BTC算法艺术铭文平台

BTC递归铭文实现算法生成艺术

RKStone

BAStudio Co-Founder

算法生成艺术家

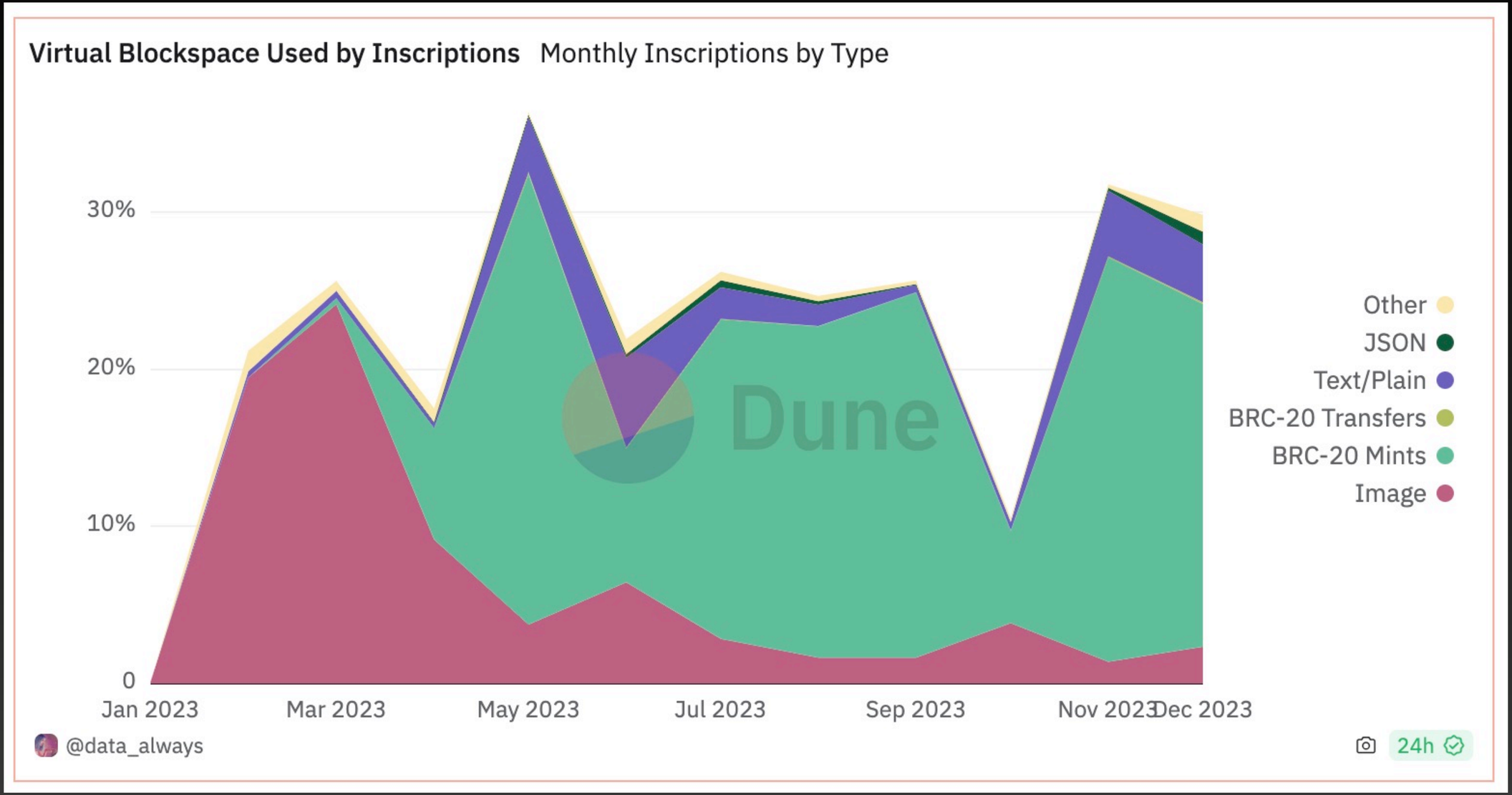
内容提要

1：BTC重要迭代及Ordinals铭文原理

2：算法生成艺术及市场回顾

3：BTC上实现算法生成艺术实现

从Bitcoin铭文Ordi说起



问题：BTC 网络是怎么支持NFT和BRC20的？

以太坊 NFT (基于ERC721) 由两部分组成：

1，(NF)Token，Token每个编号不同，发送到钱包交易

2，小图片，每个Token绑定一个图片，图片存在IPFS

NFT特征：可区分Token + 可辨识数字对象

序数协议基础条件1：Taproot 闪电网络

Bitcoin网络重要技术升级节点
1：2017 年比特币社区采用 SegWit（隔离见证）升级，对区块扩容做好技术准备。
2：2021 年 11 月 12 日比特币社区在区块 709,632 激活了 Taproot 升级，实现软分叉升级。

