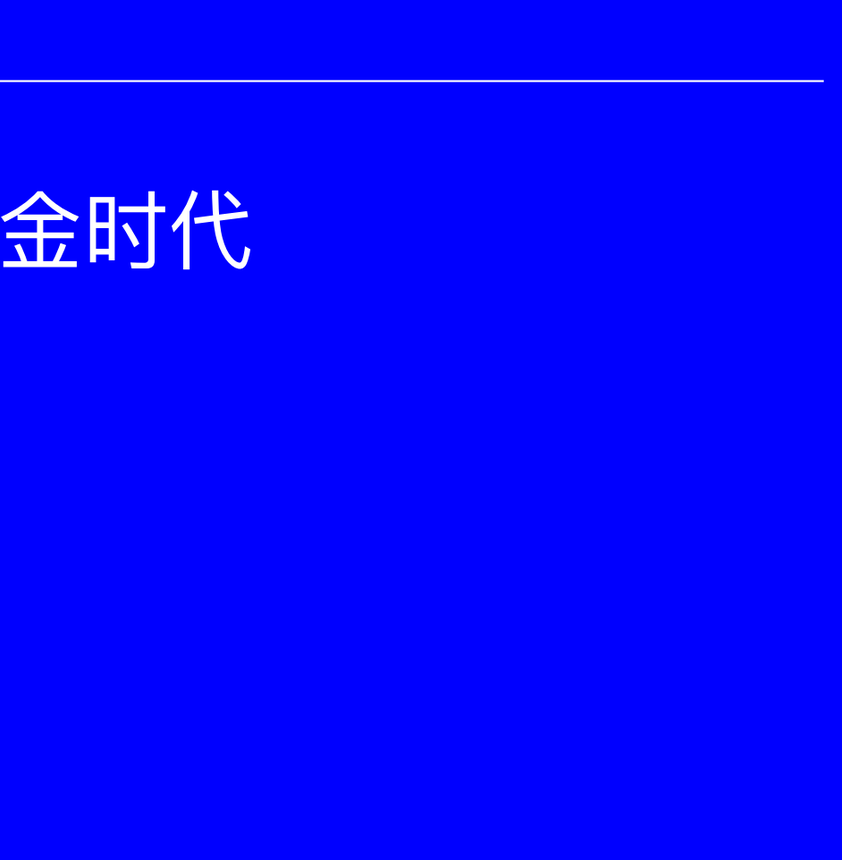
ABCDE

# The Past, Present and Future of Bitcoin Ecosystem



# C0 前言

比特币已经诞生超过15年，自创办之初比特币的定位一直是点对点电子现金支付系统，和“生态”扯不上关系，因为比特币的技术特点和天然不支持图灵完备智能合约，而围绕比特币的可扩展性一直以来也有非常广泛的讨论和争议，从区块之争和硬分叉到闪电网络，对比特币生态拓展新的尝试从未停止。

但是2023年3月8日，Domodata提出BRC20实验并部署 $ORDI，如同打开了潘多拉的魔盒，比特币一夜之间出现了大量的铭文资产，如同2017年以太坊ICO浪潮的重演，$ORDI和$SATS等资产上涨数万倍，市值突破10亿美金。

如果说比特币是数字黄金，那么铭文就是数字黄金精心雕琢出的黄金饰品，而铭文资产的爆发也让比特币正式具备了生态的基础。

那么比特币生态的未来会发展成怎么样?

比特币是如何从点对点的现金支付系统发展为数字黄金生态的?

我们在2023年的年末，在比特币即将减半之际，写一篇报告，试图回顾比特币的过去，盘点比特币的现在，展望比特币的未来。献给所有比特币生态的贡献者。

> If you don’t believe me or don’t get it, I don’t have time to try to convince you, sorry.
>
> ——Satoshi Nakamoto

# C1

# 比特币往事：

# 充满曲折的生态发展之路

ABCDE

# 2018-2023 比特币生态发展大事记

2008.11.01 中本聪发布《比特币:一种点对点的现金支付系统》

2009.01.03 中本聪在位于芬兰赫尔辛基的一个小型服务器上挖出了上帝区块：第一批比特币50个，比特币诞生。中本聪在上帝区块中插入了一句话：“英国财政大臣达林被迫考虑第二次出手缓解银行危机”。载自《泰晤士报》的这句话既说明了区块产生的时间，又是在金融危机下对银行系统的冷嘲。

2009.01.12  中本聪发送了 10 比特币给开发者哈尔·芬尼，完成第一笔比特币交易。

2010.05.21 佛罗里达程序员Laszlo Hanyecz用1万btc购买了价值25美元的披萨优惠券，比特币的第一个价格出现，折合0.0025美元/btc。 

2010.07.17 比特币交易平台MT.GOX在东京创立。

2010.08.15 Bitcoin–bugs 比特币漏洞被发现并利用，在一次交易中生成了超过 1840 亿枚比特币，并被发送到两个比特币地址上。这个非法交易很快就被发现并修复。

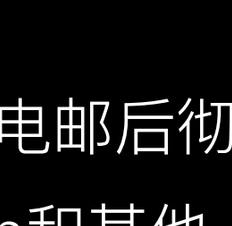
2010.12.16 Pooled–mining 比特币矿池出现。

2011.04.23 中本聪发出最后一封电邮后彻底消失。电邮内容是：我已经开始干别的事了，Gavin和其他人会很好的接手比特币项目。

2012.09.27 比特币基金会成立。

2012.11.28 区块供应量首次减半调整，从此前每10分钟50个减至25个。同时比特币发行量占到发行总量2100万的一半。

2012.12.04 染色币白皮书发布。

2013.08.15 MasterCoin ICO。 

2013.10.29 加拿大启用世界首台比特币ATM，该设备由美国Robocoin公司制造。

2013.12.05 中国央行等五部委发布《关于防范比特币风险的通知》，引发全球比特币将近30%的跌势。

2015.01 Coinbase成为美国首家合规比特币交易所。

2015.09 美国商品期货交易委员会CFTC裁定BTC为商品交易法所涵盖的商品。

2016.07.10 比特币量第二次减半。单个区块比特币产量由25个，正式变为12.5个。

2016.08.03 海外知名比特币交易平台Bitfinex价值超6000万美元巨额比特币被盗，引致币价跳水，跌幅一度超过25%。最终平台上所有用户分摊总资产36%的损失，Bitfinex发行债务代币BFX“债转股”。

2017.03.11 美国证监会SEC正式发布报告称已拒绝比特币ETF，BTC应声大跌10%。这也是比特币ETF提案第一次被美国SEC拒绝。

2017.05.23 56家比特币初创公司同意了Barry Sibert提出了Segwit2M（后改为Segwit2x）妥协方案，共同签署了纽约共识。

2017.08.01 在比特币原有的主链上，硬分叉产生的新货币诞生了。比特币现金(Bitcoin Cash)被创建。

2017.08.24 隔离见证正式激活。

2017.09.04 中国央行宣布将ICO定性为非法金融活动，暂停国内一切交易，随后，监管层继续宣布关停注册在国内的所有比特币交易所。

2017.11.19 比特币单价首次突破1万美元。

2017.12 BTC在12月诞生8个分叉币：SBTC，LBTC，BTP，GOD，BUM，Bitcoin Cash Plus，，Bitcoin Silver，Bitcoin X(比特无限)。

2017.12.11 芝加哥期权交易所正式挂牌上市比特币期货，首个交易日盘中大涨逾20%。

2018.01.01 RSK主网上线。

2018.03.15 ⚡闪电网络发布了其首个主网测试版程序。

2018.09.27 Liquid区块链正式上线。

2018.11.15 BSV分叉。

2019.09.23 Bakkt推出实物交割比特币期货合约。

2020.03.12 由于金融市场恐慌，比特币日内跌幅超50%。

2020.05.12 BTC第三次减半，减半后区块奖励为6.25 BTC。

2020.12.16 比特币破2万美元，创历史新高。

2021.01.14 Stacks主网2.0上线。

2021.02.19 比特币首次达到1万亿美元的市值。

2021.06.19 萨尔瓦多议会通过一项法案，批准将比特币作为该国法定货币，该法案在90天后正式生效。

2021.11.16 Taproot升级正式生效。

2022.12.14 Ordinals 协议发布。

2023.03.08 domodata提出 BRC20 实验，并部署 $ORDI。

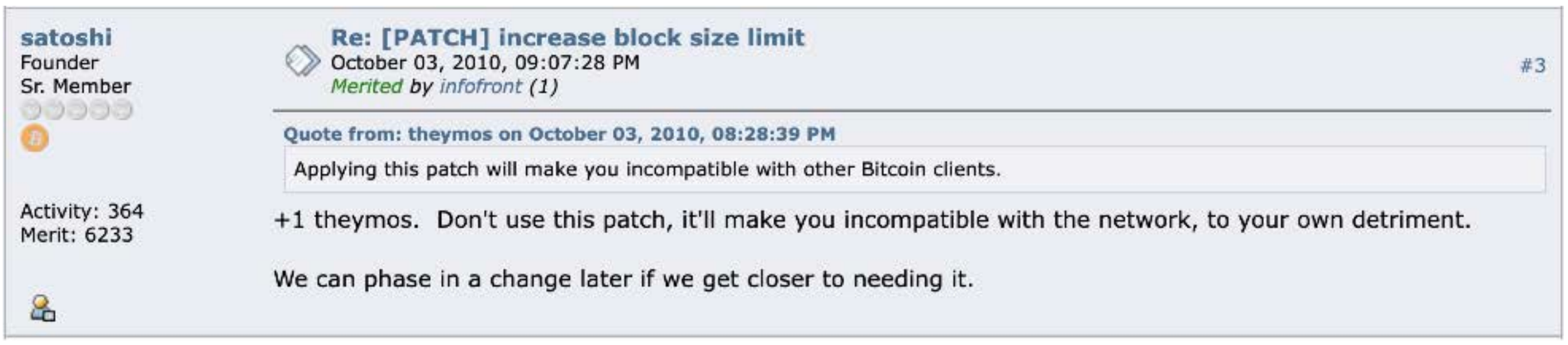
2023.10.19 Lightning Labs上线Taproot Assets的首个主网alpha版本。

## 1.1 比特币应该成为支付系统还是数字黄金?

**比特币应该成为支付系统还是数字黄金在很早的时候就存在争议。**2010年6月17日，中本聪在Bitcoin论坛写道：

该设计（比特币）支持我多年前设计的各种可能的事务类型，托管交易、保税合同、第三方仲裁、多方签名等等。如果比特币能够被大范围接受，这些都是我们未来想要探索的东西，但它们都必须在一开始时就设计好，从而确保以后能够实现。

**大规模应用和交易规模意味着更复杂的交易指令和更大的交易空间。**在2010年7–9月间，中本聪多次修改了BTC代码，包括移除了两个操作码，禁用了比特币编程语言Script的一些功能等。另一方面，BTC创立之初并没有限制区块大小，以便能够在相同时间处理的交易笔数。但当早期BTC价格非常低，恶意交易的成本也非常低，为了解决这一问题，中本聪在2010 年 9 月 12 日主持了一次软分叉，添加了区块体积不得超过 1 MB 的限制。同年10月4日，开发者 Jeff Garzik 在自己开发的新客户端里该客户端将中本聪引入的限制移除，但遭到了社区和中本聪本人的反对。中本聪指出但这种限制是临时性的，**未来可以以可控和逐步的方式提高区块限制，以便满足扩容的需要。**



**satoshi**
Founder
Sr. Member
Activity: 364
Merit: 6233

**Re: [PATCH] increase block size limit**
October 03, 2010, 09:07:28 PM
*Merited by infofront (1)*

#3

**Quote from: theymos on October 03, 2010, 08:28:39 PM**

Applying this patch will make you incompatible with other Bitcoin clients.

