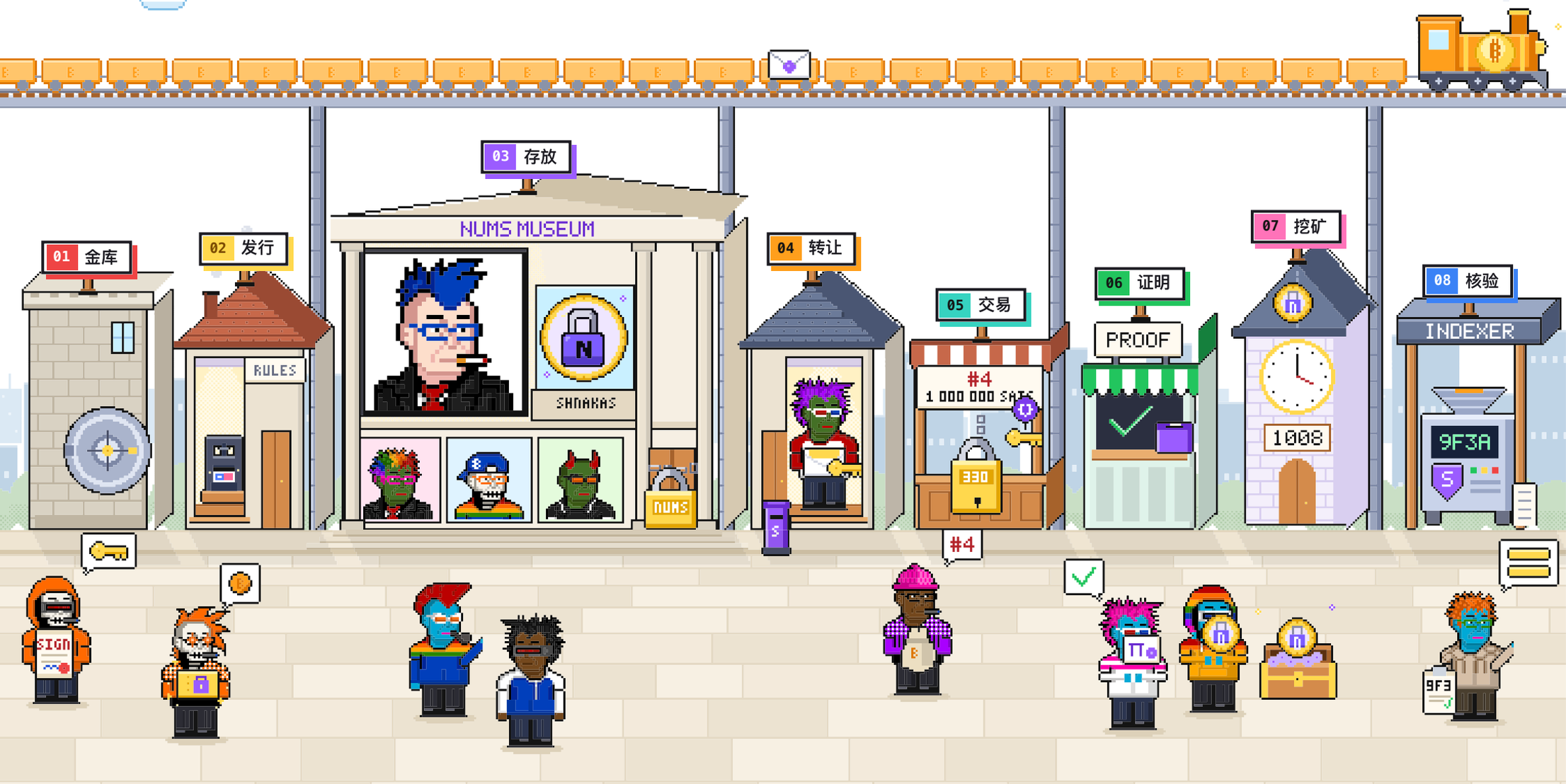
SHIELDED ORDINALS · 原理图解

SHORD

持有私密，证明公开

比特币原生的隐私协议



00 导读

SHORD 是什么，你持有的是什么

> **SHORD 是比特币上的隐私协议：作品公开，谁持有哪件不公开。你持有的是一张票据，记着哪一件、归谁；链上只留它的指纹，明文和钥匙都在你自己的金库里，只有你的钥匙能花它。**