1：Taproot 实现了BTC三个的技术改进提案(BIP)：

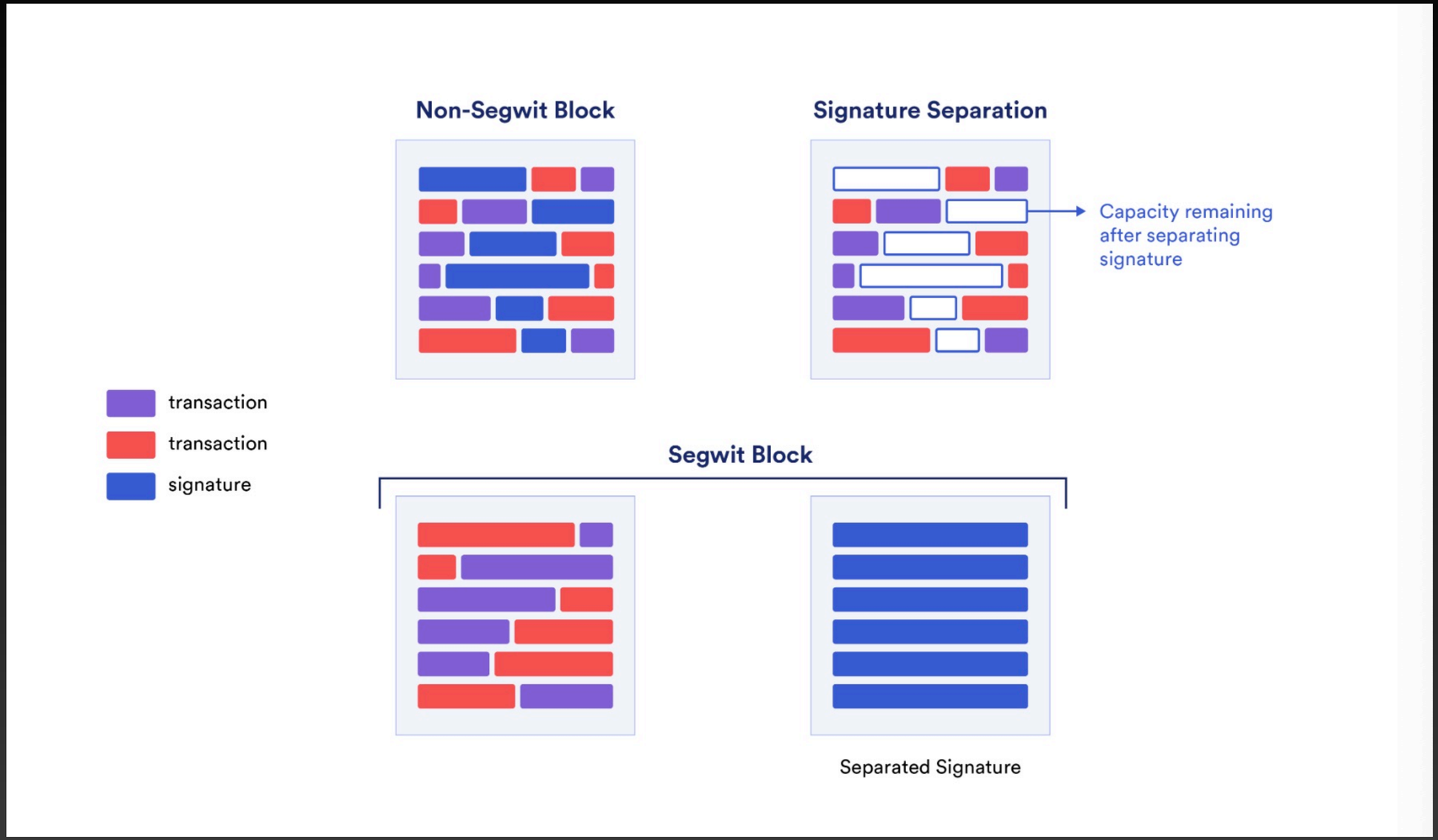
BIP 340、BIP 341 和 BIP 342

BIP 340：Schnorr Signatures 取代椭圆加密验证方式(ECDSA)。

BIP 341：脚本升级，可读取Schnorr签名，并实现MAST 和 P2TR能力。

BIP 342：将BTC脚本升级为Tapscript，使BTC脚本更新能力更加强大。

序数协议的基础条件 2：隔离见证



序数协议的执行原理

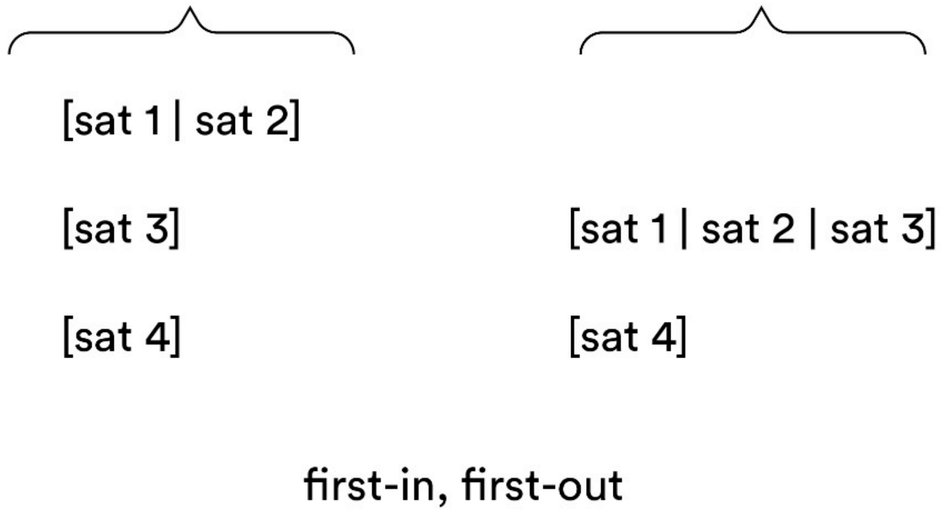
Ordinals Minted

Mining reward:
50 BTC

Ordinal numbering:
0-4,999,999,999

Bitcoin Genesis Block

Ordinals Transferred



交易所假铭文事件

sats & sats

```
mysql> SELECT @@character_set_database, @@collation_database;
+----------------------------+----------------------+
| @@character_set_database | @@collation_database |
+----------------------------+----------------------+
| utf8mb4                    | utf8mb4_0900_ai_ci   |
+----------------------------+----------------------+
1 row in set (0.00 sec)

mysql> select HEX('ratꜩ'), HEX(WEIGHT_STRING('ratꜩ')),HEX('rats'), HEX(WEIGHT_STRING('rats'));
+------------+-----------------------------+------------+-----------------------------+
| HEX('ratꜩ')  | HEX(WEIGHT_STRING('ratꜩ'))  | HEX('rats') | HEX(WEIGHT_STRING('rats')) |
+------------+-----------------------------+------------+-----------------------------+
| 7261CA     | 1E331C471E951E71            | 726174     | 1E331C471E951E71           |
+------------+-----------------------------+------------+-----------------------------+
1 row in set (0.00 sec)
```

