるかもしれませんが、仕組みは述べたとおりです。

13. 完全な分散化への道

プロトコルには現在、所有者がいます。それをデプロイしたアドレスです。この役割は本物であり、本稿はそれを小さく見せません。それはまた、構造上狭く、約束によって一時的なものです。

サイクルの実行中、中核パラメーターはロックされます。所有者はサイクルの途中で割合、増分、費用を変えられず、コントラクトをアップグレードすることもできません。所有者の操作はサイクルの間の隙間に限られます。三つのより狭い権限はいつでも使えます：次に来るサイクルの有効化を延期すること（ただしその最初の一筆が届くまで）、次のサイクルまでの遅延を調整すること、そして周辺のコントラクト——公共財金庫の受け手、NFTメタデータのURI、エスクローの受け取りタイムアウト——を管理することです。どの所有者の権限も、エスクローされた配分、刻印されたNFT、記録されたシード、誰かのCSTの残高には届かず、一筆からETHを受け取るチームのウォレットもありません。

これらの権限が存在するのは、仕組みが新しいからです。V2が存在するのは、実際の振る舞いがどんなシミュレーションも捉えられなかった教訓を教えたからで、V3が存在するのも同じ理由です。限られた公開の調整の時期こそ、設計を完成させる方法です。一覧の中で最も強い権限はアップグレードそのもので、それさえ公開されています。新しい実装は、次のサイクルが始まる前にオンチェーンで見え、検証できます。

それは次のように終わります。残りのアップグレード——V3を始めとして——が完了し、仕組みとトークンの設計が最終的なものと判断されたとき、特権的な管理はデプロイしたアドレスから完全に取り除かれます。所有者の役割は、宇宙評議会への移転か完全な放棄によってデプロイ者から永久に離れ、正確な仕組みは事前に告知されます。その時点から、どの私的な当事者もプロトコルをアップグレードしたりそのパラメーターを変えたりできず、デプロイしたアドレスは他のどのアドレスも持たないものを何も持ちません。残るのは、デプロイされたままのプロトコル、その調整の層としての評議会、そしてアートです。

この過程のすべての段階は、最後の一つも含めて、オンチェーンで公開されています。

14. 明確化とリスク要因

14.1 Cosmic Signatureではないもの

Cosmic Signatureは宝くじでも、カジノでも、ギャンブル商品でもありません。胴元も、ディーラーも、賭けもありません。参加者は参加そのものと価値を交換します。すべての一筆は、アートワークを形づくり、サイクルを延ばし、オンチェーンに永久に記録される表現の行為です。プロトコルはいかなる種類の運営者の取り分も持ちません。第5節のすべての配分トラックは、参加者、係留中のNFT、累積準備金、または公共財へ流れます。

Cosmic Signatureは投資商品ではなく、本稿のいかなる部分も投資助言や証券の募集ではありません。CSTとCosmic Signature NFTは参加とアートのための物です。プロトコルはそれらの価格、流動性、将来の価値について何も約束せず、他人の努力から利益を得る期待をもってそれらを取得するべき人はいません。

14.2 リスク要因

- スマートコントラクトのリスク。コントラクトはレビューされ、形式的に分析され、ソース検証されていますが、そのどれも保証ではありません。価値を保持するどんなソフトウェアにも、未知の欠陥は存在しうるものです。
- 乱数の限界。星選の選定はブロックから導かれたエントロピーを使います（第11.3節）。シーケンサーは原理的にそれに影響しうるもので、設計はその結果を限りますが、なくすことはできません。
- タイミングの責任。48時間の確定期間と5週間のエスクローのタイムアウトは現実の期限です。それを過ぎて受け取られなかった配分は、設計により、他の人が受け取れるようになります。

- パラメーターの変更。分散化のステップが完了するまで、第13節に述べるとおり、パラメーターはサイクルの間に変わることがあります。すべての変更は次のサイクルが始まる前に公開されます。
- アセットの変動。ETH、CST、NFTの価値は動きます。参加には実際のお金がかかります。一筆は参加とアートへの支出として扱い、金銭的な利得への道として扱わないでください。
- 規制の不確実性。デジタルアセットの法的な扱いは法域によって異なり、変化し続けています。