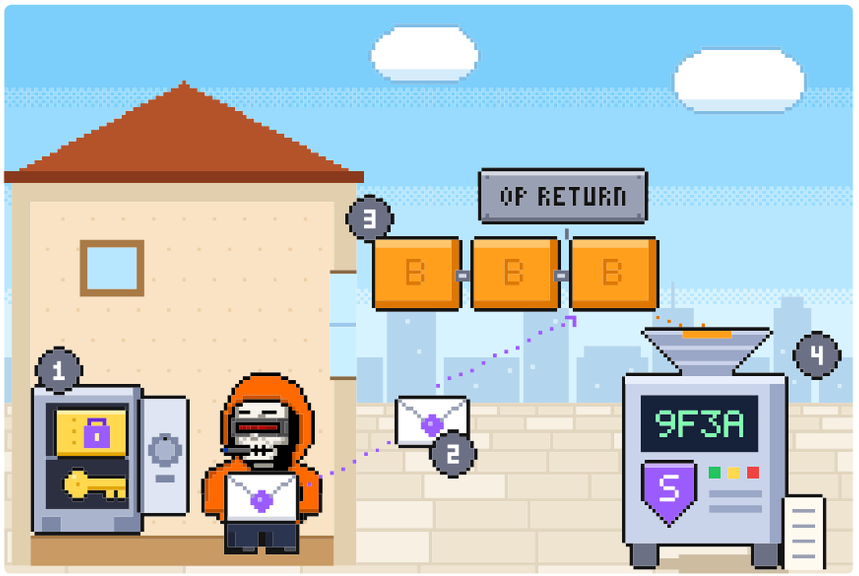
图中

1. 金库：在你自己的设备上，放钥匙和票据明文，证明在这里做。
2. 信封：每次操作写进一笔比特币交易发出去，作品的信封在 OP_RETURN 输出里（图上的牌子）。
3. 区块：比特币按顺序记下交易，谁都能读。
4. 索引器：逐块按 SHORD 的规则验收信封，把公开的账记在自己机器上；屏幕上的 9F3A 是账的摘要（第 08 章）。

普通 Ordinals 作品放在谁的地址里就归谁，谁都查得到。SHORD 把作品停在谁也花不动的 NUMS 地址，持有关系改记在票据里，它自己的说法是“作品公开，持有人隐藏”。比特币只认 BTC 交易本身，SHORD 的账由索引器按规则来算，所以一笔交易比特币确认了，SHORD 仍可能不认。本文拿 Shielded Nakas（NAKA）和持有它挖出的符文 SHNAKAS 举例。

链上公开的	链上看不出的
作品本身和它停放的地址	作品归谁
SHORD 交易本身，以及信封里的作废码和密文	私密转账花的票据和收件人
挂单编号、价格和收款方式	金库钥匙和票据内容

提醒 打开网页金库时钱包签的那段签名，能算出金库的全部钥匙，别给任何人（第 01 章）。



技术卡 00 以一次私密转账为例：每样东西从哪来、放在哪

东西 · 用途	金库	比特币区块	索引器
钥匙 花票据、读密文	从种子算出 只在本机	不上链	不碰钥匙
票据明文 记着哪一件、归谁	转出方做好 收件方解出保存	不上链	看不到明文
承诺 cm 票据的公开指纹	转出方算好	写进信封	加进记录树
密文 ct 收件方靠它读出票据	用收件方的 查看公钥加密	写进信封	存着，供金库扫描
作废码 nf 防止一张票据花两次	花旧票据时算出	写进信封	记进作废码清单
证明 π 证明这笔转账合规	转出方在本机生成	写进信封	验过就算 不存进账

索引器这一列全从区块算出：同一条链、同一版规则，谁重放都得到同样的结果

技术说明 技术卡给想核对实现的人看，跳过不影响读正文。这张卡以一次私密转账为例；铸造、购买和取回由收的人自己做新票据，承诺由索引器补算，也不带证明。证明参数的来历见附录 D。



