SAT20 协议白皮书

SAT20 协议

概述

SAT20 是一个"**聪本位(Satoshi Standard)**"的 BTC 原生资产发行和流通协议，其核心特征是**资产绑定聪**，跟随聪自由流动。 聪网是 BTC 主网的原生扩展协议，基于闪电通道+平行 BTC 网络，其存在的目的就是为了拓展 BTC 主网原生资产的流动性。聪网是 SAT20 落地的样本。

聪网 （SatoshiNet）

聪网是 BTC 主网的原生扩展网络，基于闪电通道+平行 BTC 网络，为 BTC 和主网的原生资产提供一个安全快捷经济的原生流通环境。聪网是 SAT20 协议落地的样本，基于 SAT20 协议建设。

聪网的特点：

1. BTC 的原生扩展二层网络
2. 无桥：基于闪电通道
3. 无币：所有资产来自 BTC 主网
4. 同共识：同地址，同网络费，同资产
5. 出块快，费用低
6. 支持智能合约

资产流通协议（STP）

SAT20 资产流通协议，聪穿越协议（Satoshi Transcending Protocol），是一个基于闪电网络通道的协议，定义聪资产的流通规则。

聪穿越协议的特点：

1. BTC 原生：继承闪电通道 RSMC 协议，由 BTC 主网确保资产安全，用户拥有掌控权
2. 全资产支持：支持 BTC 主网的原生资产协议，比如 Ordinals，Runes，BRC20，ORDX 等
3. 动态闪电通道技术
4. 简单的原子接口：

- ✧ 打开和关闭
- ✧ 锁定和解锁
- ✧ Splicing
- ✧ 聪交换

5. 兼容其他公链

资产发行协议（ORDX）

SAT20 资产发行协议，是一个强化版本的 Ordinals 协议，发行的资产称为聪资产(SAT20 ASSETS)，资产绑定在聪上，具有聪的属性：

1. 聪不可销毁，所以资产不可销毁。
2. 聪绑定的数据不可变更，所以资产发行后就不可变更。
3. 聪在哪里，资产就在哪里，资产跟随聪在不同的网络上自由流动。
4. 聪属于谁，资产就属于谁，转移聪时，资产也就跟着转移。
5. 聪的非均质化特性，决定资产的非均质化特性，资产天然具备 SFT 属性。
6. 聪可以绑定任意数据，甚至是智能合约，决定了资产具备某种意义上的智能化

愿景

一聪一世界。 One sat, one universe.
让每个人都能享受 BTC 网络带来的乐趣。

背景

聪做为 BTC 的基本单位，从命名开始，就已经赋予了深远的含义。如果 BTC 生态真的是 BTC 的发展趋势，那一个“聪本位”的资产发行和流通协议，是必然的结果，早晚会出现在 BTC 生态中。

1. 首先，聪资产是 BTC 原生资产发行最自然的方式，对 BTC 网络没有不良影响。资产只有在铸造阶段需要写入一些简单数据在 BTC 网络，其后不论转移还是进入二层网络，都不需要再写入任何数据，不会对主网有任何干扰。从另外一个角度来看，聪是用户的资产，聪资产通过这个绑定聪的方式，也自然属于用户，其安全由主网保证。无论从哪个方面来看，聪资产都是 BTC 生态中最自然最原生的资产发行方式。

2. 其次，聪资产天然适应 BTC 的技术发展。无论 BTC 的技术如何发展，未来有何种二层网络，聪资产必将是其中一员，不需要任何人的许可，也不需要多余的操作，聪资产就跟

随着聪的自由流动，流动到这些网络上。如果 BTC 一层的智能合约，比如 BitVM 能如期发布，聪资产一样可以使用于 BitVM 而不需要有任何的改动。

3. 最后，即使 BTC 还没有一种原生的扩展网络，那么探索实现 BTC 的原生扩展网络，让聪自由流通，让聪的价值得到充分的挖掘，也是 SAT20 的使命。在这种使命的推动下，我们创造出了聪网这样的扩展网络。

总之，SAT20 聪资产协议，是 BTC 生态发展过程中必然出现的产物，是“聪”这个 btc 最小单位的潜力的挖掘，也是 BTC 资产独特性的体现。而随着 BTC 技术的发展，聪的价值，会逐渐被认识并且充分利用起来。

聪网 SatoshiNet

介绍

聪网是 BTC 原生扩展二层网络，由闪电网络通道（RSMC 协议）和一个平行的 BTC 网络组成。

聪网是原生的，基于以下的核心技术：

1. 聪网的资产全部来自一层主网：聪网不发行资产，所有在聪网上的资产，都是来自主网。
2. 聪网的资产由主网保证安全：所有聪网的资产实际都在闪电通道中，而闪电通道的安全性由主网保证。
3. 用户拥有掌控权：无论任何时候，即使聪网关闭，用户也可以取回自己的资产，不需要任何第三方的配合。
4. 同共识：同地址，同资产，同网络费。

聪网是向**另外一个方向进化的闪电网络**。不同于原始的闪电网络通过 RSMC+HTLC 的组合来发展成为一个网络的架构设计，聪网保留了 RSMC 协议，放弃 HTLC 协议，充分挖掘闪电通道的潜力，让闪电通道变成一层网络和二层网络的穿越通道，同时使用一个平行的 BTC 网络作为二层网络来记录闪电通道的交易状态，让闪电通道的状态变更变成可追踪可回溯并且不可更改的 UTXO 账本记录，同时通过激活 OP_CAT，甚至是更多的操作码，让聪网变成一个具备图灵完备智能合约的网络。聪网真正让 BTC 生态具备跟 ETH 生态竞争的能力。
聪网是在 BTC 核心代码之上发展起来的，跟 BTC 主网相比，主要有这些不同：

1. 共识机制：POS
2. 出块速度：12 秒
3. 交易网络费用：10 聪

4. 增强的 UTXO 模式：支持任意资产的显式表达
5. 支持图灵完备的智能合约：激活 OP_CAT 等指令，让比特币脚本成为图灵完备的脚本

聪网也是不断进化的，所有在主网无法落地的技术，都可以在聪网实现其狂想，甚至有一天能通过聪网连接到其他所有的公链，让 BTC 主网真正成为价值互联网的基座。
聪网也是 SAT20 协议的最终目标，为 BTC 和主网上的原生资产提供一个安全快捷经济的原生流通环境。聪网为 BTC 生态的发展打开了一个全新的可能性。

原生性

比特币主网因为不支持图灵完备的智能合约（BTC 主网对安全和稳定要求，导致担忧激活 OP_CAT 所带来隐藏风险远远大于潜在收益，这导致激活 OP_CAT 基本是无望的），这决定了 BTC 生态的发展之路跟 ETH 生态是绝然不同的。

eth 因为有图灵完备的智能合约，所以一层网络可以对二层网络的交易数据做验证，这让 eth 二层网络的资产和交易具备由一层主网确保安全性的可能。而这一点，在 btc 生态完全没有可能性。简单说，btc 主网是一个孤岛，它不可能接受来自外界的交易数据和资产数据。换句话说，btc 生态的资产只可能在主网，资产的结算也只能在主网上。任何不在主网的资产，任何不在主网结算的网络，都不是 BTC 原生二层网络。从这个标准来看，唯一 btc 主网原生扩展网络就只有闪电网络。