没有正确区分开“ts”和这个特殊字符"ꜩ"

序数和铭文的理解

在BTC上有以下概念：

1，将BTC拆分编码，每个聪Sat单独编号(序数)，聪(Sat)就是(NF)Token。发送到钱包交易。

2，小图片，每个聪(Sat)绑定一个图片，图片存在BTC链上。这种小图片就是铭文。

可拓展到任意类型媒体，json(BRC20)，视频，音乐，js(代码)，html(艺术类)。

由此看到：序数协议+铭文 == 以太坊NFT（NFToken+小图片）

注：BRC20是Json铭文，本质上是一种NFT的特例应用。NFT可以作为FT使用，但FT不能做NFT。

理解：ERC404本质是NFT(721)的一种变体的用法，跟BTC NFT本质一致

序数和铭文内容： ord.io

INSCRIPTION

55,836,094

ID

7631f...c88i0

OWNED BY

Alien Gringos

FILE TYPE

HTML text/html;charset=utf-8

FILE SIZE

2.39 KB

CREATED

January 16, 2024, 4:23 PM GMT+8 22 hours ago

CREATION BLOCK

826,002

CREATION TRANSACTION

7631f...1fc88

CREATION FEE

48,774 sats

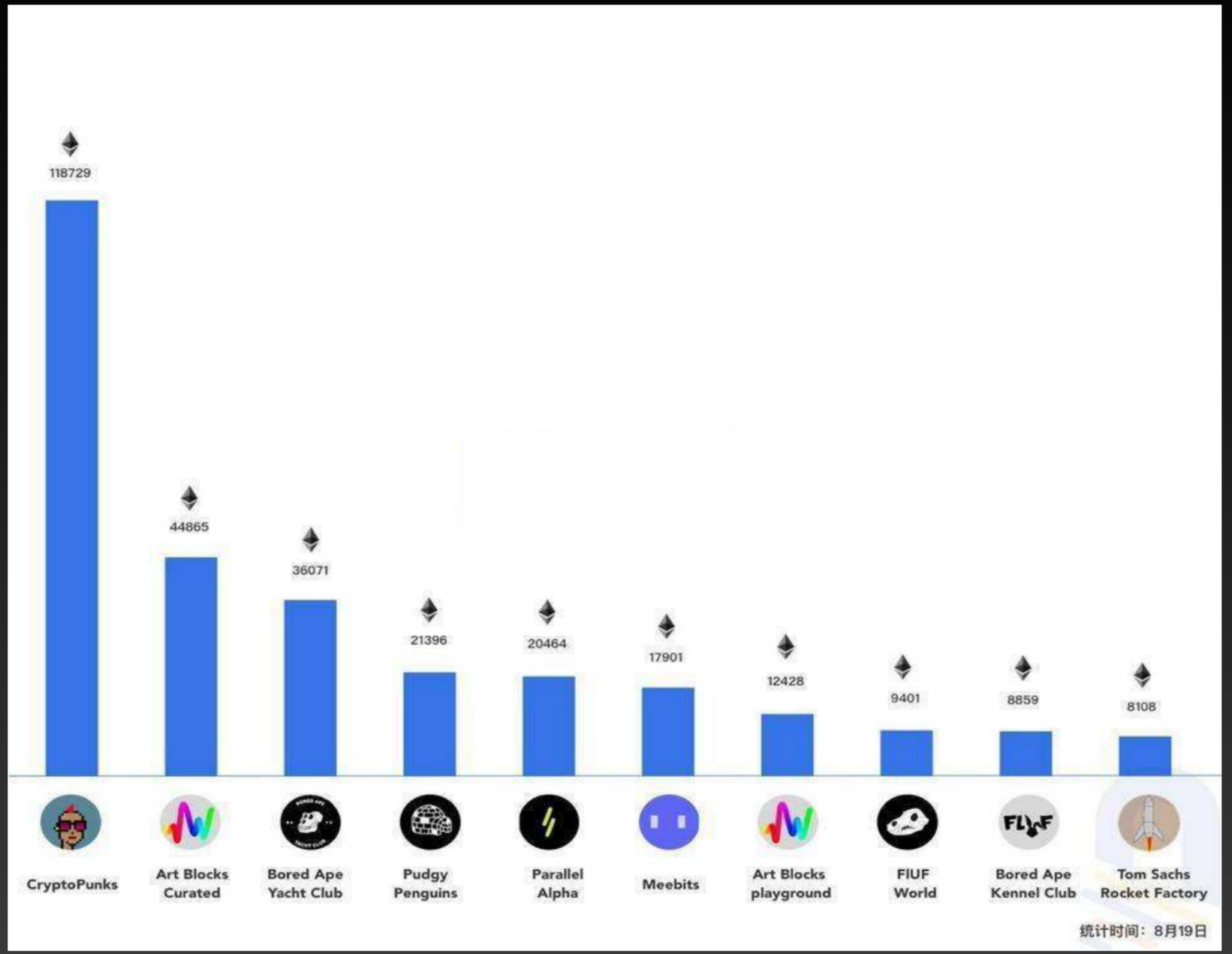
铭文上链代码片段 1：铭文内容写入脚本

```
const hex = $( '.file' ).innerText;
const data = hexToBytes( hex );
const script   = [
    pubkey, 'OP_CHECKSIG',
    'OP_0', 'OP_IF', ec.encode('ord'), '01', mimetype,
    'OP_0', data, 'OP_ENDIF' ];

const leaf       = await Tap.getLeaf(Script.encode(script));
const [ tapkey ] = await Tap.getPubkey(pubkey, [ leaf ]);

const redeemtx = {
  version: 2,
  input: [{
    txid: txid,
    vout: vout,
    prevout: { value: amt, scriptPubKey: '5120' + tapkey },
    witness: []
  }],
  output:[{
    value: amt - fee,
    scriptPubKey: decodedToAddress
  }],
  locktime: 0
}
```