15. 結び

Cosmic Signatureは、誰の許可も、そしていずれは誰の世話も必要としないジェネラティブアート・プロトコルを築く試みです。仕組みは完全に規定できるほど小さいものです。費用が下がっていく期間、一筆が延ばすカウントダウン、固定の配分の割合、累積する準備金、そして物理とシードの純粋な関数であるアート。残るアップグレードはわずかで、公開されています。それが終われば所有者の役割は消え、残るのは本稿が述べるものです。時計、準備金、トークン、評議会、そして途切れることのないシグネチャーの連なり——その一つひとつが、それを形づくった手の記録です。

付録A：検証済みコントラクトアドレス

コントラクト	アドレス（Arbitrum One）
プロトコルコントラクト（プロキシ）	`0x6a714Ae7B5b6eA520F6BCA23d2E609C4Fd5863F2`
プロトコル実装（V2）	`0x50eB3d05d2C463949DE9238D419385594f7AdB97`
CSTトークン	`0xAD91843e6A58Ba560F577E676986AFb1dba6FBA0`
Cosmic Signature NFT	`0xbb84Be3500A63581d3F2d5AC3bdF8685AAedad25`
Random Walk NFT	`0x895a6F444BE4ba9d124F61DF736605792B35D66b`
宇宙評議会	`0xF3D52E1c681949be7E624778dB13DaD7F8c729db`
公共財金庫	`0x96bB0ADB414d5350f435E52f94946B6C7A0760a9`
広報準備金	`0xa3802c799f5e3D3D3562A9B513a41C6aAF92e25e`
配分ウォレット	`0xE1b619e9B39ea4109D2F429Ea5eAA307759b0011`
係留ウォレット、Cosmic Signature NFT	`0x6308A405B4FF1eA890870Efe2a6D036750B81F7C`
係留ウォレット、Random Walk NFT	`0x5EB3396092841E6c5b0b51141699F6711E830529`

すべてのコントラクトはチェーン*42161*について*Sourcify*で完全一致の検証済みです。プロキシのアドレスがプロトコルの永久のアドレスで、実装は第*12*節と第*13*節に述べる公開のアップグレード手続きを通じてのみ変わります。

付録B：パラメーター一覧

パラメーター	値
開始費用、最初のサイクル	0.0001 ETH（固定）
ETH調律期間の上限	前のサイクルで支払われた開始費用の2倍
ETH調律期間の下限	上限 / 200、加えて1 wei
ETH一筆の費用の上げ幅	ETH一筆ごとに1%、加えて1 wei
Random Walk NFTの引き下げ	50%、NFTごとに生涯一度
CST調律期間の上限	max(最後に支払われたCST費用の2倍、200 CST)
CST調律期間の下限	0 CST
CST調律期間の長さ	12時間の初期基準。ETH一筆ごとに約-0.398%、CST一筆ごとに+0.4%
最初の一筆の後の初期カウントダウン	開始時でおよそ24時間
一筆ごとの時間増分	開始時で1時間、サイクルごとに1%ずつ増加

パラメーター	値
確定の優先期間	48時間
エスクローの受け取りタイムアウト	5週間、その後は公開の受け取り
一筆のメッセージの上限	280バイト
ETH配分トラック	シグネチャー25%、時の戦士8%、公共財7%、係留配分6%、ETH星選4%
累積準備金	約50%が次へ持ち越される
NFTの分配ごとの功労CST	1,000 CST
サイクルごとの広報準備金	3,000 CST
サイクルごとの標準的な刻印	NFT 24点、固定CST 27,000 CST
評議会のパラメーター	提案のしきい値100 CST、2日間の遅延、2週間の期間、定足数3%
次のサイクルまでの遅延	既定で30分、所有者が調整可能

パラメーターが変化するか調整可能な場合は開始時の値を示しています。コントラクトがライブの値を報告します。

参考文献

1. Cosmic Signatureコントラクトのリポジトリ（ソース、テスト、検証ツール）. https://github.com/PredictionExplorer/Cosmic-Signature
2. Cosmic Signatureアプリ. https://app.cosmicsignature.com
3. Cosmic Signatureプロトコルサイト. https://cosmicsignature.com
4. Cosmic SignatureコントラクトのHackenセキュリティレビュー、2026年1月. https://hacken.io/audits/cosmic-signature/sca-cosmic-signature-cosmicsignature-contracts-oct2025/
5. Protocol Guildのドキュメント. https://protocol-guild.readthedocs.io
6. OpenZeppelin Governorのドキュメント. 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.