但传统的闪电网络，并不支持目前 BTC 主网上的原生资产，比如 Ordinals NFT，BRC20，Runes 等等资产。这让闪电网络这个原生的二层扩展网络变得名不符实了。

聪网是向另外一个方向进化的闪电网络。传统的闪电网络通过 RSMC+HTLC 两个核心协议组成网络，而聪网放弃 HTCL 协议，选择 RSMC+平行 BTC 网络的方式，建设新一代的闪电网络。相比较传统的闪电网络，聪网具备这些优势：

动态闪电通道：传统的闪电网络通道是一个 UTXO，而聪网底层的聪穿越协议的闪电通道是一组 UTXO，而且随时可以通过 splicing 技术增加或者减少 UTXO，或者调整某个 UTXO 的容量。

支持 BTC 原生资产。传统闪电网络不支持主网主流的资产发行协议，而聪网支持所有协议，比如 Ordinals, ORDX, BRC20, Runes.

轻量化设计。目前应用最广的闪电网络版本，比如 lnd，没有轻量化版本，不能编译成 wasm 模块，无法运行于浏览器中。而聪网的闪电通道模块可以编译成 wasm 模块，可以运行于浏览器中。

除了这些不同之外，聪网的闪电网络模块完全继承了闪电网络 RSMC 协议，而该协议是闪电网络通道安全的保障。该协议确保用户随时可以通过广播承诺交易，取回属于自己的资产，也有能力构造惩罚交易应对作恶的通道对等方。这些机制同样在聪网上得以实现，这是用户确保自己资产安全的根本。

另外，聪网的这些特性，也是因为聪网是主网的自然扩展：

- 聪网的资产都来自主网
- 聪网的地址跟主网地址一致，用户没有任何违和感
- 聪网的网络费用也是使用 BTC
- 聪网的账本同样使用 UTXO 模型，因为其代码本来就是 BTC 源代码

总之，继承了闪电通道的原生性和平行 BTC 网络的一致性，聪网是原汁原味的原生 BTC 扩展网络。

安全性

聪网的安全机制由这方面来保证：

1. 基于 RSMC 合约的闪电通道，是主网的原生扩展，共享 BTC 主网安全，这是最关键的基础。
2. 基于 BTCD 源代码的聪网，由 BTC 技术提供技术层面上的安全，杜绝资产双花。
3. 聪网上的每一聪和每一份资产都来自主网，提供资产层面上的安全，杜绝资产增发/销毁。
4. 聪网的 POS 机制，从经济上确保聪网节点没有作恶的动机。

最终，聪网融合上面的因素，确保了整体方案坚如磐石般的安全，这一安全是建立在 BTC 的技术和共识基础上的。只要 BTC 主网技术和共识不出问题，聪网上的每一聪都是在用户的掌握之中，没有任何人可以拿走。

POS

聪网采用类似 ETH 网络的 POS 机制，矿机通过质押 Pearl 获得挖矿资格，并且通过一个非盈利的基金会组织引导和推动聪网的建设和发展。

BTC 主网已经足够安全，而聪网的资产都来自主网，而且资产都是锁定在闪电通道中，用户拥有掌控权，所以聪网的去中心化要求并不高，采用 ETH 的经验构建一个 POS 的共识网络，完全可以获得足够的去中心化水平，同时兼顾了 BTC 主网最欠缺的高效率，并且因为聪网的 POS 机制，其对硬件算力要求基本没有要求，也进一步降低了维持聪网的成本，这最终降低了聪网交易网络费用。

总之，聪网的 POS 共识是跟主网的 POW 共识是非常完美的互补关系，各施其职，为 BTC 生态提供一个安全、稳定、高效、经济的基础。

增强型 UTXO

在一层网络，UTXO 仅有聪的数量，并没有包含其他数据。当聪穿越到二层网络后，其属性会在 UTXO 中完全体现，这极大提升了 UTXO 的能力。

enUTXO 中将包含聪的数量和资产信息，这极大方便聪的流转和聪上资产的验证，除了杜绝双花之外，也让聪网支持任意一种资产提供可能性，还能很直观的了解一个资产的流转历史。

智能合约

聪网支持两种形式的智能合约。

1. 模版合约：直接通过 OP 指令，将某个合约固化在聪网源代码中。
2. 激活 OP_CAT 指令，支持图灵完备的链上智能合约。

流动池

流动性池子是聪网维持低成本运作的关键模块，降低了动态调整通道导致的费用飙升的几率。聪网基金会有责任建设一个公共的流动性池子，提供最基础的流动性。

流动性池子也可以由第三方运营。

基金会

聪网基金会是一个非盈利组织，是一个专注于推动聪网生态系统发展和技术创新的非营利组织。它致力于支持聪网平台的研发、教育、推广及基础设施建设。

职责

1. 聪网技术的研发
2. 聪网网络的基础建设和扩展
3. 资助基于聪网的开源项目
4. 促进聪网的教育与推广

收入来源

1. 捐赠
2. 聪网核心业务的分成：挖矿，资金池
3. 参与聪网核心业务：挖矿，资金池

组织结构

1. 执行董事会
2. 技术团队
3. 运营团队
4. 社区与教育团队

管理模式

1. 去中心化决策
2. 透明度和公开性

重要项目

社区与文化

战略合作和未来发展

备注：聪网基金会并不是 SAT20Labs 主导的组织，聪网基金会也不是 SAT20Labs 的上层组织，相互之间并没有统辖关系。我们在这里只是提供了发展聪网基金会的建议。

经济模型

聪网的收入来源主要是两个部分：交易的打包费用（也就是网络费用），资金进出聪网的资金池的收益。聪网基金会从这两个收入源中提成，早期从 20%开始抽成，然后根据网络发展，逐步下降。

1. 基础假设 为了更好地考虑平台方和交易池参与者的收益来源，采用以下参数：

- 每笔交易打包费用：固定 10 聪
- 日均交易量：
  - ✧引导期：从 0 起步，到每天 0.1 万笔交易，让网络稳定下来，准备好更多项目进入
  - ✧建设期：每日交易量从 0.1 万-10 万，至少有 10 个比较活跃或者大的币种入驻
  - ✧成熟期：10 万-1000 万，至少 100 个活跃币种交易
  - ✧爆发期：1000 万以上，最热门的 BTC 生态币种都在聪网交易