铭文上链代码片段2： 签名发起上链铭刻

```
const sec = await Tap.getSeckey(seckey.raw, [ leaf ]);
const sig = await Sig.taproot.sign(seckey.raw, redeemtx, 0, { extention: leaf });
const cblock  = await Tap.getPath(pubkey, leaf);

redeemtx.input[0].witness = [ sig, script, cblock ];
var rawtx = Tx.encode(redeemtx);
var txid = await pushBTCpmt( rawtx );
```

2021年NFT交易数据回顾 ETH

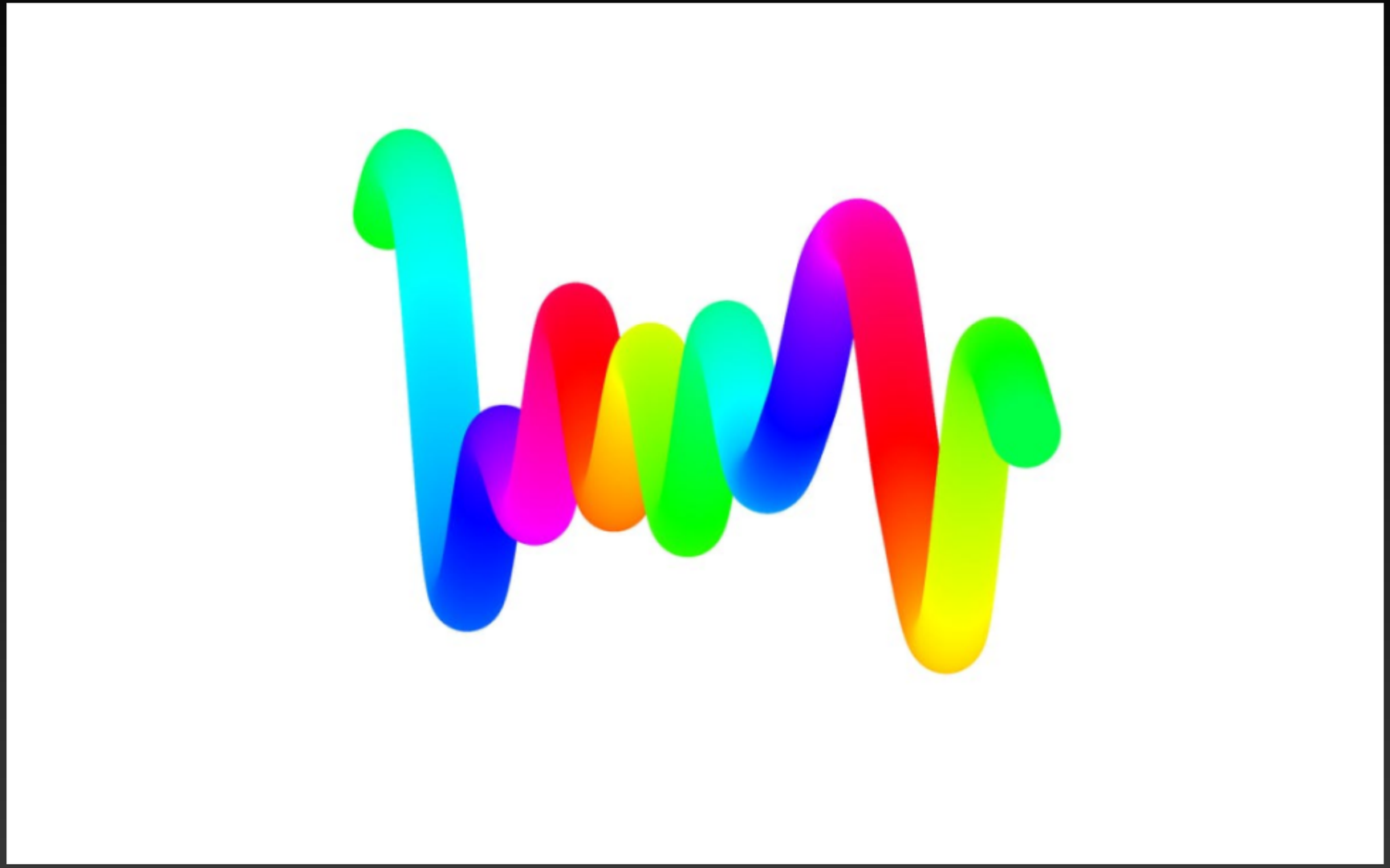


2021年NFT交易数据回顾 ETH

NFT Collectible Rankings by Sales Volume (24 hours)