技术卡 01 一份签名，算出全部钥匙

钱包对官网这段固定文字签名
`Ord Dropz shielded vault key v1 …`

↓

`seed = SHA-256("shord/seed/v1" ‖ sig)`

↓ 种子算出各把钥匙和地址

花费密钥 spend	查看密钥 view	取回密钥 return	卖出收款 payout	金库 BTC btc
花掉票据	解开密文	取回挂单	这次挂单专用	收 BTC、找零
种子直接算出		种子 + 这次挂单的作废码		种子 + 序号

同一签名，同一金库
同一钱包、同一账户
和同一地址类型
换了就是另一个空金库

签名泄露 = 金库交了出去
能转走作品、取走金库的 BTC，
看到你持有过哪些作品

钱包自己的 BTC 不在其中
签名推不出钱包私钥

技术说明 卡上的 ‖ 表示前后接起来。每把钥匙都是 SHA-256(固定标签 ‖ 种子 …) 算出来的，标签是 shord/spend、shord/view 这样的固定文字。手机上的 24 个助记词，就是这 32 字节的种子加一字节校验。隐私地址 shord1… 是持有人公钥 Poseidon(sk) 接上查看公钥，两样都推不出私钥，所以能公开。

01 金库

持有靠什么，钥匙从哪来

持有，就是握着钥匙：金库里的钥匙花得动哪张票据，你就持有哪件作品。网页金库的钥匙，全部由钱包的一份签名算出：这份签名就是整个金库。

图中

1. 官网：钱包在这里签一段固定文字，金库就打开了。
2. 签名纸：这份签名算成金库的种子。
3. 影子是一串钥匙：种子算出金库的全部钥匙。
4. 仿冒网站：招牌只差一个字符（红色的 0），签了名，钥匙就归它。
5. 手机：同一个种子编成 24 个助记词（不是钱包的助记词），在 Shielded Vault 里打开的还是这个金库。

钥匙不用另外备份。换台设备，用当初那个钱包的同一账户、同一地址类型再签一次，打开的还是这个金库；换成别的，打开的是另一个空金库。票据都在链上的信封里，金库拿钥匙扫一遍就找回来；眼下只有官网的索引器列得全，项目方说新版本会开源，到时自己搭的索引器也行（附录 H）。

收作品用的隐私地址 shord1… 也由种子算出，可以公开给别人。官网写着它“只有别人直接给你发送藏品时才需要”，买和卖都用不着。

签名框里写着：“Anyone with this signature can move your shielded pieces.”这份签名算出整个金库，管的不只是作品，还有金库里的 BTC 和收过的票据。