2. 挖矿节点 挖掘节点通过锁定 Pearl 获得挖矿资格参与挖矿。
   - 全网质押目标：50,000,000 $Pearl （资产总量的 33%） 对应上面的四个建设期，每个阶段要求的节点不同。 质押数量暂时按照 100 万枚 Pearl 计算。
   - 引导期：3-5 个节点，不考虑经济利益。
   - 建设期：10-100 个节点，交易量每天小于 10 万笔。如果有 100 个节点，平均每个节点每天打包 72 块，每块有 10 个交易，每块收益 10x10=100 聪，每天收益 72x100=7200 聪，每年 2628000=0.02628btc，以 10 万美金每 BTC 计算，大约是 2628u。
   - 成熟期：100 个节点以上，假设还是 100 个节点，但是交易量增加 10 倍，那么每个矿机每年的收益增加到 26280u，这个时候质押的 pearl 应该不需要 100 万枚，可能只需要 10 万枚。
   - 爆发期：理想情况，聪网每天的交易量 1000 万笔，矿机 1000 台，每台矿机质押 10 万枚 Pearl，流动性基本锁定在矿机。如果交易量能够到 1 亿笔，质押量可能就下降到 1 万枚 Pearl。

3. 流动性池子 流动性池子提供进出聪网的流动性。聪网基金会主导两个池子（BTC 和 Pearl），在不同阶段，池子要求的资金也不一样（目前没有可以测算数据）。这两个池子的收入由基金会支配，基金会负责建立并管理这两个池子。如果资金来自第三方，原则上按照池子的资金比例获得盈利分成，但需要考虑基金会的提成。

4. 收益分配模型 原则：
   - 谁提供服务，谁获得收益。
   - 基金会从收入中分成，用于生态建设。不同时期分成比例不同
     - ✧引导期：不分成
     - ✧建设期：20%
     - ✧成熟期：10%
     - ✧爆发期：1-5%，最低确保 1%的分成

流动性池参与者收益

以最终的爆发期计算。每天聪网交易量 1000 万笔，预计其中 1%的资金进出聪网，而进入聪网不收费，退出聪网收取服务费，假设这个费用采用固定的基础服务费(5000 聪)+1%的资金费率。假设每天 1 万笔交易退出，平均一笔 1 千刀（100 万聪），这一笔交易需要支付 5000 聪固定服务费+1 万聪资金费，共计 1.5 万聪，那每天有 1.5 枚 BTC 的费用。当然这里面还有至少 0.5-1 个 BTC 的调整通道和清扫各种零散 utxo 的费用，但也有 0.5 个 BTC 的盈利。但是，需要多大的资金池，才能支撑起这个盈利呢？假设资金池整体需要 1000 个 BTC，每天盈利 0.5 个 BTC，一年就有 183 个 BTC，相当于有 18%的盈利，这应该是很高的估算值。而这个盈利，按照成熟期基金会分成 10%之后，也有差不多 16%的收益。

以爆发期的数据为例：

1. 资金池总投入：1000BTC
2. 资金池总收益：0.5*365 = 182.5，大约$18,200,000
3. 假设交易池初期总资金规模为 $100,000,000，参与者按资金比例分享收益：
4. 年化收益率： 18,200,000/100,000,000×100% = 18.2%
5. 单个参与者示例：
    - ✧ 质押资金：$10,000
    - ✧ 年收益：10,000×18.2%=$1,820

挖矿节点收益

所有的节点，都需要支付一部分收益给基金会，最多 20%。 另外，普通挖矿节点，需要支付给核心节点的数据服务费，最多 10%。 剩下的都是节点运营方自己的收入。

以爆发期的数据为例，每天 1000 万笔交易，1000 个节点，每个节点平均打包 1 万笔交易。

1. 单节点收入： 每天：10000x10 聪 = 10 万聪 每年：100000 x 365 = 0.365BTC，约 3.65 万 u 其中基金会分成 5%，核心节点分成 10%，剩下 85%，约 3.1 万 u
2. 单节点成本 成熟期，质押 10 万枚 Pearl，价值可能是 10 万 u 矿机的硬件成本不高，硬件+网络成本一年费用小于 3000u
3. 单节点回报率： 成熟期，单节点回报率 30%

动态调整机制

为了平衡平台收益和参与者吸引力，同时适应市场发展，可以加入以下动态调整机制：

1. 基金会分成比例：从一开始的 20%，逐步下调，可能会稳定在 1-5%。
2. 聪网网络费：目前是 10 聪，未来随着 btc 价格的提升，聪网交易量的加大，这个费率有可能下调，最终可能下降到 1 聪。

备注：这里只是作为建议提出，最终实施方案由基金会审核批准实施。

不断进化

聪网也是不断进化的，从诞生的第一天开始，它就是不断进化的产物。聪网是闪电通道协议

向另外一个方向进化的产物，不同于传统的闪电网络；聪网也是主网技术不断进化的产物，所有历史上种种导致 BTC 网络分叉的技术或者理念，都可以在聪网上落地，并且持续发展，比如大区块，比如更多的 OP 指令，比如更快的打包速度等等。

聪网可以提高打包速度，只要一个区块填充完成，就可以马上出包，不需要等待。这可以让出块速度提高到网络吞吐容量的极限和本地计算验证的极限。在现代网络的计算机硬件的支持下，1 秒成 4M 数据的传输和验证，是很轻松的工作。这个角度，已经可以轻松达到 1 秒一万笔甚至更高的交易容量。

聪网可以有计划扩大区块大小，如果有这个需求的话，只要网络和硬件能跟得上，16M 甚至更大区块都可以胜任。

聪网可以为了图灵完备的智能合约激活各种 OP 指令，这让聪网具备发展原生第三层网络的可能性，或者有可能连接到其他公链。聪网将变成 BTC 主网对外连接的中介网络，BTC 通过聪网可以自由流通到所有网络，真正释放 BTC 和主网原生资产的威力。
更多的想象空间，可能在于各种基于聪网的应用服务上。 比如聪网天然支持 BTC 主网的 DID，如果聪网再增加一个 DA 服务，等等。其无限的想象空间留待每个人自己去想象，去创造。

备注：从技术可能性来说，聪网既然可以成为 BTC 主网的原生扩展，那同样的协议，也可以应用到 ETH 网络上。只要 ETH 网络支持聪穿越协议的接口，ETH 就可以通过聪穿越协议，通过闪电通道连接到 BTC 主网。这样 BTC 和主网的原生资产就可以流通到 ETH 网络上。或者退后一步，不直接连接，而是通过聪网连接，是不是更简单一点？也有了一定的缓冲。 另外，反过来可行不可行？比如让 ETH 进入 BTC 主网流通？

[场景]

SATSWAP

聪交换市场是聪网上的第一个应用，为聪网上的资产提供一个高效的交换平台。

稳定币

聪网上的稳定币，除了能发挥稳定币该有的作用之外，在某种程度上还能弥补闪电通道的容量调整成本比较高的问题。

微支付

聪网的费用很低，天然适合各种微支付应用的发展，比如基于 AI 的服务。

DePIN

很多 7-8 年前的老手机，已经具备 4 核 CPU 和 2G 以上的内存，还有 16G 以上的存储空间，这样的手机足够当作一个轻量级的节点，提供一些计算和存储服务。而且这些旧手机的耗电量极小。如果大量这样的手机连接起来形成网络，就会产生规模效应。