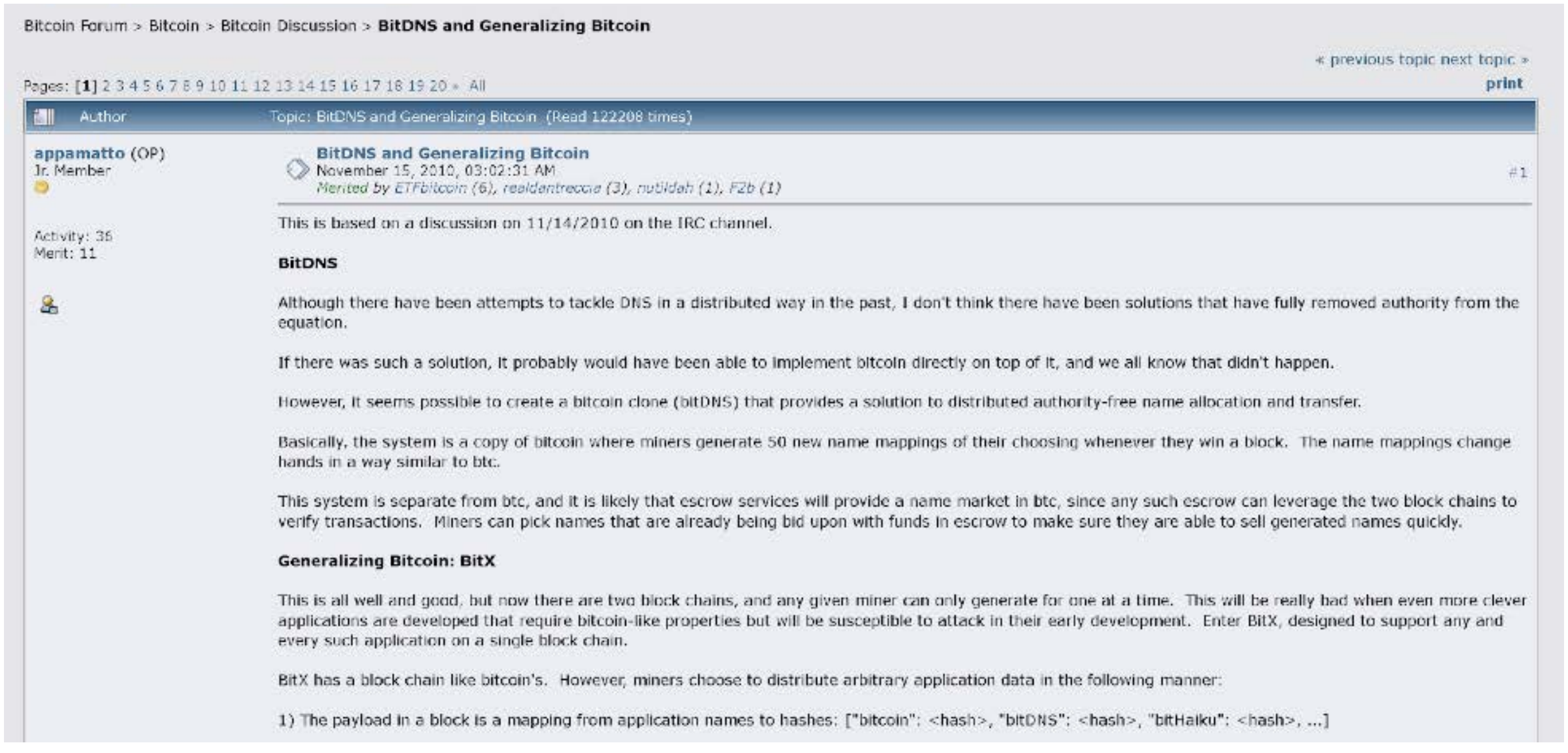
+1 theymos. Don't use this patch, it'll make you incompatible with the network, to your own detriment.

We can phase in a change later if we get closer to needing it.

Source：Bitcointalk

到了2010年的12月，由于未知的原因，中本聪发出了最后一条公开消息并退出了公众视野，但此时关于BTC定位和可拓展性的问题并没有真正盖棺定论，1MB限制也为后续等一系列争论埋下了伏笔。

在此期间，bitcointalk论坛上也出现了除付款以外的比特币应用场景讨论，例如appamatto 在在2010年11月提出了在比特币网络上构建去中心化域名服务的提案，但该提案并没有被包括中本聪在内的早期成员认可，提案中的BitX成为了以太坊和其它项目的核心组成部分，而BitDNS最终发展成为了首个山寨币 Namecoin。



Bitcoin Forum > Bitcoin > Bitcoin Discussion > **BitDNS and Generalizing Bitcoin**

« previous topic next topic »

Pages: [1] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 » All

print

Author | Topic: BitDNS and Generalizing Bitcoin (Read 122208 times)

**appamatto** (OP)
Jr. Member

Activity: 36
Merit: 11

**BitDNS and Generalizing Bitcoin**
November 15, 2010, 03:02:31 AM
*Merited by ETFbitcoin (6), realdantreccia (3), nutildah (1), F2b (1)*

#1

This is based on a discussion on 11/14/2010 on the IRC channel.

**BitDNS**

Although there have been attempts to tackle DNS in a distributed way in the past, I don't think there have been solutions that have fully removed authority from the equation.

If there was such a solution, it probably would have been able to implement bitcoin directly on top of it, and we all know that didn't happen.

However, it seems possible to create a bitcoin clone (bitDNS) that provides a solution to distributed authority-free name allocation and transfer.

Basically, the system is a copy of bitcoin where miners generate 50 new name mappings of their choosing whenever they win a block. The name mappings change hands in a way similar to btc.

This system is separate from btc, and it is likely that escrow services will provide a name market in btc, since any such escrow can leverage the two block chains to verify transactions. Miners can pick names that are already being bid upon with funds in escrow to make sure they are able to sell generated names quickly.

**Generalizing Bitcoin: BitX**

This is all well and good, but now there are two block chains, and any given miner can only generate for one at a time. This will be really bad when even more clever applications are developed that require bitcoin-like properties but will be susceptible to attack in their early development. Enter BitX, designed to support any and every such application on a single block chain.

BitX has a block chain like bitcoin's. However, miners choose to distribute arbitrary application data in the following manner:

1) The payload in a block is a mapping from application names to hashes: ["bitcoin": <hash>, "bitDNS": <hash>, "bitHaiku": <hash>, ...]

Source：Bitcointalk

# 1.2 Bitcoin 2.0的资产发行尝试

中本聪离开后，继承人Gavin Andresen主导建立了Bitcoin Core和Bitcoin基金会。在此期间，针对BTC 的可拓展性探索一直存在，尤其是在资产发行领域。

- **Colored Coins（染色币）**

eToro首席执行官 Yoni Assia在 2012 年 3 月 27 日发表的一篇文章中第一个提出彩色币。这个想法不断发展，在Bitcointalk等论坛上，彩色硬币的概念开始形成并获得关注。最终 Meni Rosenfeld于 2012 年 12 月 4 日发布了一份详细介绍彩色货币的白皮书。

染色币的设想是通过给比特币的特定部分添加特殊的标注（即染色），来代表更广泛的资产和价值。染色币在实现上出现了一系列实体，大致分为两类：

**基于OP_RETURN**：如 Flavien Charlon 在2013年提出的 Open Assets，利用 OP_RETURN（在 Bitcoin v0.9.0 中被提出，可以用于在 Bitcoin 上存放少量的数据，最初的限制为 40 bytes，后提高至 80 bytes）。操作码存储到脚本中，并通过外界读取的方式来完成“染色”和交易。（这种模式与 Ordinals 依靠外部索引确定资产合法性类似）。

**不基于OP_RETURN**：典型代表是ChromaWay 在2014年提出的EPOBC Protocol，EPOBC资产的额外信息存储在比特币交易中的nSequence字段，每个EPOBC资产的类别和及合法性需要追溯到genesis交易来确定。

- **MasterCoin（Omin）**

JR Willett 在 2012 年 1 月 6 日发布了MasterCoin的设想并取名“比特币第二份白皮书”并在2013年7月通过ICO的方式正式启动项目，最终募集到了5120个BTC（价值50万美元）。MasterCoin 和Colored Coins区别在于它建立了一个完整的节点层，通过扫描比特币区块来维护状态模型数据库，该数据库驻留在区块链之外的节点中。这种设计可以提供比Colored Coins更复杂的功能，例如创建新的资产、去中心化交易所、自动化价格反馈等。

2014年，Tether也通过Mastercoin协议在比特币上推出了稳定币，即我们熟知的Tether USD (OMNI) 。

- **Counterparty**

Counterparty于2014年正式推出。Counterparty也使用 OP_RETURN 将数据存储至BTC网络中。但与染色币不同，资产在Counterparty不是以 UTXO 的形式存在，而是通过 OP_RETURN 载入信息来表明资产的转移，当一个资产持有者使用持有地址对歹有特殊数据的交易进行签名后，资产便完成了转移。通过这种方式，Counterparty可以实现资产的发行、交易以及兼容以太坊智能合约的平台。