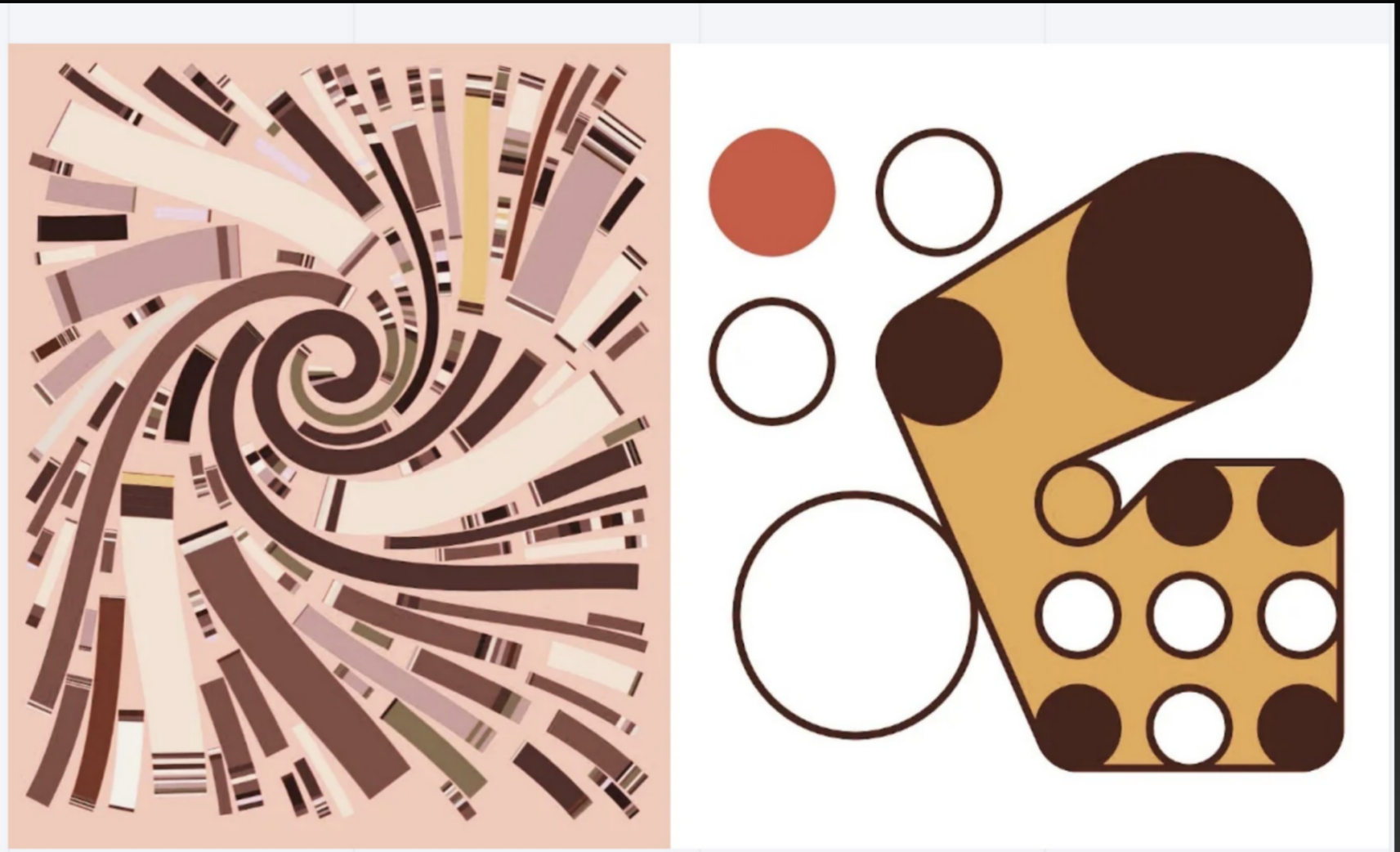
	Product	Sales	Change (24h)	Buyers	Txns
1	Art Blocks	$34,196,440	▲ 38.43%	1,271	2,207
2	CryptoPunks	$24,064,710	▲ 50.37%	58	71
3	Axie Infinity	$23,319,894	▲ 1.38%	22,974	59,152
4	Curio Cards	$12,598,437	▼ 7.32%	553	877
5	Bored Ape Yacht Club	$9,825,644	▼ 36.73%	50	58
6	0N1 Force	$6,141,958	▼ 46.24%	226	316
7	PUNKS Comic	$3,634,149	▲ 4.77%	117	190
8	Parallel Alpha	$3,123,266	▼ 3.52%	355	1,004
9	NBA Top Shot	$2,904,278	▲ 70.68%	5,795	28,915
10	Mooncats	$2,585,830	▼ 46.05%	297	465

算法生成艺术：基于算法和随机系统的的艺术形式创作，
以代码算法为基础，生成一定艺术性的图像或动画(非AI生成)