非常妙的是，SAT20 的资产，仅仅与聪相关，聪的数量虽然大，但是需要的存储空间和计算量其实非常小，每个人家里放一台旧手机当作轻量级的节点，就形成一个去中心化的索引服务网络，不仅仅可以验证自己的资产，也可以维护整个网络的安全，更可以提供一些存储和计算服务，分布式保存网络数据，执行 SVM，借此赚取一些服务费用。

一个由旧手机组成的去中心化的 BTC 资产索引服务网络。

资产流通协议 STP

概述

SAT20 资产流通协议是一个关于聪资产如何进入 BTC 原生二层网络，在二层网络如何交易转移，如何安全退回一层主网的协议。其核心技术基础是闪电通道的 RSMC 协议，通过该协议，资产锁定在主网，并且用户拥有资产的控制权，随时可以将资产取回。

SAT20 资产流通协议仅仅是一个协议，并不是二层网络。BTC 生态需要一个原生的二层网络，能够支持 BTC 主网原生资产在聪穿越协议的支持下自由流通到二层网络上。何谓 BTC 原生二层网络？我们认为标准只有一个，那就是用户完全的掌控权。用户必须能够完全掌握自己的资产安全，不需要经过任何人的许可，随时都可以进入二层网络，或者从二层网络退出，不会影响资产的安全。

SAT20 资产流通协议的核心概念有以下几个：

1. 聪锁定和解锁：通过闪电通道技术，将聪锁定在主网上，然后在二层网络解锁进入二层网络。或者相反的过程回到主网。
2. 聪穿越：锁定在主网的聪，自动穿越到二层网络。
3. 聪交换：锁定在通道中聪，通过聪交换技术，在不同的通道中穿梭。
4. RSMC：闪电网络的核心技术，确保用户对通道中的资产拥有控制权。
5. 动态通道容量调整技术：通过 Splicing 技术对闪电通道的容量进行调整。
6. 支持主网上的主流资产发行协议：Ordinals, ORDX, Runes, BRC20 等。

协议

聪穿越协议的核心是闪电通道，协议的主要内容是协调操作聪资产在一层网络和二层网络的流动。资产的流动实际就是资产所有权的流动，因为聪和资产都是锁定在主网，只是将资产的所有权转移到到二层网络进行流通，最终还是需要回到主网做资产最后的结算。

协议的原则是用户是主动方，基本上所有动作都必须由用户主动来发起，而远端服务节点作为自动应答的机器人，根据协议自动应答，配合用户的操作。这个原则确保所有的操作都是用户意图的体现，最大限度确保用户的资金安全。

一层网络是主网，二层网络可以是任何支持聪穿越协议的公链，我们以聪网为例。

打开通道

这是标准的闪电网络通道的打开方式，用户提供打开通道的资金，远端服务节点自动应答，协助打开通道。打开通道后，根据闪电通道 RSMC 协议，用户就持有了承诺交易。这是用户资金安全的根本保障，在远端节点不应答的情况下，用户也可以自己广播承诺交易，取回自己的资金。

同样，远端服务节点也持有承诺交易。双方的地位是对等的。

现在，用户可以通过其他的操作，来对通道中资金的所有权进行分配，或者调整通道的容量。这些操作，都会引起承诺交易的更新。双方都只持有最新的承诺交易。如果一方广播了老的承诺交易，另一方就有能力构造一个对应的惩罚交易，清扫这个老的承诺交易的输出，结果相当于把通道中的资金都清扫到自己的地址中。这也是闪电通道 RSMC 协议赋予用户的能力。

聪穿越协议的另一个重要功能，是在打开通道时，将通道中的聪资产，自动 Ascend 到聪网，并在聪网上生成对应的 UTXO。这时资产就穿越到了二层网络了。

关闭通道

用户随时可以决定关闭通道取回属于自己的资金。关闭有两种方式，协商关闭和强制关闭。

1. 协商关闭：正常情况下，远端节点都会在线，自动支持用户的关闭请求。协商关闭的好处是双方资金可以在交易确认后就可以马上花费，费用最低。
2. 强制关闭：在远端节点不在线或者永久关闭的情况下，用户可以广播最新的承诺交易，取回自己的资金。跟协商关闭不一样的是，承诺交易会将资金先输出到一个中间地址，用户只有等待一个默认的 CSVDelay 的时间后（一般是 144 个区块），才能花费这些输

出。

在执行通道关闭的同时，二层网络上相关的资产，必须执行一个 Descend 操作，将这些资金从二层网络上穿越会一层网络，确保聪网上的每一份聪资产，都是锁定在通道中的。

解锁和锁定

打开通道后，资产自动穿越到二层网络，但是还是锁定在通道中。可以想象一层网络和二层网络是两个水库，通道连接这两个水库，锁定在这通道中的水，其实就是处于一种临界状态，需要经过特殊的操作，才能真正进入一层或二层网络。进入或者退出二层网络的操作，就是解锁和锁定；而进入或者退出一层网络的操作，就是 splicing。

解锁和锁定是在二层网络上执行的操作：

1. 解锁：将资金从通道中释放到用户在聪网的地址上。以后用户就可以跟在主网一样，自由签名使用自己的资产。
2. 锁定：将资金锁定回通道。主意通道的容量是固定的，解锁和锁定操作无法改变通道容量，所以能不能锁定回通道，受通道容量限制。

Splicing

splicing 是闪电网络中的一种新协议，目的是用来动态调整通道容量，只不过应用最广的 LND 还没有实现 splicing 功能。 我们使用 splicing 技术来对通道进行动态调整。

splicing 技术是在一层网络上执行的操作:

1. splicing-in：将新的 utxo 拼接进闪电通道，扩大通道容量。这个操作相当于给通道充值，可以充任意的资产进入通道，只要索引器支持。
2. splicing-out：将闪电通道中的资产，通过拆出部分 utxo 的方式输出到指定的地址。这相当于从通道中提取资产。

同样，在执行 splicing 操作是，因为效果相当于给二层网络充值/提取资产，所以涉及到的资产，必须自动完成 Ascend/Descend 操作，确保二层网络中的资产跟通道中的资产是严格匹配的。

以上，就是聪穿越协议的核心技术，完全基于闪电通道，是目前 BTC 生态中，另外一种原生的扩展协议。

聪交换

聪绑定的资产，在聪交换技术的支持下，可以在不同的 utxo 之间穿越，这是聪获得超流动性的核心。

聪锁定，聪穿越，聪交换，是 SAT20 资产流通协议的核心技术，这一技术确保了用户资金的安全的前提下，让聪和聪资产得以自由流动在 BTC 原生网络中自由流动，不论是一层还是二层。