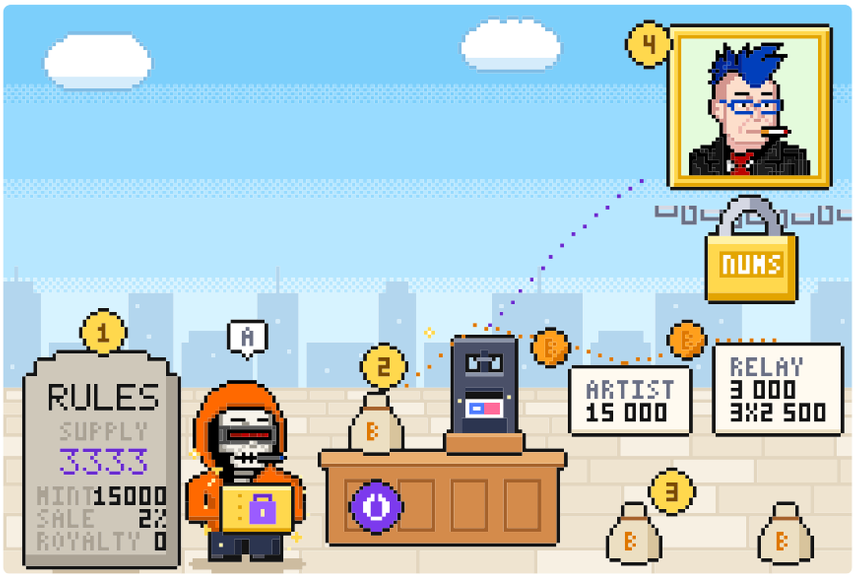
误解 不转钱，只签个名，不会丢失资产。

事实 **这份签名就是金库的全部钥匙。只在官网签，不给任何人。**

02 发行

规则写在父铭文，铸造的钱分给谁

合集从一枚父铭文开始，供应量、价格和收款地址都刻在里面。铸造照规则付钱，索引器照规则验收，对不上就不算。



图中

1. 规则石碑：父铭文，碑上刻着 NAKA 的供应量和价目。
2. 铸造：A 带着自己金库做好的票据在柜台付款，交易花掉一枚平台许可币（柜台上的紫色币）。
3. 分钱：15,000 给艺术家，铭刻费和 3 个额度给中继。
4. 铸好之后：平台另发交易，把作品铭刻成子铭文，停进 NUMS。

索引器验收一次铸造看三件事。编号要在供应量内，还没铸过。付给每个收款脚本的钱不能少于规则写的数，多付不算错。交易要花掉一枚许可币，NAKA 的许可币只有平台能签。三样都对上，索引器才收下这次铸造。新票据由铸造的人自己的金库生成，索引器补算承诺。

按官网默认，铸一件顺带买 3 个中继额度，合计 25,500 sats，矿工费另算，每一笔给谁见技术卡。中继额度是预付的代发次数，一个额度让官方中继代发一次私密转账、挂单或撤单（第 04 章）。

NAKA 的作品文件不先上链：父铭文不放图，只放全部文件的哈希树根，图铸出来以后才铭刻上链。父铭文要等最后一件铭刻完才停进 NUMS，之后谁也不能再给它添子铭文；10 月 28 日它还没停进去（附录 G）。SHNAKAS 符文另有蚀刻，不在父铭文里（挖矿原理）。

技术卡 02 规则刻在父铭文，付款照规则验收

父铭文 · 刻在链上的规则（NAKA，单位 sats）			
作品	供应量 3,333	文件树根 artRoot	
铸造	铸造价 15,000	铭刻费 3,000	平台铸造费 0
中继、成交	中继额度 2,500/个	成交费 2%，最低 1,000	
公钥	铸造许可公钥 gateKey	挂单锁公钥 lockKey	
收款	艺术家、平台、中继三类收款脚本；NAKA 的艺术家和平台是同一地址		

↓ 索引器从父铭文的交易里读规则，不经网站

铸造一件（MINT）

15,000 → 艺术家
3,000 铭刻费 → 中继
3 × 2,500 额度 → 中继，官网默认
平台铸造费 0
合计 25,500，矿工费另算
交易花掉一枚许可币

成交一件（BUY）

标价 → 卖家
2%，最低 1,000 → 平台
买家在标价之外另付
例：标价 100,000，买家共付 102,000
NAKA 没有版税
交易花掉挂单锁

误解 合集规则是网站后台的设置，项目方可以修改。

事实 **规则刻在父铭文里，刻下就改不了，网站后台也改不了它；索引器只认链上这一份。**

技术说明 信封头里的合集编号，是父铭文编号 SHA-256 的前 8 字节，索引器只收带这个编号的信封。许可币是锁在平台许可公钥上的一枚比特币输出，每笔铸造交易花掉一枚；批量铸造一笔最多 20 件，也只花一枚。



技术卡 03　**一张票据，链上只有承诺和密文**

内容

票据：明文只在金库里，不上链

编号	额度	持有人公钥	随机数	作品秘密
assetId	tickets	ownerPk	ρ	s

计算

```
inner = Poseidon(ownerPk, ρ, s)
cm = Poseidon(assetId, tickets, inner)
```

= 承诺：进记录树的指纹

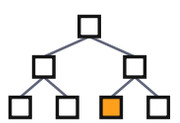
```
ct = Enc(assetId, tickets, ρ, s)
```