当代生成艺术作品，2021年

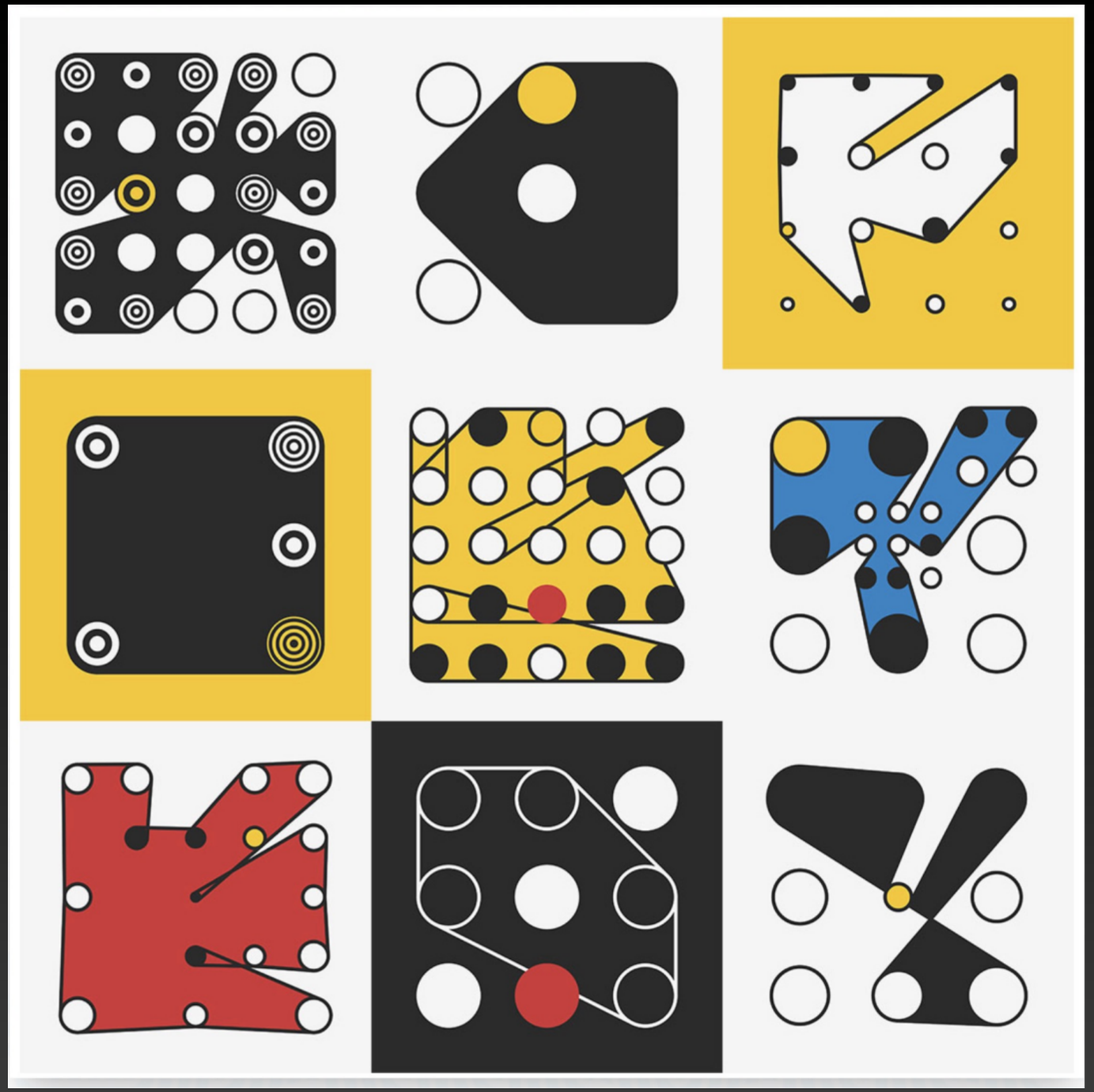
算法生成艺术：基于算法和随机系统的的艺术形式创作，
以代码算法为基础，生成一定艺术性的图像或动画(非AI生成)



Some Art Blocks NFTs are selling for millions. Image: Art Blocks

当代生成艺术作品，2021年

Ringers作品系列
ArtBlocks首发



BTC NFT是否也有这种机会?

1: NFT技术已支持

2: 对于高清图片，上链gas非常高。例如高清头像类

3: 对于算法艺术，由于只存储代码属性，非常适合BTC

递归铭文定义：(摘自ordinals官方文档)

Recursion 递归

Bticoin链上沙盒的一个重要用处就是是递归的使用：
允许访问 ord 的 /content 端点，允许铭文通过请求 /content/<INSCRIPTION_ID>.