RSMC

在闪电网络中，RSMC（Revocable Sequence Maturity Contract）是一种合约类型，用于确保闪电网络通道的安全性和可靠性。 RSMC 是基于时间锁定的合约，它允许参与方在特定条件下撤销或关闭闪电网络通道。它的设计目的是防止欺诈行为和恶意操作，并确保交易的安全性。 用户的资产都是锁定在通道中，用户通过持有承诺交易，并且有能力构造惩罚交易来确保自己资产的安全。在任何时候，用户都可以不需要任何第三方的许可，取回自己的资金。

动态通道

传统的闪电网络通道是一个 UTXO，而聪穿越协议的闪电通道是一组 UTXO，而且随时可以通过 splicing 技术增加或者减少 UTXO，或者调整某个 UTXO 的容量，甚至是将一个多签地址作为整个闪电通道管理起来，这种灵活性是将资产从主网带到二层网络所必不可少的。

1. 多 UTXO
2. 任意增加、减少 UTXO
3. 任意调整 UTXO 大小

全资产支持

聪穿越协议支持主网上的原生资产发行协议，包括 Ordinals, ORDX, Runes, BRC20 等协议。实际上，只要是基于 UTXO 模型的资产发行协议，都可以被聪穿越协议所支持，都可以上到聪网进行交易。

兼容性

聪穿越协议是一个独立的协议，有能力将 BTC 主网上的资产，不管是 BTC，还是 Ordinals，Runes，BRC20，ORDX 等等资产，在用户的完全掌控之下，穿越到另外一个网络，只要这个

网络能支持聪穿越协议的原子接口(UTXO 类型的公链天然支持，有智能合约并且支持资产发行和销毁的公链也支持)。

聪穿越协议的这个能力，来源于闪电通道的 RSMC 协议。如果我们将 BTC 主网看做一个水库，而其他公链，比如 ETH 当作另外一个水库，那么聪穿越协议的作用，就是使用闪电通道将这两个水库通过一个管道连接起来，然后通过聪穿越协议控制这个管道中的水，如何进入和退出，而且这个过程是用户自己可以完全掌握的。

资产发行协议 ORDX

介绍

SAT20 资产发行协议是一个在 BTC 主网上发行全类型数字资产的协议，其核心是**绑定聪**，所以称为聪资产（SAT20 ASSETS）。聪资产具有鲜明的特征，是世界上第一个“**聪本位**”的 BTC 原生资产发行协议，资产具备聪的属性。

SAT20 资产的基本属性

1. 聪不可销毁，所以资产不可销毁。
2. 聪绑定的数据不可变更，所以资产发行后就不可变更。
3. 聪在哪里，资产就在哪里，资产跟随聪在不同的网络上自由流动。
4. 聪属于谁，资产就属于谁，转移聪时，资产也就跟着转移。
5. 聪的非均质化特性，决定资产的非均质化特性，资产天然具备 SFT 属性。
6. 聪可以绑定任意数据，甚至是智能合约，决定了资产具备某种意义上的智能化

SAT20 资产的基本能力

SAT20 资产的发行依赖两个基本能力：

1. 识别聪和跟踪聪的能力
2. 在聪上读写数据的能力

SAT20 资产的核心原则

SAT20 资产基于聪的两个基本属性建立起来，这也是 SAT20 资产的最核心的原则：

1. 聪的非均质化特性。聪的出生顺序决定了聪是独特的，可识别的，可以用某种编码方式来给每一个聪编码，这个编码就是聪的身份证，永不变更。

2. 聪的不可销毁特性。BTC 是一个账本模型，本质上要求账本平衡，聪做为账本的输入和输出，不可能销毁，否则账本将不平衡。

其他相关服务

另外，为了更方便的索引聪和读写聪，一些基于聪的核心服务也必须建立起来：

1. 名字服务。基于聪，方便记忆和传播，是 IP 建设的基础，也是协议发展必不可少的核心服务。
2. 数据服务。读写聪绑定的数据，只有所有者才能写，任何人都可以读。以后支持有收入的业务在读取数据时需要付费。
3. 付费服务。SAT20 支持编译成 WASM 格式的软件在 VM 上运行，有收入的业务在 VM 中运行其他软件包时需要付费，费用由节点提供商和软件开发者分享。费用低廉，但不为零，以聪计价。

协议验证版本在高度 827307 正式启用，正式版计划在高度 845000 正式启用。

协议

SAT20 资产发行协议只有 deploy 和 mint 指令，不需要 transfer 指令。

Deploy

KEY	Required	Description
p	Yes	协议名称: ordx
op	Yes	指令: deploy
tick	Yes	名称: 只允许 3 或 5-16 个字符，（为 brc-20 保留 4 个字符）
lim	No	每次 mint 的 token 的限额，默认是 10000。如果 deploy 特殊 sat 上的 token，默认是 1。
n	No	每聪绑定的 token 数量，默认是 1，最大是 65535。(v2)
selfmint	No	自己铸造的比例（两位小数），只有持有该 ticker 的地址才能铸造（父子铭文）。
max	No	mint 的总量，64 位整数。
block	No	mint 的开始高度和结束高度（开始-结束）。
attr	No	sat 的属性要求，比如"rar=uncommon;trz=8"，可扩展。
des	No	描述内容

例如，公平发射的 ticker：

```
{
    "p": "ordx",
    "op": "deploy",
    "tick": "satoshi",
    “block”: "830000-833144",
    "lim": "10000"
}
```

或者，项目方控盘的 ticker：

```
{
    "p": "ordx",
    "op": "deploy",
    "tick": "Gamever",
    "selfmint": "100%",
    "max": "1000000000",
    "lim": "10000"
}
```

部署 ticker 的规则：

1. ticker 的名字必须没有被用过
2. 如果有 block 参数，要求该 deploy 被确认的高度，必须比 start 高度大 1000 以上 违背规则的 ticker 无效。

attr 是一个可以扩展的属性，目的是让越来越多特殊的 sat 可以通过这个属性被筛选出来。目前支持的属性有：

1. rar：稀有度，在 Ordinals 中定义：common, uncommon, rare, epic, legendary, mythic
2. trz：trailing zeros，尾部为零的数量，比如 trz=8，说明该 sat 的编号的尾部有 8 个零
3. 未来支持自定义的属性

mint

KEY	Required	Description
p	Yes	协议名称: ordx

op	Yes	协议名称: ordx
tick	Yes	名称: 只允许 3 或 5-16 个字符，（为 brc-20 保留 4 个字符）
amt	No	mint 得到的 token 的数量，默认等于 lim，不能超过 lim
sat	No	sat 的序号，设置了 attr 属性的 ticker，mint 时需要提供满足条件的 sat