除此以外，也有观点认为Ethereum、Ripple和BitShares 也属于更广义的“Bitcoin 2.0”。

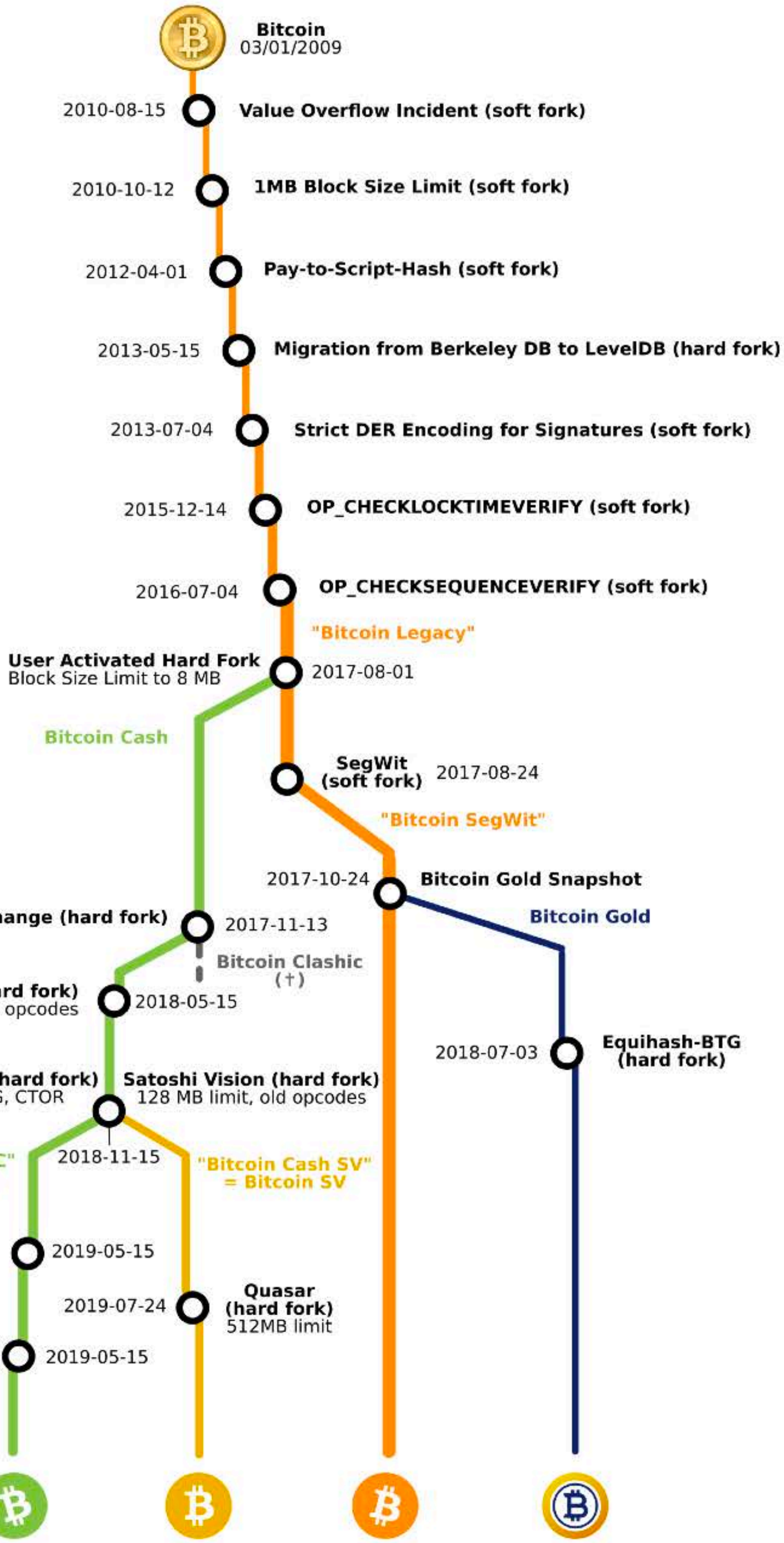
## 1.3 区块大小之争与硬分叉

随着比特币的更加普及，网络交易拥堵和确认时间增长问题愈发严重。2015年，Gavin Andresen 和 Mike Hearn 宣布将在新版 BitcoinXT 中实现 BIP-101 提案，希望将区块上限提高至 8 MB。而 Greg Maxell, Luke Jr, Pieter Wuille 等核心开发者则持反对意见，认为这种做法会提高运行全节点的门槛，而且带来不可控的影响。这场争论最终在议题和参与范围均出现了扩大化。

两种路线并不存在绝对的优劣，坚持小区块路线无法回答“区块奖励降低以后，低交易量如何维持足够的激励以保证安全？”这个核心问题。而 8 MB也不会是最终解决方案，一旦选择了大区块，最终很可能需要不断地扩容，无限扩容导致的技术风险堆叠和不可预测风险也确实存在。**这场争论的本质仍然是“比特币的愿景到底是什么？”**争论最终导致了社区分裂和 2017 年开始的硬分叉。而除了BCH（和后面的BSV）以外，这一时期还出现了许多其它BTC分叉币，据BitMEX Research，仅在BCH分叉后的一年内，就出现了至少 50 种新的分叉币。

ABCDE

# Main Consensus Forks of Bitcoin (2009 — 2019)




"Main Consensus Forks of Bitcoin" v3
@lugaxker / lugaxker#106;
Source: blog.bitmex.com/bitcoins-consensus-forks/

## 1.4 SegWit & Taproot

**在分叉以后，BTC 链在维持区块大小的前提下也逐渐引进了一系列新的技术方案以提高可拓展性，其中最重要的就是SegWit 和Taproot。**

隔离见证（Segregated Witness）作为直接提高区块大小的“替代方案”在BCH分叉的同时被引入，SegWit 将交易分为两个部分，前一部分包含发送和接收地址，第二个部分保存交易签名或见证数据，移除主区块但保留验证功能。见证数据的移出使得在相同区块大小下所能容纳的交易更多，以另一种方式提高了吞吐量。SegWit 以软分叉的方式引入，采用率不断提升，到2020年已经超过60%，到2023年12月已达到95%。


Source: https://buybitcoinworldwide.com/stats/segwit-adoption/

2021 年 11 月，另一项重要升级 Taproot 同样以软分叉的形式正式生效。此次升级从结构上来说由BIP340、BIP341 和 BIP342 组合。其中BIP340 引入了可以同时验证多个交易的 Schnorr 签名，取代了椭圆曲线数字签名算法 (ECDSA)，再一次扩大了网络容量并加快了批量交易的处理速度，为部署复杂的智能合约提供了可能性；BIP341 实现了默克尔化抽象语法树（MAST）来优化区块链上的交易数据存储；BIP342（或 Tapscript）采用比特币的脚本编码语言来适应 Schnorr 签名和 Taproot 实现。

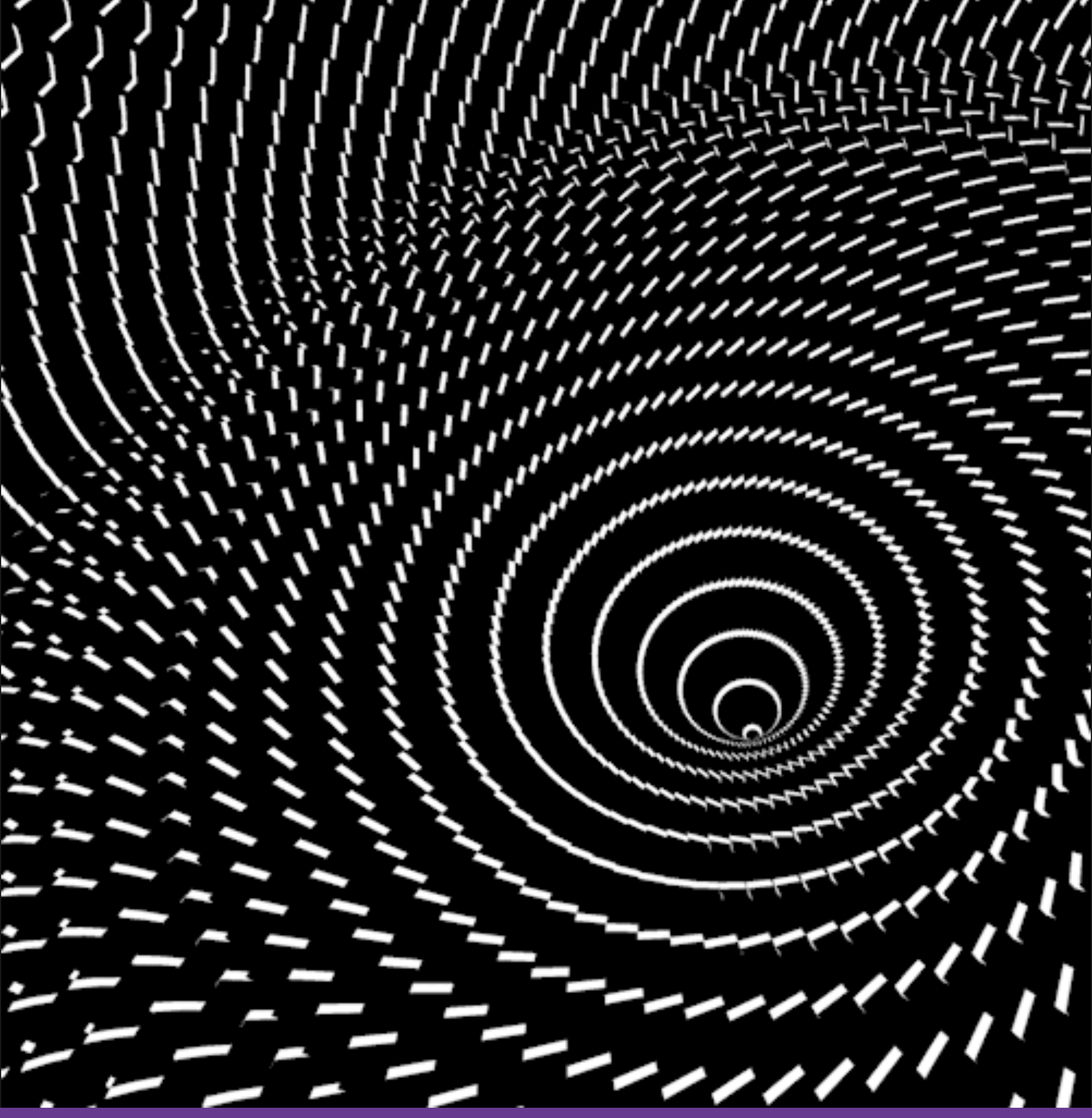
指的一提的是，SegWit 最初并没有对验证信息的长度做出限制，这也就导致后续项目可以通过验证信息的方式绕开 1 MB的区块大小限制，也为后续Ordinals 的兴起埋下了伏笔。对于这种做法，社区也出现了争议，一些反对者认为SegWit 没有设置长度限制是一种“失误”，因此利用验证信息传递数据的方式是一种不正当的“攻击行为”。

## 1.5 Bitcoin Layer2的早期探索

伴随着区块大小之争尘埃落定，比特币 L2 开始大规模走进大众视野，其中最主流的路线是闪电网络（ Lightning Network ）和侧链（Sidechains）两类解决方案

闪电网络最早在2015年由 Joseph Poon 和 Thaddeus Dryja 提出，核心思想是在多签地址中锁定一部分比特币，从而建立一个单独管辖的协作协议。闪电网络中的交易在链下进行，最终结果由 BTC 网络确认。2018 年3 月，Lightning Labs 宣布闪电网络正式上线比特币主网，代表应用有Strike、Taro、Lightspark等。

侧链的思路是从比特币网络获得/向比特币网络转出比特币，但交易行为与BTC网络独立。侧链方案的尝试更早一些，2014年Blockstream就出版了第一篇比特币侧链方案的技术论文，但该方案并没有被真正实施。而RSK在2015年发布白皮书，2018年1月，RSK 最终启动了完整功能的主网；同年9月，Blockstream 启动了 Liquid Network 侧链。除RSK和Liquid Network以外，Stacks、RootsStocks、Drivechain等也属于侧链解决方案。另外，开发者们也在状态通道、Roll-up等方向进行了探索与实践。



# C2

# 比特币生态：

# 一串铭文打开潘多拉魔盒

在这之前，很多对于比特币的印象，甚至和“生态”都扯不上关系，因为比特币的技术特点和天然不支持图灵完备智能合约的限制，比特币能够勉强算上生态的只有闪电网络与Stacks这种，且常年处于门庭冷落的状态。大家的焦点都集中在“智能合约平台”上，无论是ETH，还是L2，或是一众Alt L1。