= 密文，用收件人的查看公钥加密

私密转账：转出方的金库算好 cm 和 ct，再附证明
铸造、购买、取回：收的人交 inner 和 ct，索引器补算 cm

存放

信封（cm 或 inner，加 ct）→ 比特币区块（永久公开）



记录树只收 cm：一片叶子

技术说明　记录树深 20 层，最多收 1,048,576 张票据，只增不减：每张新票据一片叶子，票据花掉了叶子也还在。花票据时，证明以最近 100 块里的某个树根为准，只说明票据在树上，不说是哪一片；是否已经花过，由索引器查作废码清单（第 04 章）。

03 存放

作品在哪，你买到的是什么

> **你买到的不是那张图，是一张票据。图铭刻后停在 NUMS 地址，谁也转不走；转手时换的是票据，图一直不动。**

图中

1. 作品：挂在 NUMS 画廊里，谁都看得见，谁也拿不走。
2. 没有钥匙孔的锁：NAKA 已铭刻的 3,327 件都锁在这个地址，没人知道私钥，也没有脚本（附录 G）。
3. A 家里的票据写着 #4：锁在 A 的金库里，指向画廊里那一件。
4. 区块顶上的 CM：票据的承诺。
5. SHNAKAS：2,100 万枚符文也停在这个地址。

这张票据记着三件事：哪一件（作品编号）、还能请中继代发几次（中继额度，第 04 章）、归谁（持有人公钥）。另外还有两个随机数 ρ 和 s，让票据算出来的东西看不出内容；s 叫作品秘密，和图片无关。

票据本身不上链。上链的是它算出来的指纹，叫承诺：混了那两个随机数，谁也看不出是哪一件、归谁。索引器把每个承诺收进记录树，这棵树就是“出现过哪些票据”的公开账本。指纹算不回票据，所以每个承诺还带着一份密文，是用持有人的查看公钥锁上的票据内容，只有持有人解得开。明文只留在生成和收下它的金库里。

不过有些操作本身就公开编号：铸造、购买、取回时，大家都知道是哪一件换了新票据。私密转账不公开编号，转完以后，外人对不上新承诺是哪一件、归谁。

SHNAKAS 也是这样存的：你持有的钱袋同样是一张票据，只是编号换成了钱袋号；每袋多少枚跟着钱袋号公开登记，所以看得到每袋多少，看不出归谁（挖矿原理）。

误解　买了 NAKA，图会转进我的钱包。

事实　**作品一直停在 NUMS 地址上，普通钱包里看不到它是正常的，持仓在 SHORD 金库里看。**

04 转让

私下转给别人，链上看见什么

> **任何人能验证私密转账有效、票据没被双花，但是看不出花掉的是哪一张、转给了谁。**

图中

1. 旧票据：A 手里打叉的那张，转账被索引器认下后就作废。
2. 信封：写进最新一块，就是装着信的那节车厢。
3. 作废码清单：牌上是开头几位，红的刚记入；重复就拒收。
4. B 的钥匙：查看密钥解开密文，金库里多出一张新票据。

A 要把 #4 转给 B，就在收件人一栏填 B 的隐私地址（shord1…）或隐私名字（如 bob.naka，附录 J）。金库先算出旧票据的作废码，再给 B 写一张新票据、用 B 的查看公钥加密，最后生成一份证明：旧票据在树上、归 A，新票据还是同一件，但不说是哪一张。信封可以由 A 自己付矿工费发出，也可以交给官方中继代发，扣票据上的一个中继额度，或者用官网另卖的预付中继（第 08 章、附录 I04）。

索引器拿到信封，验过证明、确认作废码是第一次出现，才把它记进清单、把新承诺加进记录树。旧票据再花就会被拒收；外人对不上作废码属于哪片叶子，所以不知道花掉的是哪一张。B 的金库扫到这笔交易、解开密文，算出的承诺和树上的对得上，新票据才算到手。密文写给 B 的查看密钥，B 的金库一扫就能解开（附录 H）。

SHNAKAS 钱袋整袋转出，和转作品一模一样。只给一部分，得分两步：先把钱袋拆成 2 到 16 个，再发送其中一个。拆分不像转账，原钱袋号和每袋数量都公开，只是看不出归谁（附录 I07）。