例如：

```
{
  "p": "ordx",
  "op": "mint",
  "tick": "satoshi"
}
```

每次 mint 时，需要做的规则检查：

1. 协议必须是 ordx
2. op 必须是 mint
3. ticker 必须已经部署过
4. amt 小于等于 deploy 的“lim”
5. 如果 deploy 有“selfmint”：
   - 只有持有 ticker 的地址才能 mint（父子铭文）
   - 该次铸造的数量，加上已经铸造的总量，不超过 max*selfmint
6. 如果 deploy 有”max“：该次铸造的数量，加上已经铸造的总量，不超过 max
7. 如果 deploy 有”block“：该次 mint 的 block 高度要在规定之内
8. 如果 deploy 有“attr”：mint 时检查指定的 sat 是否具备以下属性：
   - 如果有 rar 属性：检查该 sat 是否是这种类型
   - 如果有 trz 属性：检查该 sat 的序号是否有足够的尾数零
   - 如果有自定义属性，根据自定义规则做检查

如果不满足以上规则，当次 mint 无效。

协议 v2.0

SAT20 资产发行协议 ORDX 会在兼容老版本的基础上，根据 BTC 生态建设的需要，不断对协议进行升级。

本次升级主要是为了支持聪资产更好的在二层网络流通，同时让协议更简洁，更好用。

本次升级内容:

数据写入方式

ORDX 协议的数据写入方式，从最初的铭文方式，升级为 OP_RETURN 数据方式。

新的指令

v2.0 版本主要支持 ordinals nft 的销毁和交换指令。 这两个指令的效果是永久的，由 owner 发起执行，将对应的 ordinals nft 永久销毁，或者转移到另外一个聪上。

数据格式： OP_RETURN | MAGIC_NUMBER | CT_TYPE | CONTENT
MAGIC_NUMBER = OP_16
CT_DESTROY = OP_4
CT_SWAP = OP_5

销毁的 content： Satoshi | Inscription Number

交换的 content： assetName |（start, end） | (start, end)
注意输入的聪范围，必须是自己能控制的聪；但输出的聪，不一定是自己能控制的聪，也就是可以远程交换，直接将聪的绑定资产送给其他人。 如果该 utxo 中该资产有多个 range，每个 range 都需要有一个 op_return 来执行。 assetName 的格式：协议：类型：tickername（如果是 nft，填 inscription_number）

探索新功能

stake/unstake 跟 deploy 有类似的地方，但其资产发行方式需要通过质押指定的资产才能发行对应的新资产。这可以简化质押资产的管理方式。 该操作指令必须配合聪网的通道才能生效。质押发行的资产不绑定聪。 assetName | amt

备注：请注意以上新功能仅处于探索阶段，并没有正式实施。

聪的编码：序号

SAT20 严格按照聪的出生顺序来给聪编号的，严格保证**编号和聪一一对应并且从 0 递增**。这意味着，在有效范围内，每一个序数都对应一个聪，每一个聪都对应一个序数。这种严格的一一对应关系是永久不变的。该序数的基本原则：

1. 第一个聪的序数为 0。
2. 按照出生顺序递增编号，没有空缺。
3. 聪的转移遵循先进先出原则。
4. 在奖励交易中，奖励的聪做为第一个输入，其他交易作为费用的聪按顺序排在后面。
5. 奖励数量与实际奖励数量严格相等。

SAT20 的序数理论脱胎于 Ordinals 协议，但是跟 Ordinals 协议有原则上的不同：

1. Ordinals 协议认为聪是可以销毁的，而且实际上，在 ordinals 序数理论体系中，在区块 840000 之前已经销毁了 2895502904 个聪。这一结果可以通过查询 ordinals 网站确认（https://ordinals.com/status）。
2. Ordinals 协议按照理论给聪编号，导致有很多的序数背后并没有实际的聪对应。举个例子，在高度 840000，也就是第四次减半，其区块的第一聪，epic，序号是 1968750000000000，这会让误会在 btc 已经发行了 19687500 枚 btc。但实际上，到这个高度之前，网络上仅仅有不到 19687497.2 枚比特币，原因是历史上有很多个奖励区块没有足额领取奖励。所以在 ordinals 序数理论中，在第四次减半的 epic 聪 1968750000000000，之前有很多个序数，背后并没有聪的存在。

SAT20 不直接沿用 ordinals 协议的序数理论，核心原因就是我们认为聪是不可销毁的，这一点跟 ordinals 协议的序数理论形成本质的区别，导致我们无法基于 ordinals 的序数理论发展 SAT20 资产。所幸的是，ordinals 的序数理论已经正式进入 BIP 的流程中。我们期待聪早日有一个正式的编号规则，我们也希望聪的编号能更符合 BTC 的基本原则，并且按照实际情况对聪编号。等聪的编号有了标准方案，我们将第一时间响应标准的聪编号规则，这不会影响 SAT20 的资产的安全性。

另外，SAT20 完全支持 Ordinals NFT，主要原因是因为 Ordinals NFT 是一种绑定在聪上的资产，符合 SAT20 资产的定义，也就是说 Ordinals NFT 也是一种 SAT20 资产。

（具体背景请参考 github issue：
https://github.com/ordinals/ord/issues/3690#issuecomment-2083950493 和
https://github.com/ordinals/ord/issues/3702#issuecomment-2081429205）
（
备注：ordinals 理论现在已经有了正式的 BIP 编号，正式进入考察流程。Ordinals 理论成为 BTC 标准的可能性非常的高。最终 Ordinals 理论使用的编码方案，都会成 SAT20 的编码方案。具体参考：https://github.com/bitcoin/bips/pull/1408 ）

聪的读写：铭刻

在聪上写数据的技术称为铭刻（inscribe，来源于 Ordinals 协议）。

目前在 BTC 主网上写入数据的方式有如下几种：

1. UTXO，比如 SRC20 的数据写入方式
2. SegWitness，隔离见证区，比如 Ordinals 的写入方式
3. OP_RETURN，比如 Runes 的写入方式

SAT20 支持多种方式在聪上铭刻数据，其目标是尽可能不影响 BTC 网络的安全。目前 SAT20 采用 Ordinals 协议的铭刻技术。 在未来，SAT20 会根据实际的情况，支持更多的数据写入方式。

资产发行模式

SAT20 资产的发行有三种主要模式，主要根据这三个参数进行调节：

1. selfmint：自己铸造的比例，必须设置 max 参数
2. max: 发币总数
3. block：可以铸造的区块高度区间

项目方主导

项目方主导的项目，必须设置 max 和 selfmint 参数，可以有两种方式：

1. 完全控盘 selfmint: 100%
   max: 64 位整数，必须设置
   block: 可设置也可不设置

这种模式下，只有持有 deploy 这个 nft 的地址才能铸造，资产将由项目方完全持有。 比如稳定币，一般都是由项目方铸造。

2. 部分控盘 selfmint: 小于 100%的某个值，比如 10%
   max: 64 位整数，必须设置
   block：必须设置，并且开始区块至少在部署确认之后的第 1000 个区块