谁也没有想到，一个Ordinal协议，把铭文Inscription这个概念彻底带火，让整个BTC生态燃了起来，一举反超所有智能合约平台，甚至讽刺的是，连绝大多数智能合约平台也开始搞起了铭文。

## Ordinal的发展历程

**3月8日**：@domodata 提出 brc20 实验，并部署 $ORDI

**3月9日：**$ORDI被 mint 完毕，mint一张价格5U左右

**3月10日至3月23日：**$ORDI场外交易，交易 0.03U 左右

**3月23日：**UniSat上线 BRC20交易市场，价格迅速拉升至 0.3U，随即因为双花问题，UniSat关闭交易市场

**4月27日：**UniSat再次上线 BRC20 交易市场，只针对部分用户开放，$ORDI价格迅速拉升到 1U，并持续走高

**5月5日：**Opensea 宣布支持 Ordinals 和 BRC20，情绪彻底 fomo，价格来到 6U，各种新的 BRC20被各个社区炒作，如 nals，xing，oshi，shib 等

**5月8日：** $ORDI 上线 gate.io，当天 BTC 链上手续费占矿工总收入的 43.7%，上线 gate 后，价格从9U冲到20U

**5月9日：**$ORDI冲到最高点 28U，gate.io开始上线各种BRC20，如 BANK等，piza等，IRC20，DRC20 等也陆续出现，分流 BRC20

**5月9日–5月12日：**随着大户的砸盘，以及整个市场的低迷，ordi的价格持续下降到7.5U左右，市场情绪降低

**5月12日：**OKX宣布与UniSat达成官方合作，共建 BRC20 行业标准，一剂强心针后，$ORDI价格回暖，当天回调至12U左右

**5月20日：**@okx 和 @HuobiGlobal 上线$ORDI，价格从12U上升至15U，随之而来的就是长达4个多月的持续下跌

**9月11日：**跌破3U，Ordinal黑暗的一天

**10月18日：**UniSat发布 brc20–swap，ORDI开始回暖。至此，$ORDI开始上涨

**11月3日：**BRC20生态逐渐起势，价格逐渐涨至6.2U，当日 $sats 市值超过$ORDI

**11月7日：**Binance宣布上线$ORDI，从7.4U暴涨至13.5U，开始逆袭之路

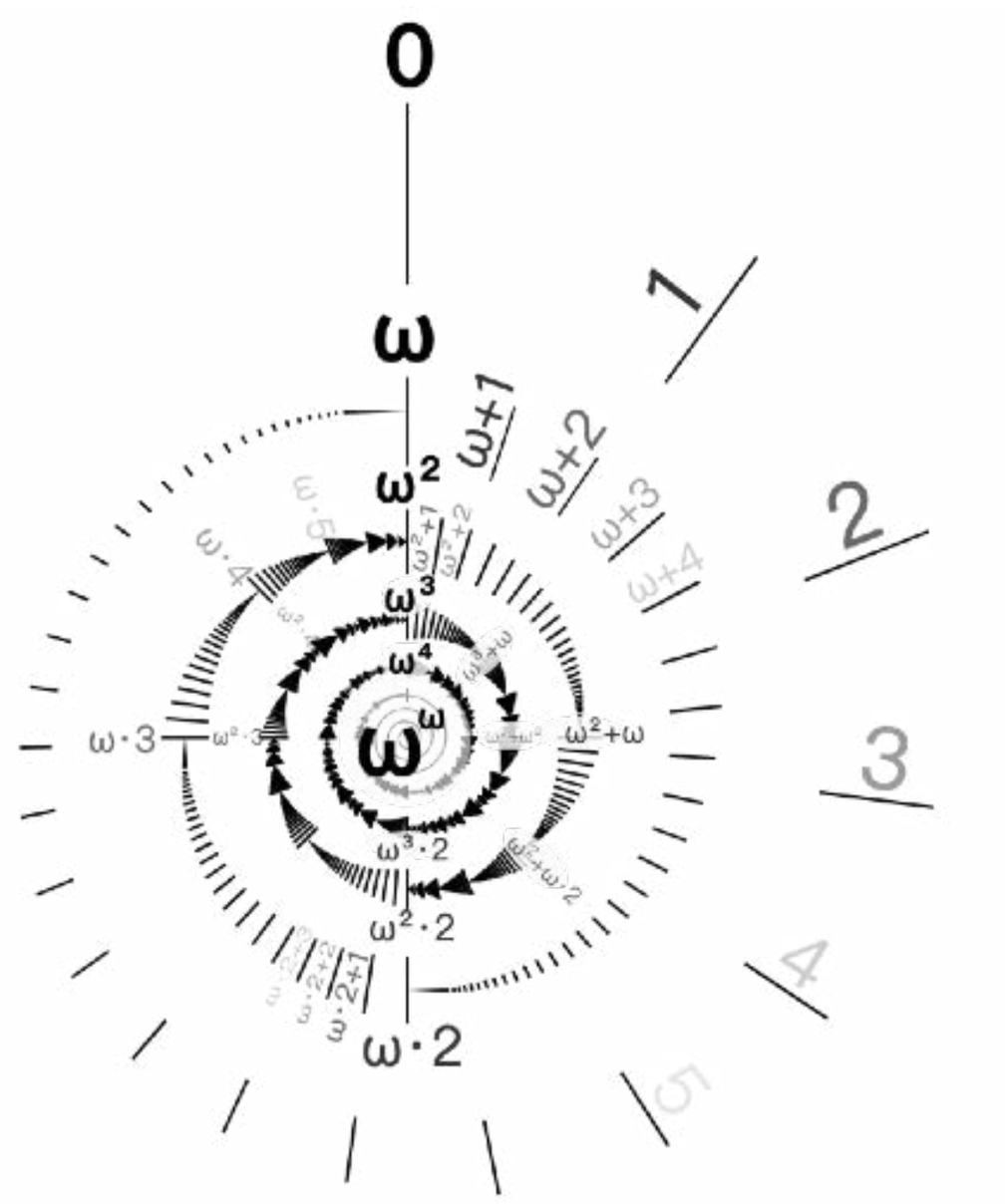
**11月10日至12月1日：**在20U左右徘徊

**12月2日：**$ORDI从21.7U涨至32U，超过5月份达到历史新高

**12月5日：**$ORDI涨至69U，市值突破10亿美金

## 2.1 Ordinal与BRC20

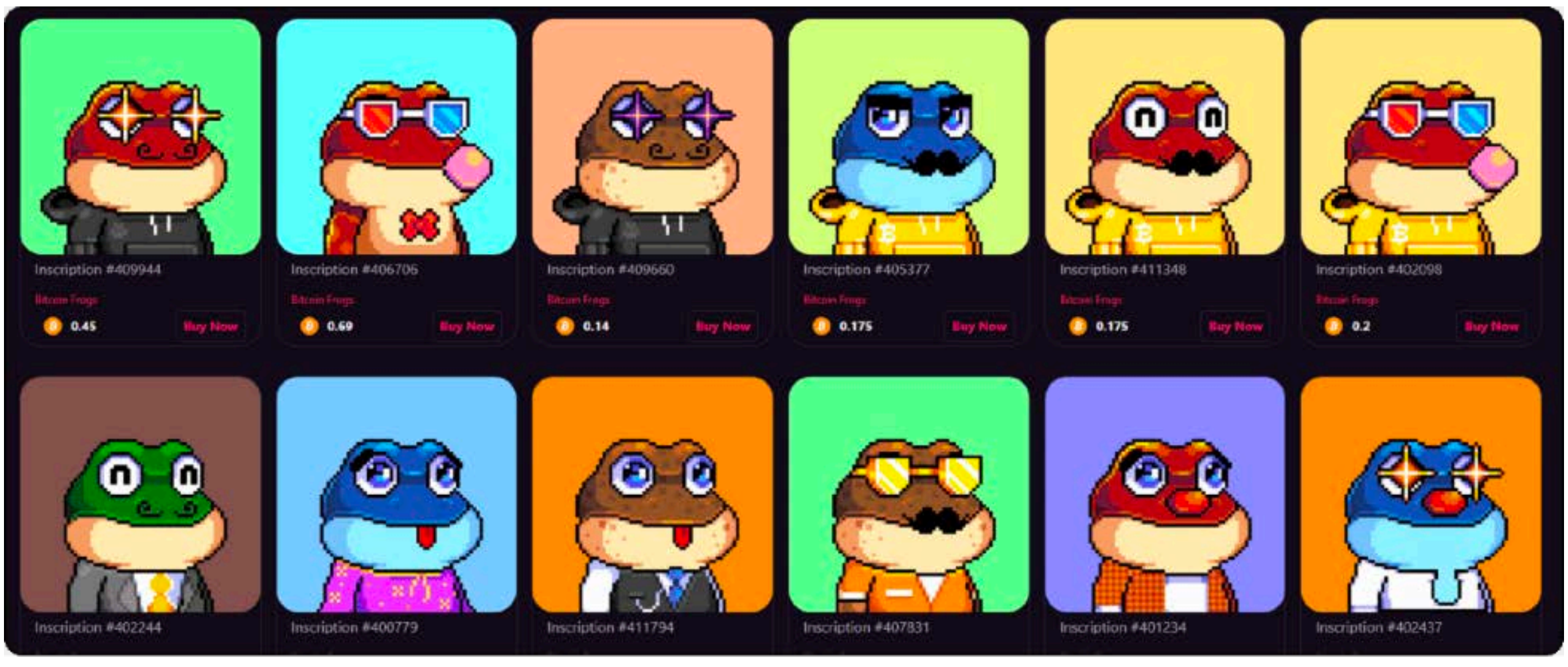
如果要用一句大白话解释清楚Ordinal是什么，那么我想最容易理解的便是 – Ordinal就是一个把BTC当成网盘来用的铭刻协议。




而之所以可以把BTC当成网盘来用，正是因为2年前的那次Taproot升级，移除了之前单笔交易在隔离见证字段放置的数据量限制，直接拉满顶格到4M，让BTC被动的开始具备一个“不可篡改，永久存储”的网盘性质 – 是不是听着很像Arweave?