这有许多的用例方式：

1: 重新混合现有铭文的内容。

2: 将代码、图像、音频或样式表片段发布为共享公共资源。

3: 生成式艺术收藏品，其中算法被铭刻为JavaScript，并从具有唯一种子的多个铭文中实例化。

4: 生成个人资料图片集，其中配件和属性被刻为单个图像，或在共享的纹理图集中，然后以拼贴风格组合，在多个铭文中以独特的组合。

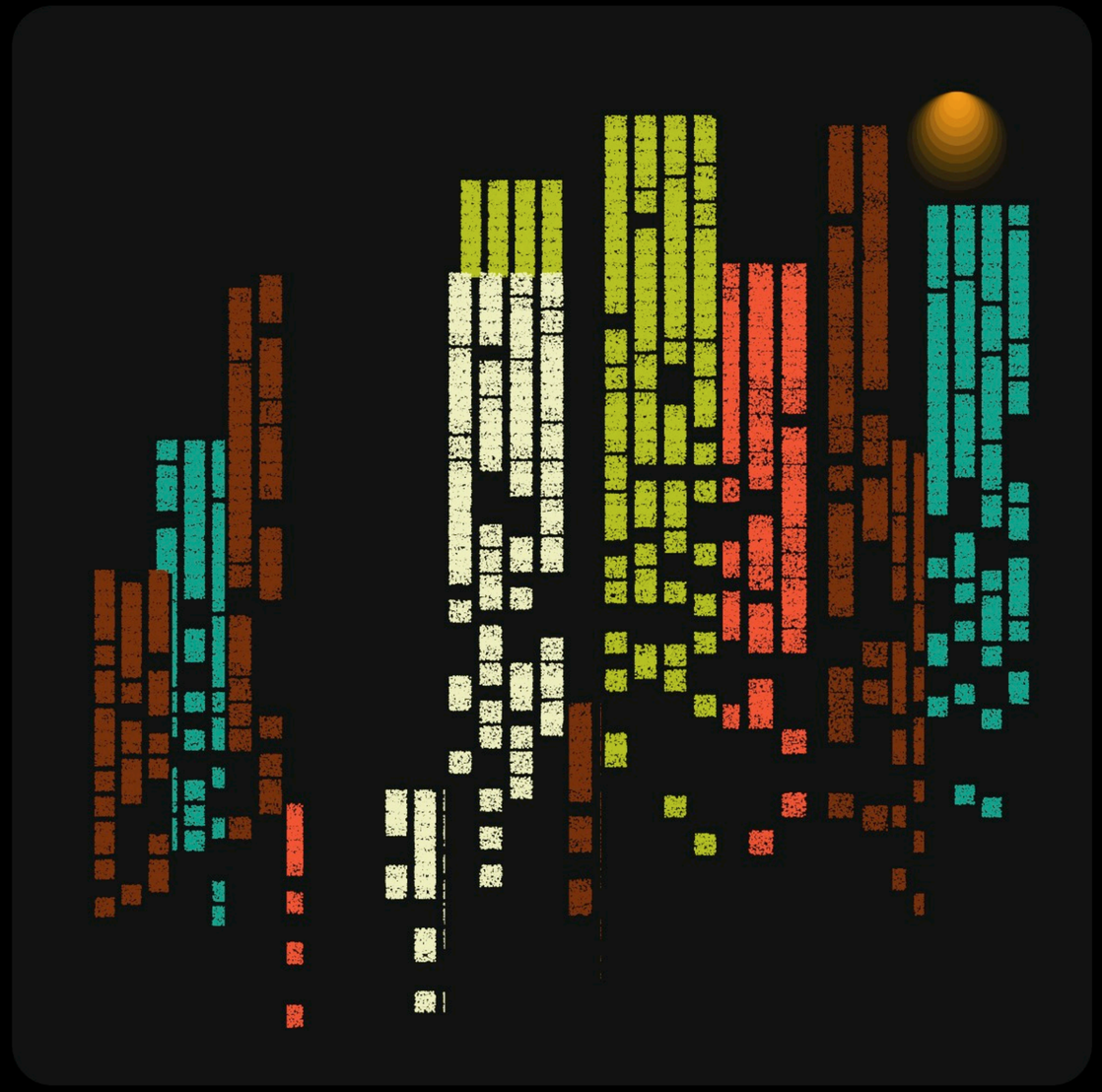
递归铭文实现方案

```
1
2  <html lang="en">
3
4  <head>
5    <meta charset="UTF-8">
6
7    <script type="module">
8      import * as fcompress from '/content/
         f815bd5c566c6e46de5cdb6ccb3a7043c63deeba61f4234baea84b602b0d4440i0';
9
10     async function getFileFromBase() {
11       const compressed = new Uint8Array(
12         await fetch('/content/
             c9752853f73dac8c805ed926735b191d957fddf87856d1462d6b29181726651 7i0').
             then(res => res.arrayBuffer())
13       );
14       const decompressed = fcompress.decompressSync(compressed);
15       const origText = fcompress.strFromU8(decompressed);
16       eval(origText);
17     }
18     getFileFromBase();
19   </script>
20
21   <script type="text/javascript" src="/
     content/36600ab5b10719877ea06d6c82dc75111207f3f544c2f4b869417db69d23feeci0">
22   </script>
23
24 </head>
25
```

递归铭文实现方案

```
25
26  <body>
27    <script type="text/javascript">
28
29      let type = 2;
30      let backShapecolor = 0;
31      let badPos = 1;
32      let mecolor = 240;
33      let blueshape = 1;
34
35      function setup() {
36        createCanvas(800, 800);
37        colorMode(HSB, 360, 100, 100);
38        rectMode(CENTER);
39        noLoop();
40      }
41
42      function draw() {
43        drawtheproj(type, badPos, mecolor, backShapecolor, blueshape);
44      }
45    </script>
46  </body>
47
```

递归铭文实现方案



0 0

INSCRIPTION

53,703,276

ID
e9e69...227i0

OWNED BY
rkstone

FILE TYPE
HTML text/html;charset=utf-8

FILE SIZE
1.27 KB

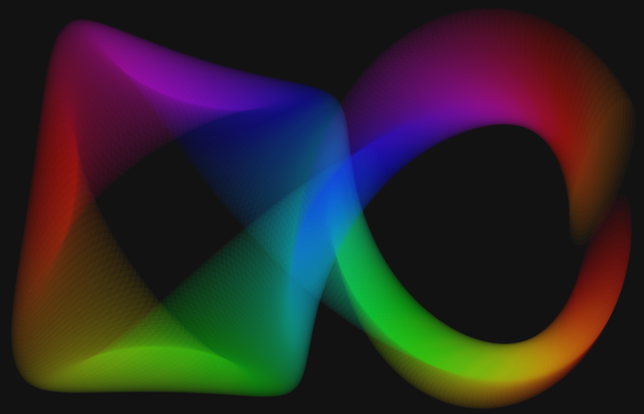
CREATED
January 8, 2024, 1:13 PM GMT+8 9 days ago

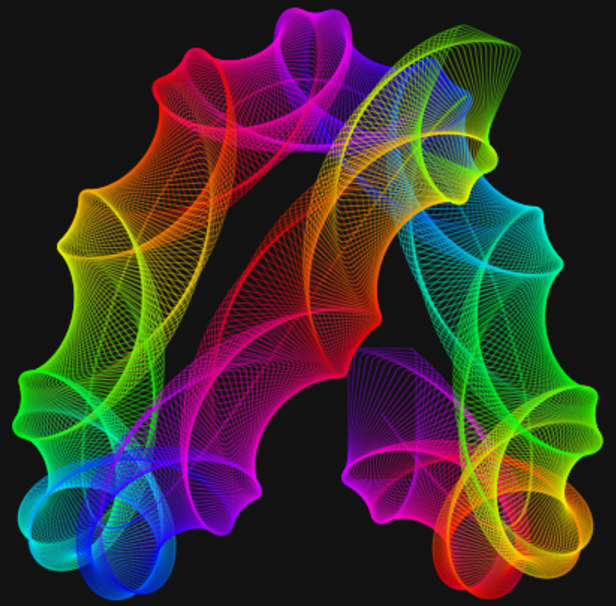
CREATION BLOCK
824,820

CREATION TRANSACTION
e9e69...b2227

CREATION FEE
31,212 sats

彩谱作品系列





RoseCurve 玫瑰曲线算法

Specification 规范 [edit]