这种模式下，持有 deploy 这个 nft 的地址，最大不能超过设定的比例。超过部分无效。 其他地址可参与铸造。规则参考公平发射。

公平发射

selfmint: 不设置
max: 64 位整数，可设置也可不设置
block: 必须设置，并且开始区块至少在部署确认之后的第 1000 个区块

这种主要由社区主导的发行模式，主打社区成员公平铸造，由 block 控制。 deploy 的确认区块必须是开始区块的 1000 个区块以上，否则该 ticker 无效。 如果有 max 限制，即使结束区块未到，总量达到了，其他 mint 也无效。 如果结束区块达到，而 max 未到，也无法再 mint。

无限制

selfmint: 不设置
max: 可设置，也可不设置
block: 不设置

这种模式下，mint 被其他因素制约，不可能无限制 mint，具体制约条件，由项目方设置。比如，要求在某种稀有聪或者某个 ticker 上继续铸造。

我们期望通过这种模式的设置，让项目有完全的选择权，也让参与者能清楚知道，参与的项目是哪一种类型的项目。

聪对象

在传统的软件中，数字对象是可以无限复制的、廉价的对象。仅仅是这样普通的廉价的默默无闻的数字对象，结合算法，就构建起了我们现在的整个软件世界，包括传统互联网。在传统互联网往下一代互联网进化的过程中，一种完全不同的数字对象，已经呼之欲出，成为构建下一代互联网的基础。不可复制，有独特的价值并且有主，是这种全新的数字对象最核心的属性。

这种新的数字对象都是有价的并且有主的，复制出来的赝品一文不值，谁是创造者毋庸置疑，first is first。其内容的使用如果带来利益，谁获得利益也清清楚楚。这样的数字对象自带价值，自带权益和归属权，还天然带有可编程性。这是价值网络的最佳底层基础。这是可以发挥创造力的最佳载体。

btc 的最基本单位，聪，就是这样一个真正的有价值承载的数字对象，我们称之为“聪对象”。

无法凭空创造，也永不销毁。是你的，就不可能被夺走。有史以来，第一个具备如此之多让人过目难忘的属性的数字对象。潜力无限。我们无法用言语表达出的赞叹，只能归功于中本聪的巧夺天工的构思。

“聪对象”的独特属性：有价，独特，有主，可编程性，在 BTC 主网和二层网络，会迸发出什么样的创新？我们无限看好，并且积极参与。

名字服务

聪是我们整个协议生态的基础，其序数可以看作是聪的索引。但是，序数是一个 64 位的整数，太长，不容易记住。为了更快索引到每一个聪，我们有必要发展一套基于聪的名字服务，供用户记住每个对他来说意义重大的聪。序数跟名字的关系，和 IP 地址和域名的关系类似。SAT20 的名字服务，是一种完全去中心化的，基于 BTC 的名字服务，每个人都可以公平使用，不受任何第三方控制。
名字服务的核心，是每个名字都是唯一的。没有子名字空间。这避免了欺诈的可能性。 每个名字都是一个铭刻在聪上的数据，是一个 nft。一个聪只有一个名字，名字和聪也是一一对应的。 名字绑定在聪上，谁拥有聪，名字也就属于谁。聪转给谁，名字也就转给谁。 名字也是一种聪资产。

命名规则

1. 名称的第一个实例有效。
2. 名称使用 UTF-8 字符。
3. 大小写无关。所有名称/命名空间都将以小写形式索引。
4. 名称不允许有空格。
5. 名称不允许标点符号。(带句号的名字，都是来自其他名字协议)
6. 名字长度，从 3 字节开始申请，但 4 字节暂时禁止注册。

注：4 字节预留给 BRC20 的 ticker。1-2 字节协议内部使用，从协议层面禁止注册，永不开放注册，杜绝无谓的炒作。

组合规则

名字可以组合起来，形成某种特别含义。协议制定基本的规则如下：

1. 名字用@符号组合起来，比如 Alice@sat20
2. 组合名字时需要双方都签名许可，也就是说组合是一种契约关系

3. 后一个名字，比如 sat20，属于组织形式上更高一级的名字，比如是公司，俱乐部等一些组织

兼容性

SAT20 名字服务兼容目前 BTC 网络上的主要名字服务。比如.btc 为例，某个名字，1.btc，将做为一个整体，而不是分成名字 1 和名字空间.btc。根据我们的开发进展，我们计划兼容这些名字服务：（只读取名字，不支持铸造）

1. .btc
2. .x
3. 其他

注意，带.的名字，和不带.的名字，是不同的名字，比如 123.btc 和 123，是两个独立的名字，相互之间没有关系。

垄断性资源

名字是一种核心资源，也是一种资产。比如 Ticker 名字 Pearl，就是一个名字，由 Deploy 这个 ticker 的地址自动持有。如果一个名字已经被注册，其他人就无法部署这个名字的 ticker。通过注册某个名字，将自动获得该名字相关的所有权限，SAT20 协议维护这种权限。

版税

拥有某种资源的人，在资源被使用时，会自动根据某种可配置的税率收取版税，资源所有人自动获得版税收入。

D-Indexer

Indexer 可以相互连接起来，形成一个去中心化网络。这是一个对 BTC 生态非常重要的网络，是用户节点得以真正运作的网络，即使是手机，也能成为节点。 这个去中心化网络的核心功能，将逐步揭晓。

[场景]

FT

每一个 coin 都绑定在聪上面，聪在哪里，coin 就在哪里。以下是一些例子。

东方之珠


```
{
   "p": "ordx",
   "op": "deploy",
   "tick": "Pearl",
   "block": "828200-828800",
   "lim": "10000",
   "des": "The Oriental Pearl."
 }
```


大概在 2024 年 2 月 1 日前后开启 fair mint，持续到 2 月 5 日左右结束（由区块高度 828200-828800 决定有效的 mint 时间）。这是 sat20 协议的第一个 token，也是一个 meme 币，仅供试验，没有价值，不要 FOMO。

还可以在稀有聪上铸造 FT，这是我们计划做的试验：

矿工的翡翠


```
{
   "p": "ordx",
   "op": "deploy",
   "tick": "Jades",
   "lim": "1",
   "attr": "rar=uncommon",
   "des": "Miner's Jades."
 }
```


每个区块的第一个 sat 才能 mint 成功，预计每个 Jades 值 1 个 BTC。

数字黄金


```
{
   "p": "ordx",
   "op": "deploy",
   "tick": "Golds",
   "lim": "1",
   "attr": "trz=8",
```

"des": "The first satoshi in a BTC"
}
每个 BTC 的第一个 sat 才能 mint 成功。该 sat 的序号的末尾是 8 个 0。这意味着，每个 token 值一个 BTC。