而Casey Rodarmor（Ordinal创始人），则是打开了潘多拉魔盒的那个人，估计在他创建Ordinal之初，他都不会想到BTC的铭文生态会是今时今日这番景象。

Ordinal的本质其实很简单，它更像是一个NFT协议，只不过与ETH或是其他公链的NFT元数据（MetaData）大多存储于IPFS或是中心化服务器不同，Ordinal的元数据嵌入到了交易的见证字段（Witness Data），像是被“铭刻”到某个特定的聪上一样，这也是铭文这个词的来源。




Source:BitcoinFrogs

这也是Ordinal一开始的叙事和打法 – BTC不可篡改，永久存储的“网盘性质”，元数据可以支持文字，图片，视频等宽松的性质，除了4MB的大小限制（后面讲递归铭文的时候这个限制也不再有了），似乎没有什么比BTC更适合做NFT平台了，这段时间，火爆的是各种ETH NFT在BTC上的仿盘，比如BTC版的Punk， BTC版的Ape等等，没人想到最终胜出的是开始名不见经传的BitcoinFrogs。

然而有了新的玩法，市场是不会单单满足于NFT的，毕竟NFT的非同质化与流动性使得他的交易顺滑度与市值等各个维度都与FT相差了至少一两个数量级。于是乎另一个大神Domo出现了，他拿Ordinal这样一个偏NFT的协议作为基础，硬是模拟出了一套类似ERC20这样的同质化代币玩法，命名为BRC-20。而实现的方式也很“巧妙”，既然Oridinal对文件格式没有限制，那么JSON File也是可以的。

于是乎，在Deploy，Mint，Transfer三个简易“操作码”的帮助下，BRC-20借助Indexer，真的实现了类似ERC-20的铸造和转账功能。

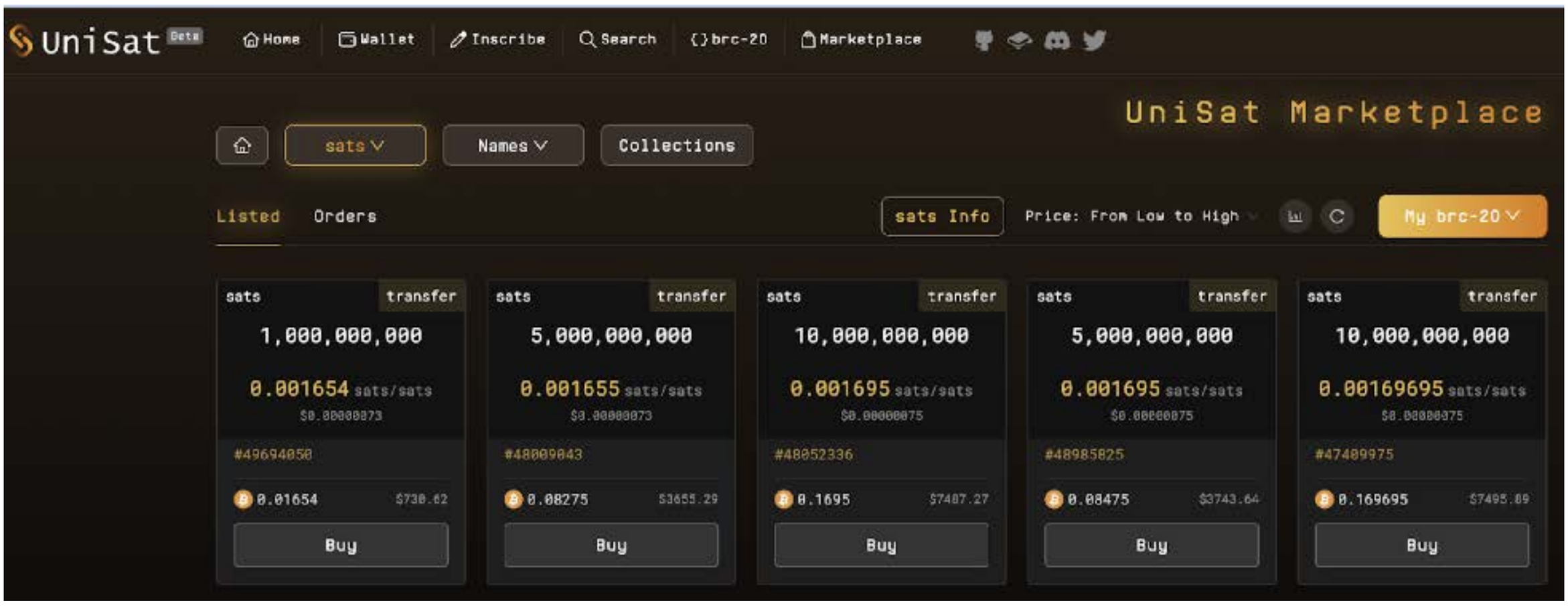
而Indexer的角色，则是一个暂时相对中心化的，提供比特币链上的所有 BRC20查找的基础设置，根据deploy, mint, transfer 的情况来索引出每个人的持有的BRC20币的数量。


BRC20生态里最值得一提的有三个名词：

- **ORDI** – 第一个BRC20铭文，当前整个铭文体系的龙头，虽然从应用属性来看算是一个Meme，然而First is First，没有$ORDI，也就不会有接下来成百上千的BRC20，BTC生态后续出现的各种XRC20，以及延伸到其他各大公链的铭文体系

- **SATS** – 因为长达6个月的mint时间，小数点后无数个0，相对Ordi更加分散的筹码结构，被UniSat赋能做BRC-20 Swap手续费的第一个“有用”的铭文等等系列属性……$SATS作为BRC20的“龙二”，市值一度超过龙头$ORDI，甚至有着与$ORDI争夺龙一的态势，无论最终花落谁家，$ORDI与$SATS成为市场公认的铭文双子星。

- **Unisat** – 目前BRC20生态里最为核心的基础设施，从最早的代打服务到钱包到Indexer到Marketplace包括最新创新性的Module……可以说没有UniSat，今天的铭文生态一定不会如此这般的繁荣。




Source: UniSat

很有趣的是Ordinal的创始人Casey并不认同BRC-20这种铭文的形式，认为这会让比特币区块空间塞满“垃圾UTXO”，影响BTC的正常转账。然而终是敌不过矿工的扶持和用户的热情，BRC20不以任何人意志为转移的开始全面铺开，也便有了后面各类XRC20改进型协议的诞生。

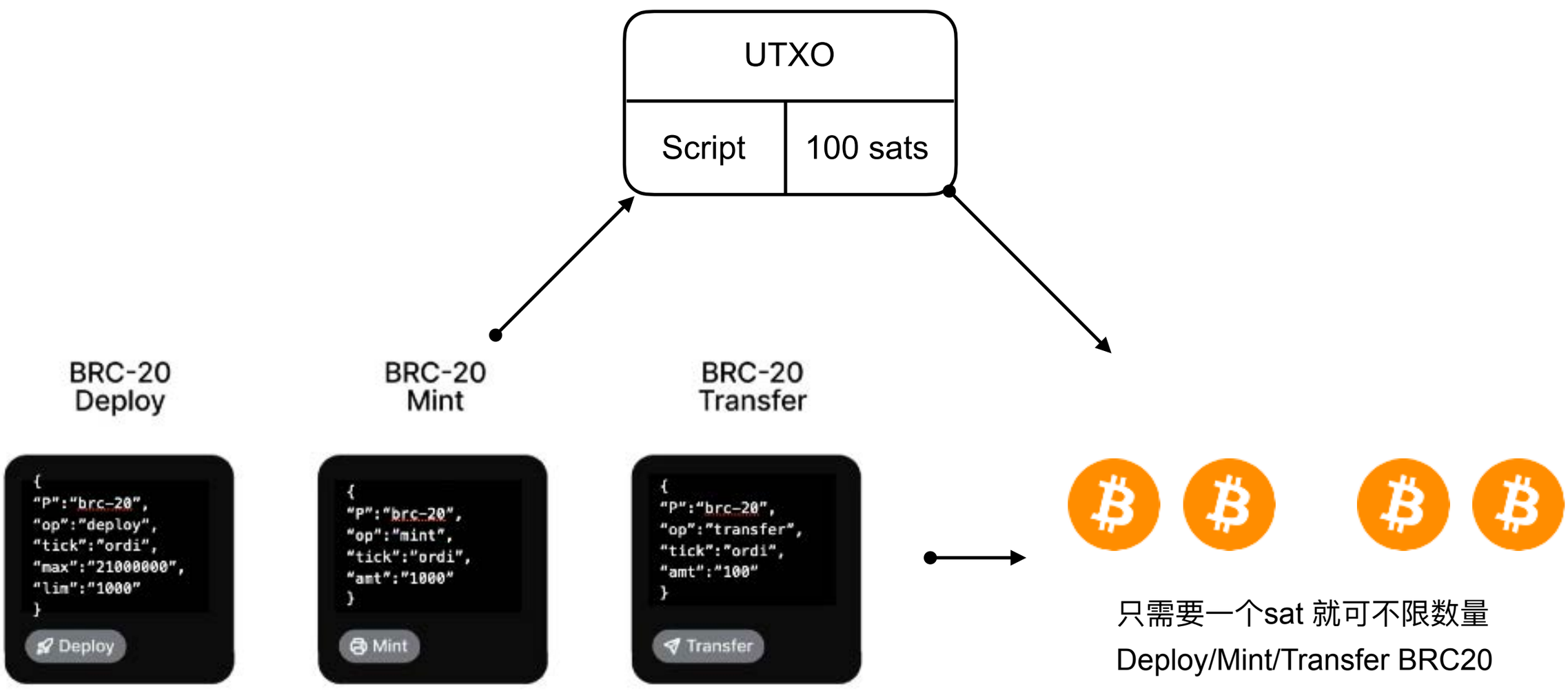
## 2.2 Atomical — 后起的新星

如果说在BTC生态里，Ordinal协议很像BTC的话，那最像ETH的一定是Atomical协议。自然，协议的代表则是Arc20这个“代币标准”。Atomical跟Ordinal的区别，或者说ARC20与BRC20的区别，从基础框架来看，还是挺大的。

最直观的区别便是，Atomical采用了类似我们前面写到的彩色币技术，把代币与UTXO里的聪直接进行了绑定，这样的结果便是 – 虽说ARC20也同样需要Indexer去索引ARC20铭文的“存在”，但他的转账交易是完全依赖于BTC Layer1 UTXO的，完全独立于Indexer，这相对于BRC20这种从铸造到Mint到转账都严重依赖Indexer的协议来说，其安全性无疑大大提升，也避免了BRC20那种所谓的“垃圾UTXO”。