A rose is the set of points in polar coordinates specified by the polar equation[2]

玫瑰是极坐标中由极坐标 [2] 指定的一组点

$$r = a\cos(k\theta)$$

or in Cartesian coordinates using the parametric equations

或使用参数方程在笛卡尔坐标中

$$\begin{aligned} x &= r\cos(\theta) = a\cos(k\theta)\cos(\theta) \\ y &= r\sin(\theta) = a\cos(k\theta)\sin(\theta) \end{aligned}$$

Roses can also be specified using the sine function.[3] Since

也可以使用正弦函数指定玫瑰。 [3] 因为

$$\sin(k\theta) = \cos\left(k\theta - \frac{\pi}{2}\right) = \cos\left(k\left(\theta - \frac{\pi}{2k}\right)\right).$$

Thus, the rose specified by $r = a\ \sin(k\theta)$ is identical to that specified by $r = a\ \cos(k\theta)$ rotated counter–clockwise by

因此，r = a sin（kθ） 指定的玫瑰与 r = a cos（kθ） 指定的玫瑰相同，逆时针旋转

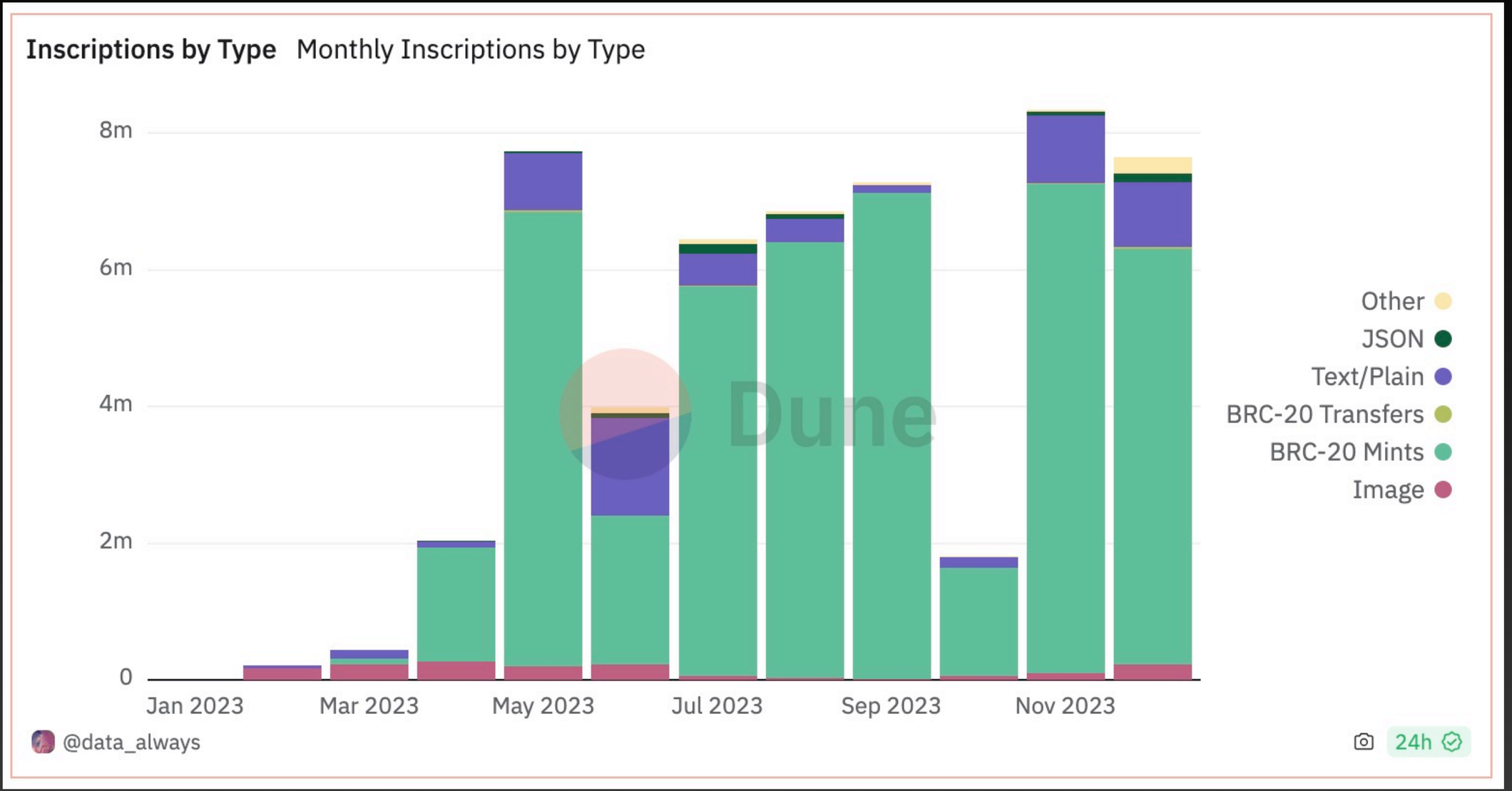
$\frac{\pi}{2k}$ radians, which is one–quarter the period of either sinusoid.

弧度，这是任一正弦曲线周期的四分之一。

项目地址(测试网)

testnet.colormask.xyz

铭文现状回顾：纯图像类铭文比例急剧下降，BRC20 铭文及其他文件类铭文成为主体



ColorMask 研发合作方案

如果你是以下情况：

Nodejs后端工程师

坚信BTC生态的后端工程师

会动画或喜欢艺术的前端(全栈)工程师

欢迎加入彩谱项目

共同建设BTC铭文艺术生态

您将收获：

BTC铭文生态的开发技术知识

BTC一层二层生态全貌

项目发售的NFT

项目的利润分红