NFT

到目前为止，Ordinals 协议已经是最优秀的 BTC 主网上发行 NFT 的协议，但是对合集的管理不太好。

现在，SAT20 继承了 Ordinals NFT 的铸造能力，并且增强了 NFT 的能力和合集的管理，简单介绍如下：

1. 使用 Ticker 对合集进行管理：SAT20 使用 ticker 来对 NFT 合集进行统一的管理，每一个铸造结果都是该 ticker 合集中的一次有效铸造，索引器已经为 ticker 的管理提供了全面的数据支撑。
2. 自定义设置铸造条件：SAT20 的铸造条件可以直接用在 NFT 的铸造上，方便项目方对 NFT 的铸造设定更多的条件。比如只能在某个区块高度内铸造，铸造时每个 NFT 包含多少聪，甚至可以对聪的属性进行设定，要求在某一类稀有聪，或者具备什么属性的聪才能铸造 NFT。
3. 为 NFT 的进一步变化提供可能性。到目前为止，Ordinals 协议铸造的 NFT，在铸造完成后就是确定的，不再改变。但是 SAT20 提供了进一步变化的可能，让该 NFT 在构成自身的聪发生变化之后，再次发生变化。

SFT

SAT20 的本质就是 SFT，FT 或者 NFT 仅仅是其某种表现形式。SAT20 的 SFT 本质，来源于两个方面：

1. 资产的底座，聪，本身就是非均质化的，可以通过聪的编号来体现
2. 聪还可以绑定不同的数据，这为 SFT 的使用带来无限的想象空间

我们通过以下例子，说明 SAT20 的 SFT 属性。

Pizza

基于稀有聪 Pizza 铸造的 SFT，演示图币一体的特性。 聪的数量和属性，决定 Pizza 的显示样式，比如是一堆 pizza，还是一张 pizza，还是 1/n pizza；馅料也会改变，不同聪属性有不同的馅料。

稳定币

发行多套稳定币，每套具有不同面额，比如 1 元，10 元，100 元，1000 元等。 每套根据需要铸造多张 NFT，每一聪就是一枚 coin。 稳定币铸造在聪上，跟聪流动到二层网络，承担交易媒介，减少二层网络对大量 BTC 的要求。

RWA

以房产为例，比如一栋大楼做为一个 Ticker 发布，每个房间算一个 nft，这个 nft 可以拆成多份，方便交易和流通。

游戏装备

游戏装备可以通过组成该 NFT 的聪的属性不断调整，可以充分激活交易。

小结

SFT 具有无限的潜力，以太坊上的 ERC3525 就是很好的的例子。

DID

基于 SAT20 名字服务，实现 DID 的以下特性：

1. 唯一性：每个 DID 是唯一的，不重复的，以确保标识的独特性：由协议从底层支持 DID 的唯一性。
2. 去中心化：DID 不依赖于中央机构或中介来验证或管理，而是由参与者自主控制和验证：谁拥有持有该名字的聪，谁就是该 DID 的主人。
3. 可验证性：DID 具有可验证性，可以通过密码学证明来验证其所有权和控制权：同上。
4. 持久性：DID 的生命周期应该是持久的，不会因为某些变化或失效而失效：聪是不可销毁的，铭刻在聪上数据也不可销毁。

DeIP

基于 BTC 的去中心化网络，DeIP（Decentralized Intellectual Property）具有以下基本属性：

1. 去中心化性质：创作者提交在 BTC 网络上的作品，自动获得 DIP。
2. 知识产权保护：类似开源软件，学习和个人使用不用付费，收费的业务使用需要付费。

3. 去中介化：通过智能合约、分布式账本或其他去中心化技术来实现 DIP 的授权、验证和管理。
4. 可验证性：数据铭刻在聪上，谁持有该聪，谁就是该 DIP 的 owner。

简单说，上链的数据自动成为具有 IP 的数字资产，有收入的业务使用属于别人的数字资产，需要支付一些费用。

路线

SAT20 是我们建设 BTC 生态的开始。在这个发展过程中，我们坚持这样的原则，也是我们对未来趋势的判断：

1. 资产在 BTC 主网上发行：BTC 主网上会有越来越多的资产。
2. 资产在二层网络上交易：无限的流动性，同时资产不脱离用户的控制，安全，经济，快捷。
3. BTC 网络将成为未来价值网络的基础，一聪一世界必将到来。

SAT20 资产发行协议（ORDX Protocol）

2024 上半年完成资产发行协议的开发工作。

SAT20 资产流通协议（Transcending Protocol）

一个让 BTC（聪）自由流通的协议。 我们希望在 2025Q1 中完成穿越协议的开发。

原生扩展网络：SatoshiNet

SatoshiNet 是一个魔改的 BTC 网络，基于 BTCD 源代码，是第一个基于聪穿越协议的 BTC 主网原生扩展网络。任何有利于 BTC 发展的技术，都可以在这个网络上试验。聪网预计 2025Q2 正式上线。

聪交换市场：SatSwap Market

聪交换市场是聪网上的一个 DEX，由 ordx.market 负责开发并运营，提供聪网的资产交易服务。 ordx.market 是一个 BTC 生态中提供完整的资产铸造/浏览/交易/管理的专业平台，支持 BTC 生态中所有主流资产，支持一层和二层网络，在以后以聪网为中心，连接更多的生态和公链。 聪交换市场预计在 2025 年 Q2 跟随聪网同时上线。

开源计划

为了早期开发的效率，我们先完全闭源开发。 我们计划逐步开放并最终开源整个 SAT20 项目，最终通过社区管理的方式将 SAT20 变成完全去中心化的项目，继续发展 SAT20 协议。

SAT20 协议不是一个孤立的协议，而是一个可以融合任何 BTC 原生技术的协议，比如 BTC 的原生智能合约，或者任何 BTC 原生二层网络等未来技术。 我们希望通过开源、无许可的合作方式，推动 SAT20 在 BTC 生态中的大面积使用，为 BTC 生态的繁荣贡献一份力量。 欢

迎对 SAT20 感兴趣的团队一起加入建设聪的世界。

计划：

1. 提供安装包，帮助合作团队自建服务节点 （2024.06 开始）
2. 逐步开源，成熟一个模块就开源一个模块 (2024Q4 开始推进开源)
    - ✧ 索引器
    - ✧ 流通协议
    - ✧ SAT20 钱包
    - ✧ SatoshiNet
3. 探索社区管理模式，继续推进 SAT20 发展 （开源后推进社区管理，让 Pearl 成为治理币：提案，投票...）

API

- [API]

捐赠

我们没有发行任何 token 来募集资金，只通过网站收取的服务费来支持项目的发展。你如果想支持项目发展的话，请考虑捐赠!

捐赠地址为 bc1ppejz29yxpz66yzkaxh6dek8pzsm8aajne6p4qak0xhxphkwzqnmsw45sur

收到的捐赠款将用于资助项目的维护和进一步开发，同时将支付 sat20.org 的托管费用。

感谢你的捐赠!

关于

我们是一群技术乐观主义者，一个聚焦于 BTC 生态的技术团队，我们只专注协议的开发。我们不发行任何资产，也没有任何的官方社区。任何使用 SAT20 协议发行的资产都是社区行为。我们愿意在技术上给社区提供支持，只要是符合 SAT20 协议原则并且在我们能力范围之内。我们将持续建设 SAT20 生态。

链接

- GitHub
- Twitter
- 官网