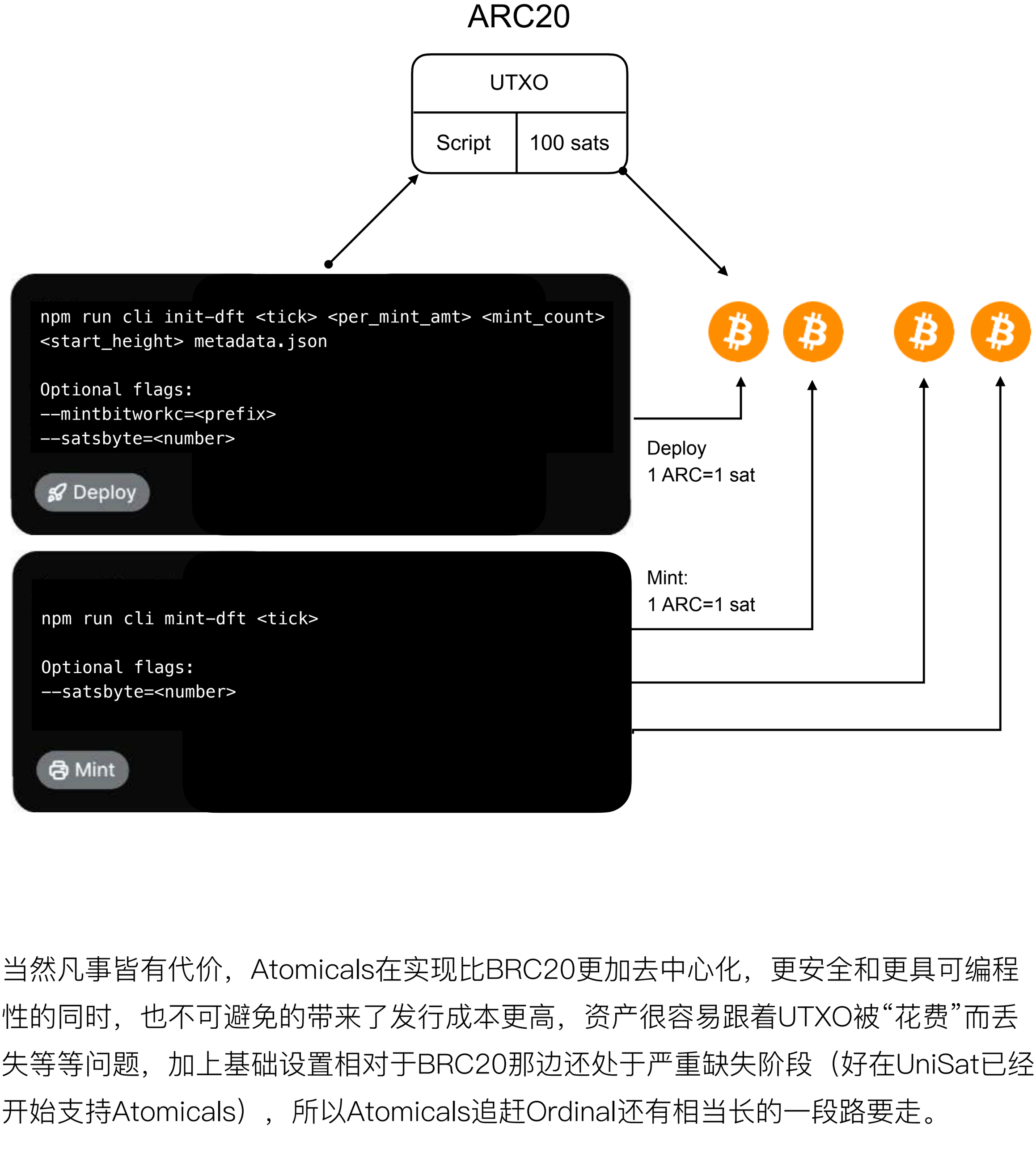
除此之外，Atomical还有几个让人眼前一亮的特点。比如在铸造过程中引入了类似比特币POW的挖矿机制Bitwork，让铸造变得更加公平和去中心化，也更贴近BTC的技术特点，比如因为UTXO本身可以在BTC交易中被组合，这使得ARC20代币的可编程性更好 – BTC与 ARC20的swap理论上只需要调换UTXO的输入与输出即可实现。

# BRC20




只需要一个sat 就可不限数量
Deploy/Mint/Transfer BRC20

# ARC20




当然凡事皆有代价，Atomicals在实现比BRC20更加去中心化，更安全和更具可编程性的同时，也不可避免的带来了发行成本更高，资产很容易跟着UTXO被“花费”而丢失等等问题，加上基础设置相对于BRC20那边还处于严重缺失阶段（好在UniSat已经开始支持Atomicals），所以Atomicals追赶Ordinal还有相当长的一段路要走。

最后Atomicals还有两点非常独特的“气质”不得不提一下：

一是创始人 – 很多人一开始把Atomicals当作Ordinal仿盘来看，进了社区发现才发现其开发时间之长、创始人的坚决、考虑的场景和 features 之多，是一套极其完整的协议，根本不是LTC之于BTC这种。有KOL看了Atomicals匿名创始人的几个访谈之后甚至感慨：这个人说话的那种理性，那种感觉，太像年轻时的乔布斯了……一个匿名的乔布斯风格的创始人，这也让整个协议的气质完全与众不同。

二是Atomicals的大杀器AVM – 前段时间ZeroSync团队抛出一记重磅炸弹，让BitVM这个“理论上可以让BTC计算任何内容”的概念在全网引发了无数讨论。当前业内的共识是，BitVM当前在技术理论上的确可行，但工程上离落地还有至少数年的时间，且计算的Cost从商业上角度目前来看也很难落地，但一旦成功的话可能是BTC扩容与发展的最佳方案。而Atomicals创始人在白皮书发表之后表示 – “bitVM 的想法很棒，我也学到很多。在Atomicals协议的机制上，稍作一些修改，应该就能实现类似的效果”。这也让AVM承载了很多圈内人的希望。

## 2.3 Rune, BRC100

- Rune

Ordinal创始人Casey一直看BRC-20不爽，却又做不了什么。在Atomincals协议问世之后，受其启发（盲猜，因为Atomicals先发布的），发布了Rune协议，用于发行FT风格铭文。

Rune和Atomicals核心层面非常接近，都是在UTXO脚本中写入TokenID、输出与数量等Token信息，把转账交给BTC 1层来处理，对于Indexer依赖程度不高。

区别则在于，Rune在脚本数据中写入Token的具体数量，不再是1sats=1token，好处在与比ARC20具备了更高的精度，但坏处是复杂度也变得更高，难以像 ARC20一样直接利用BTC UTXO的组合性。

比较搞笑的是Casey的Rune协议只是一个“想法”，没有具体产品，导致Trac的创始人基于此抢先编写了第一个可用协议，发布了pipe铭文。

后来有出现一个Rune Alpha的项目，发布Cook铭文，大家都以为是Casey的项目，没曾想Casey否认了，但在否认之前市场热度已经起来，所以即便是否认之后，Cook的市场热度依旧不低。

- BRC100

BRC100的构想是在BRC20的Deploy，Mint，Transfer功能至上，还引入了一些去中心化计算的概念，使未来可构建构建 AMM DEX、借贷，SocialFi，Gamefi等比特币原生去中心化应用。但BRC100 目前还处于待开发状态。具体开发细节请参考：https://docs.brc100.org/

## 2.4 SRC20，BRC420

- SRC20

SRC20起源于BTC Stamps 协议，这个协议并非脱胎于Ordinal，而是与Ordinal直接竞争，网上有这么一张图可以很好的说明BTC Stamps与Ordinal的区别。

Rune和Atomical核心层面非常接近，都是在UTXO脚本中写入TokenID、输出与数量等Token信息，把转账交给BTC 1层来处理，对于Indexer依赖程度不高。

区别则在于，Rune在脚本数据中写入Token的具体数量，不再是1sats=1token，好处在与比ARC20具备了更高的精度，但坏处是复杂度也变得更高，难以像 ARC20一样直接利用BTC UTXO的组合性。

比较搞笑的是Casey的Rune协议只是一个“想法”，没有具体产品，导致Trac的创始人基于此抢先编写了第一个可用协议，发布了pipe铭文。

后来有出现一个Rune Alpha的项目，发布Cook铭文，大家都以为是Casey的项目，没曾想Casey否认了，但在否认之前市场热度已经起来，所以即便是否认之后，Cook的市场热度依旧不低。

- **BRC420**

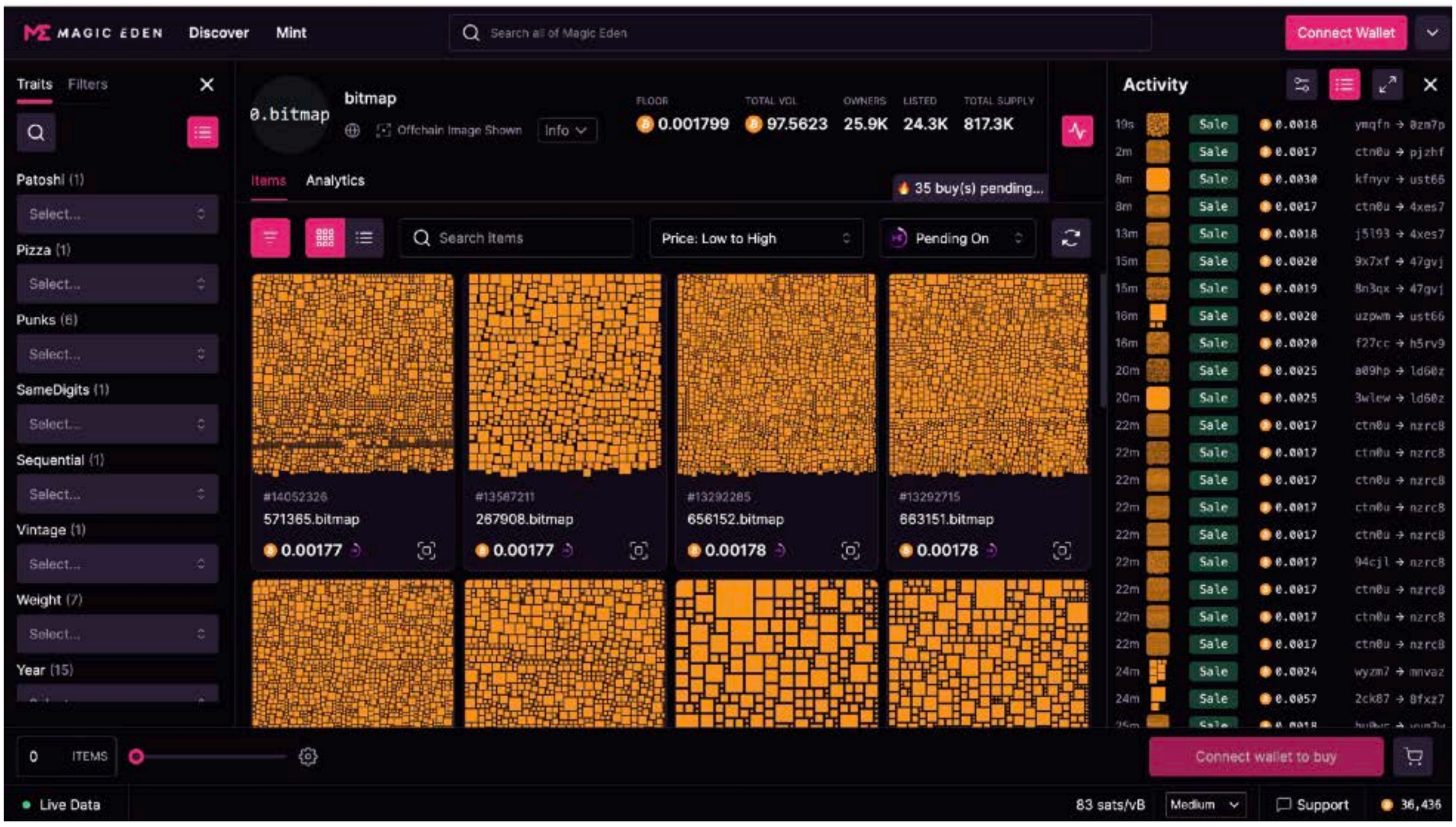
BRC420是Recursiverse团队推出的“BTC元宇宙协议”，跟之前几个资产发行类的协议不同，BRC420更偏向应用层面，也更加复杂。

BRC420带来了三个很有趣的东西：

一是递归铭文型资产，BRC420通过递归的方式定义了更复杂的资产格式，通过将多个铭文递归在一起，组合成一个复杂铭文，任何人都可以创建自己的元宇宙铭文，包括并不限于游戏形象、游戏 DLC、HTMI 脚本、音乐、视频等等……最终实现“链上铭文模块化”。

二是链上版税，因为有个递归模块化资产的相互调用，所以小到一个人物形象或宠物，大到将整个游戏脚本、虚拟机甚至AI大模型都可以组合成链上资产，这时合理的，自动执行的版税系统可以很好的鼓励开发者生态，让链上存在更多有价值的模块 – 比如很火的全链游戏，如果某个爆款的战斗系统，抽卡系统，盲盒系统等等都可以作为单独的模块铭文化，在被其他游戏调用时原作者同样可以获得版税收益。

三是Bitmap, Bitmap是个非常“酷”，也非常硬核的的东西，可以把它理解成为基于BTC的Sandbox土地，但相对Sandbox要原生的多。因为每一个.bitmap铭文，都是映射比特币上的每一个区块，数量随着区块同步增加，现有81万多个Bitmap，每年增加5万个。Holder独立地址2万多，仅次于ORDI与SATS。



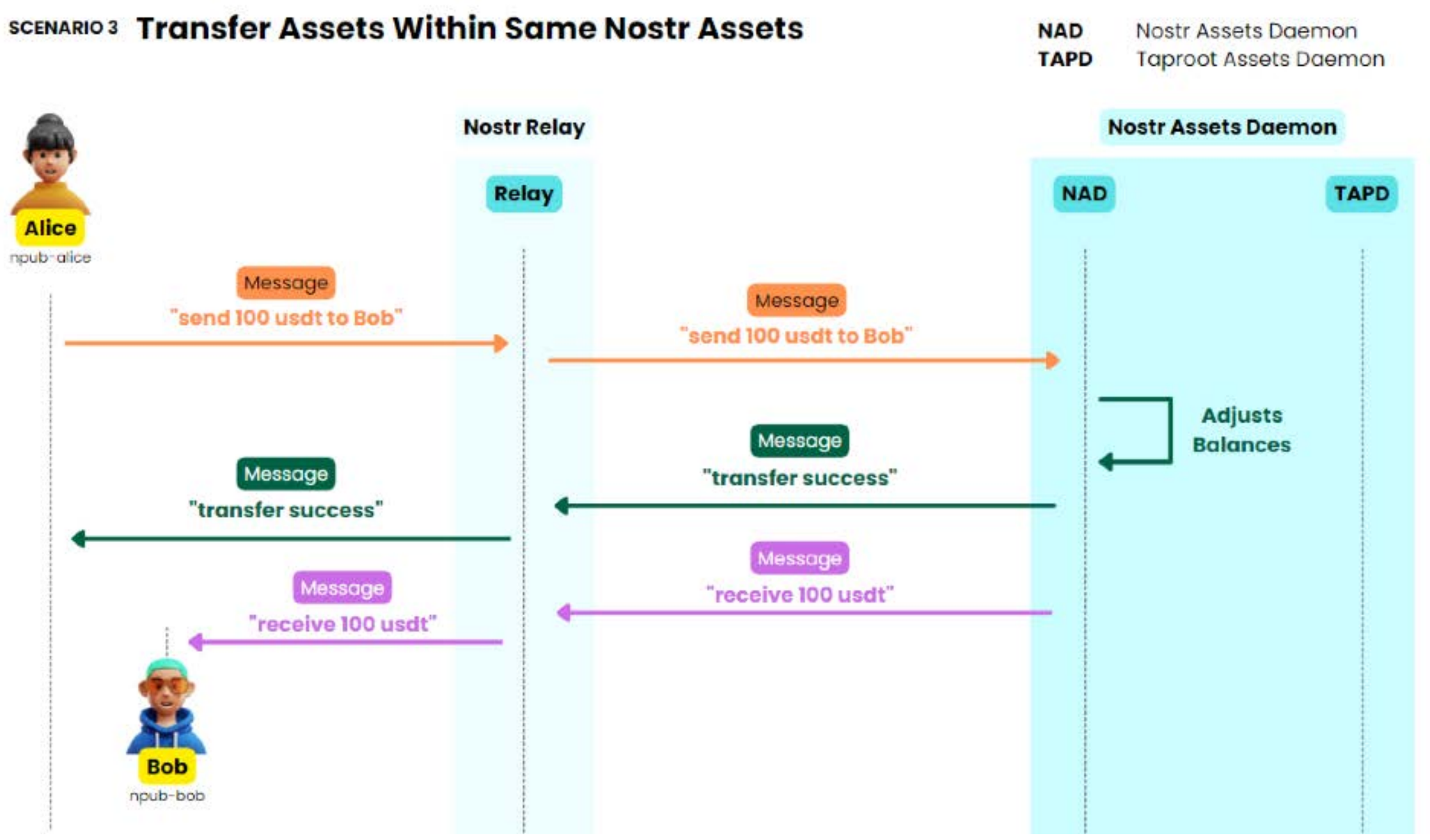

BRC420当然并不拥有Bitmap，但却是Bitmap背后最大的助推器，也垄断了Bitmap浏览器95%以上的流量，已有百余团队已在BRC420发行资产，可以说BRC420是一个与Bitmap深度绑定的应用协议。

## 2.5 Taproot Asset，RGB

这两个技术方案是Client Side Validation （客户端验证）的代表，也都是很多人眼里BTC扩容长期方案的最有力竞争者。

Taproot Asset值得一提的项目自然是Nostr Asset Protocol。与很多人想的不同，Nostr Asset与Nostr这个去中心化的社交网络消息协议关系并不是很大，因为其并非拿Nostr协议来发行资产，而是单纯作为一个Nostr上面的应用，通过使用Nostr消息来控制托管钱包，让用户通过Nostr的公钥和私钥在Nostr协议层发送与接收引入的

Taproot Asset资产。项目方也因为这个名字的事情在网络上饱受过一段时间的争议。




Taproot Asset会在明年上半年进行与闪电网络的结合测试，如果顺利的话，我们会在未来6–12个月看到更多Taproot Asset在闪电网络端的资产发行与新的应用。

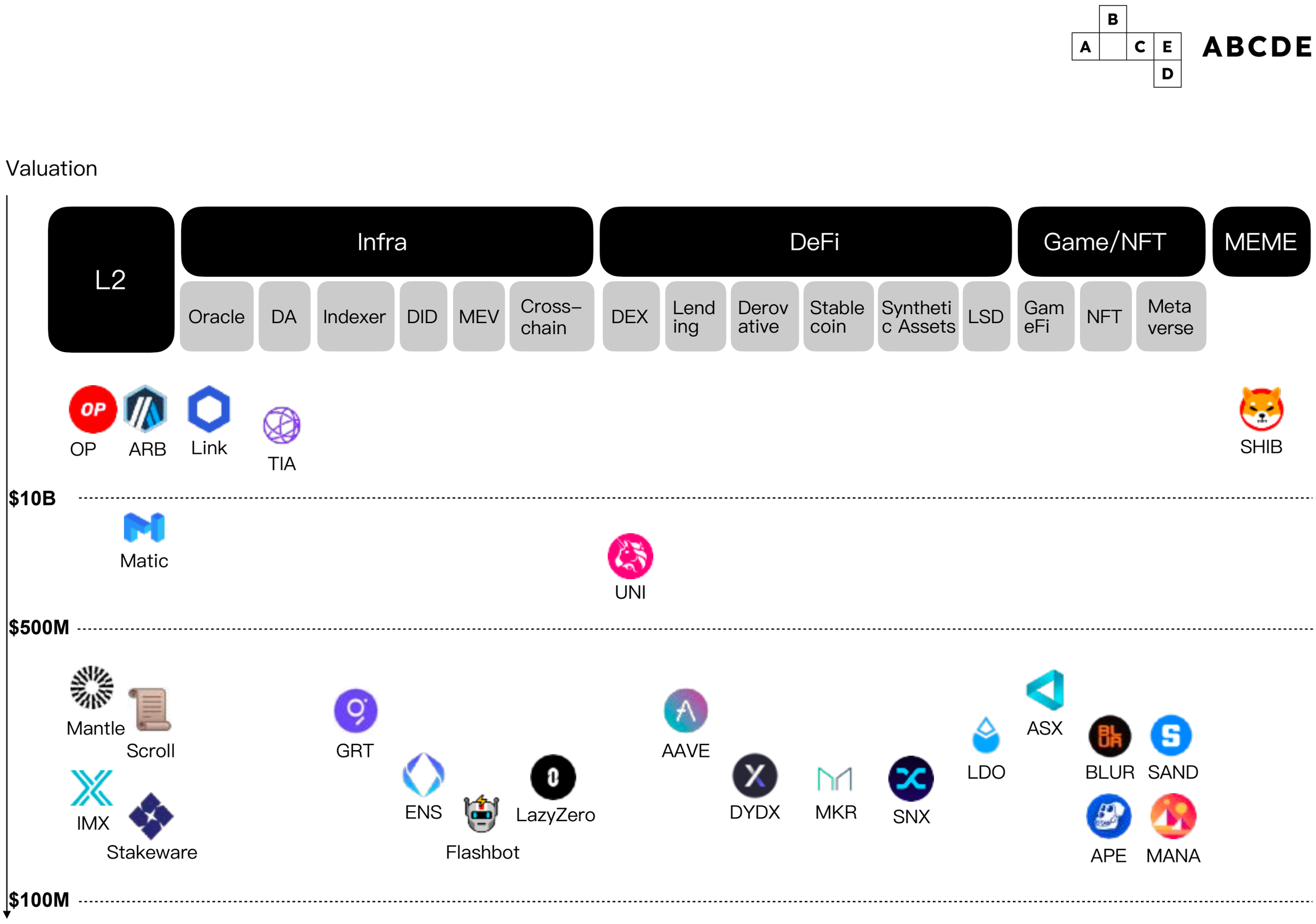
RGB在本轮火热的BTC生态算是基本踏空，但从长远来看依旧是BTC扩容的最佳方案之一，对智能合约的支持让其在可扩展性与灵活性方面更胜Tarpoot一筹，尤其是Tether有意在RGB发行USDT让其呼声甚高。基于RGB开发的团队数量也远远多过Taproot Asset。

但通过和多位RGB与Taproot开发者的交流得知，RGB当前的技术栈在于闪电网络的结合上困难重重，因此短期内Liquid侧链或许会是RGB的“临时选择”，创始人Maxim甚至有意新起一条Layer1来承载RGB。从正统性来看闪电网络无疑是最佳选择，但技术上的兼容问题能否克服，只有时间能给我们答案。

BRC420当然并不拥有Bitmap，但却是Bitmap背后最大的助推器，也垄断了Bitmap浏览器95%以上的流量，已有百余团队已在BRC420发行资产，可以说BRC420是一个与Bitmap深度绑定的应用协议。

# C3

# 比特币未来：步入黄金时代




当我们展望比特币生态的未来时，可以预见到在多个关键领域会有令人振奋的创新和变革。甚至可能会把过去几年以太坊生态的事情重新做一遍。

**1. Layer 2解决方案**

比特币网络的Layer 2解决方案是为了应对网络拥堵和交易费用高的问题。这些解决方案，如 BSquared是一个EVM Compatible Layer2，提供一个支持图灵完备智能合约的链下交易平台，提高交易效率并降低成本， 同时通过将零知识证明（ZKP）技术与比特币的Taproot集成，确保了交易的增强隐私性和安全性。该项目可以实现相比BTC更加便宜50倍以及更加快速300倍。团队还鼓励开发者在链上构建各种DeFi、NFT平台，该网络旨在将比特币发展成为一个动态平台。除此之外，Bitmap、Babylon都将开发自己的layer2的业务，Bitmap凭一层上的资产协议话语权与基数强大的社区，在layer2生态中有巨大的优势，Babylon 可凭借BTC质押带来的巨大流量赋能Layer2的建设。

**2. 资产发行与交易**

未来比特币生态中，预计将涌现更多的资产发行与交易平台，允许用户创建和交易各种数字资产。bitmap创新性的提出了 BRC420 协议，与 Ordinals 其他协议都是「单铭文」不同，BRC-420 协议是将多个铭文递归在一起，组合成一个复杂铭文。小到一个人物形象或宠物，大到将整个游戏脚本、虚拟机甚至 AI 大模型都可以组合成链上资产，以供开发者购买或支付版税。BRC-420 包含两部分，一是 Metaverse Standard（即元宇宙标准），二是 Royalty Standard（即版税标准），前者为元宇宙中的资产定义了开放格式，而后者则为创作者经济设定了链上协议。

**3. 稳定币**

稳定币在比特币生态中将扮演着重要的角色，为用户提供一种相对稳定的数字资产，旨在缓解比特币价格的波动性。这将增强比特币的用途，使其更适合作为一种稳定的价值储存手段。BitSmiley是BTC Defi的综合解决方案，填补了当前比特币铭文生态内最为缺失的“稳定币”一环。除了以BTC超额抵押形式提供兼容BRC20的URC20格式稳定币之外，BitSmiley还

提供基于BRC20的点对点借贷，以及搭建在借贷之上的保险和CDS衍生品，并已与多家BTC Layer2建立合作关系，为其提供稳定币与Defi生态产品。BitUSD整体的超额抵押机制与MakerDAO类似，铸币层面用户抵押BTC（既可以使用合作Layer2上的Wrap BTC，也可以使用BitSmiley自己的官方桥把BTC桥接进来）至BitSmileyDAO，然后mint出bitUSD。BitSmiley补足了当前BTC生态最为缺失的“铭文形态稳定币”一环，又通过借贷，保险，CDS衍生品等方案打开了BTC Defi新的大门，势必会成为BTC生态里不可或缺的关键组件型项目。

**4. 借贷&质押平台**

随着比特币的进一步普及，借贷平台将为持有比特币的用户提供更多金融服务的选择，如借贷、利息赚取等。这有助于推动比特币更广泛的金融化，吸引更多传统金融机构的参与。Babylon允许比特币持有者将闲置的比特币质押，以增加 PoS 链的安全性，并在此过程中获取收益。提出了一种比特币质押协议，该协议允许比特币持有者在无需桥接到 PoS 链的情况下质押比特币并且赚取stake 收益，并为该链提供完整的可削减安全性保证。该协议支持快速解绑，以最大限度地提高比特币持有者的流动性。此外，该协议被设计成模块化插件，可用于多种不同的 PoS 共识算法之上，并提供了可构建重置协议的基础。

**5. 跨链技术**

未来，比特币生态中的跨链技术将变得更加成熟，实现不同区块链之间的互操作性。这将加强整个区块链生态的协同作用，使得不同项目和区块链可以更容易地合作和交互。在没有智能合约的比特币网路中探索DeFi 应用，一种相对高效的方式，就是将 BTC 资产带入如以太坊等具有智能合约功能的公链中，直接利用其完善的DeFi 基础设施。Polyhedra Network推出了基于 zkBridge 的比特币跨链消息协议，以显著提高比特币网络的互操作性。这项创新旨在使比特币网络能够与其他一层（layer-1）与二层（layer-2）区块链网络进行高效且安全的跨链互操作。Polyhedra Network引入的比特币互操作性协议在区块链技术中标志着一次重大飞跃。通过使比特币网络既能作为发送方也能作为接收方，结合 zkBridge，这样的互操作协议为比特币与各种区块链网络之间前所未有的互动铺平了道路。

**6. 应用**

基于比特币的应用将蓬勃发展，涵盖多个领域。从身份验证到供应链追溯，各种去中心化应用将通过比特币的安全性和不可篡改性为用户提供更可靠的解决方案。

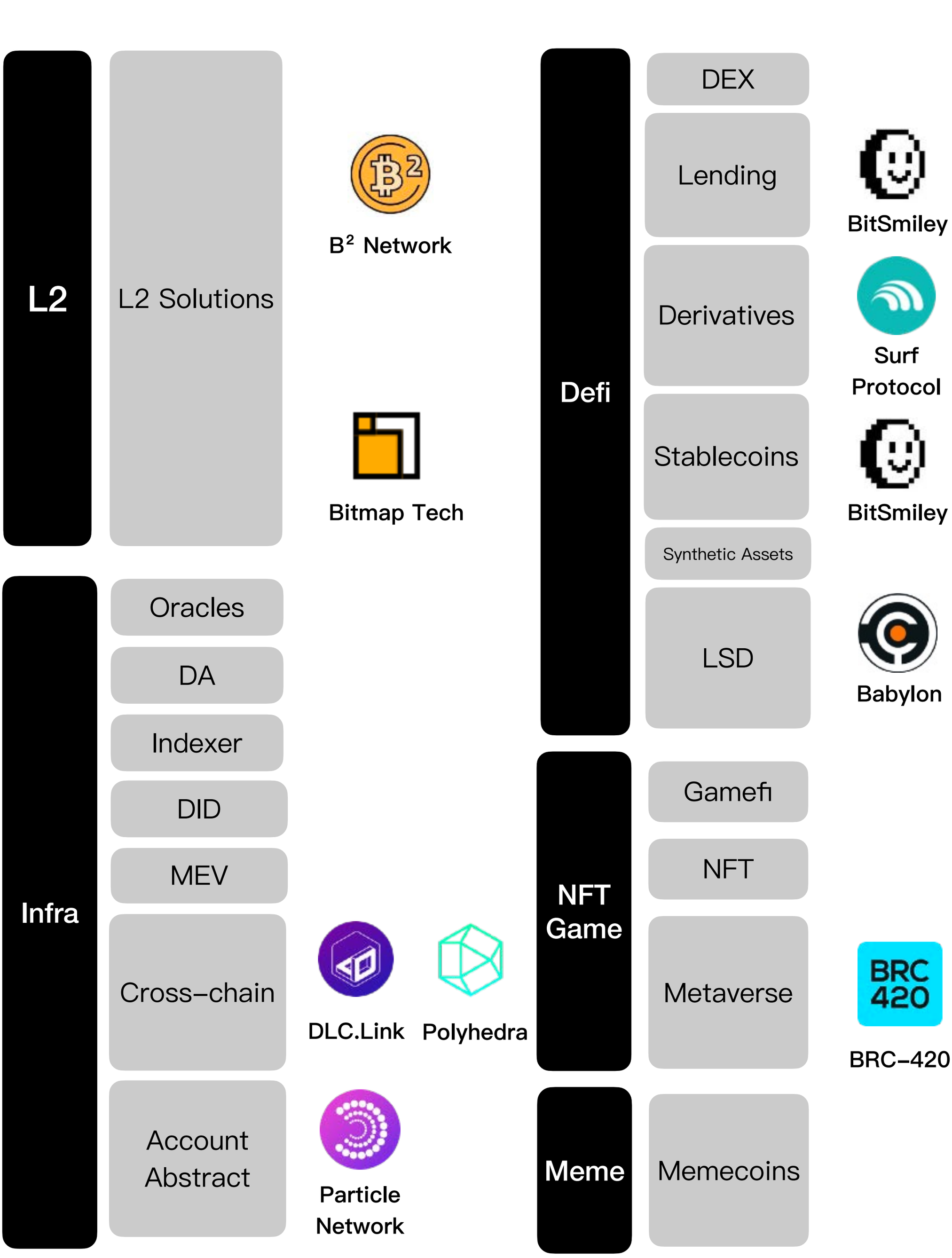
Bitmask是RGB上使用人数最多，最招牌的钱包，内置的Market Place （Coming Soon）可以方便RGB资产交易， 另外团队将会在下一阶段上线launchpad部分 。

RGB作为“原生扩容”方案，从逻辑和技术上来说是最适配BTC的。且RGB V0.1 正式发布已有半年，V0.11 Alpha 即将发布，RGB生态在半年之类有望起势。届时配合比特币减半，时机刚好。

## 7. MEV

MEV作为POW机制的一个特征，理论上也适用于比特币。在BRC20热潮中，一位比特币OG为了保护BTC免于铭文的粉尘共攻击，开发了一个名为「Sophon」的MEV机器，「Sophon」通过抢跑策略，快速部署相同名称的代币，设置供应量为1，通过支付高gas费率获取优先部署，阻止其他人再次部署相同名称的代币。Sophon短时间内引起了BRC-20代币的数量激增和下降，Sophon是BTC上MEV的一次尝试。然而在实践中，由于比特币交易主要是简单的比特币转账，MEV机会相对较少。但随着通过Taproot或Layer 2的努力将更复杂的交易引入比特币，MEV的机会可能会增加，特别是在比特币所有比特币都被挖完后，MEV可能作为一种新的挖矿收入来源。当前情况下，尚未出现鼓励矿工主动寻找MEV的经济激励，期待不久将会看到BTC Layer2上的Flashbot这样的生态项目。

## ABCDE BTC 生态投资版图



我们相信这些创新和变革将在未来塑造比特币生态，为其赋予更为广泛的可用性、可扩展性和适用性。**这个展望不仅是初步的想象，更是一个充满希望的前景，未来的实际发展将受益于技术的持续进步、社区的协同合作以及市场对于创新的不断需求。**

## 关于我们

ABCDE是专注于领投顶级Crypto Builder的VC，由Huobi Co-founder 杜均和前Crypto&Internet founder BMAN联合创办，作为创业者从0开始在Crypto行业建立了数十亿美元市值的公司，包括香港持牌上市公司新火科技（01611.HK）、交易所（Huobi）、SAAS公司（ChainUP）、媒体（CoinTime.com）、开发者平台(BeWater.xyz)等端到端的生态。

Twitter: @ABCDELabs

Email: b@ABCDE.com

Medium: @ABCDE

Website: https://www.abcde.com/

ABCDE

Thanks for reading!

## BITCOIN GENESIS BLOCK

### RAW HEX VERSION

```
00000000    01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00000010    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00000020    00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E    ....;£íýz{.²zÇ,>
00000030    67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA    gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040    4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C    K.^J)«_Iÿÿ...¬+|
00000050    01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00    K.^J)«_Iÿÿ...¬+|
00000060    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00000070    00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D    ................
00000080    01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F    ......ÿÿÿÿM.ÿÿ..
00000090    4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C    ..EThe Times 03/
000000A0    6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20    Jan/2009 Chancel
000000B0    73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66    second bailout f
000000C0    6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05    or banksÿÿÿÿ..ò.
000000D0    2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27    *....CA.gŠý°þUH'
000000E0    19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6    .gñ¦q0·.\Ö¨(à9.¦
000000F0    79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4    ybàê.aÞ¶Iö¼?Lï8Ä
00000100    F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57    óU.å.Á.Þ\8M÷º..W
00000110    8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00             ŠLp+kñ._¬....
                                                               ABCDE Labs
```

来ABCDE 办公室凭此报告领取限量比特币纪念版画