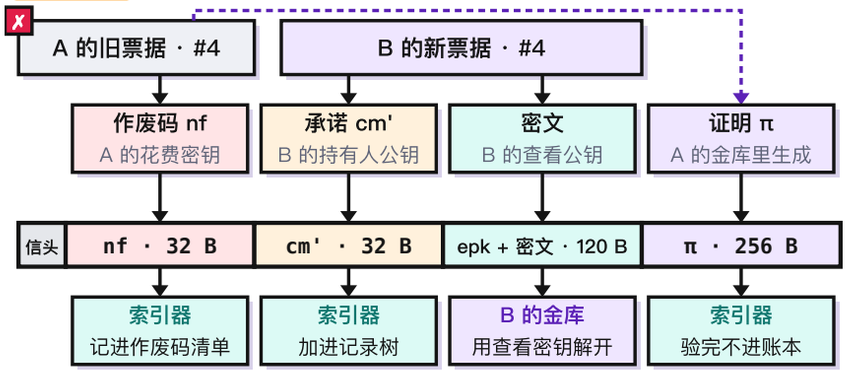
私密转账只管交出作品，不管收钱：拿它做买卖，谁先给都得信对方。要一手交钱一手交货，就用挂单（第 05 章）。

误解　私密转账谁也查不到，没有任何线索。

事实　**链上看得到有人花了一张票据；自己付矿工费，还看得出是哪个钱包发的，交给中继代发就看不出。**



技术卡 04　私密转账：一个信封，各去各处



这四样装进同一个 OP_RETURN 信封（公开 v1 格式，共 462 字节）

条宽不按比例；另有树根高度 4 字节、用掉和新买的额度 1 + 2 字节没画

证明 π：旧票据在树上、A 有花费密钥、编号没变，不说是哪一张，还绑住信封正文

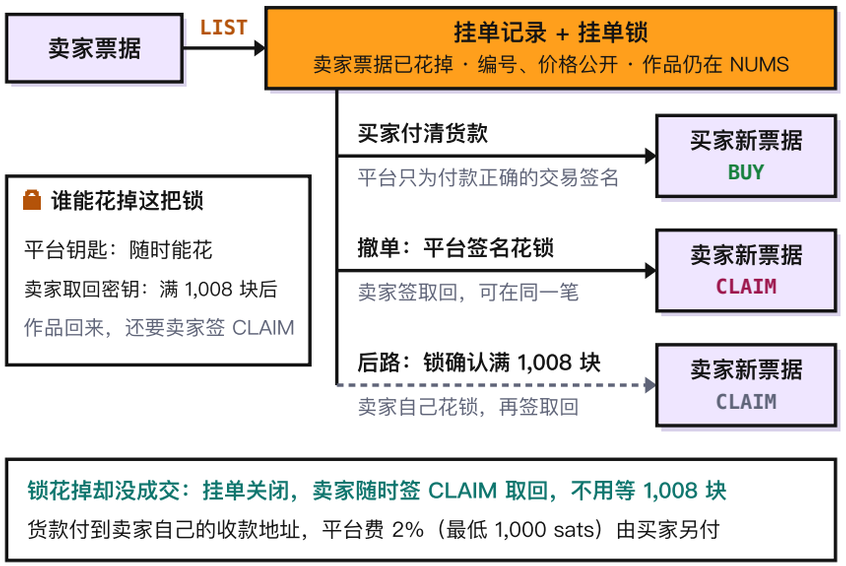
索引器全部验过才记账；#4 只在两人的金库里，信封里没有编号

钱袋拆分：另用 SPLIT 信封，写在见证里，公开原钱袋号和每个新钱袋的数量

技术说明　索引器不把旧叶子标成已花，因为一标出来，外人就能把这次花费和当初生成这片叶子的那笔交易连起来。它另记一个作废码，由 ρ 和持有人的花费密钥一起算出。缺了花费密钥，私密转账就藏不住了：新票据的 ρ 是用信封里公开的作废码算的，谁都算得到；作废码要是只用 ρ 算，外人就能提前算出新票据的作废码，一张接一张，把这件作品的每次转手串成一条线。



技术卡 05　一把锁，三条出路



技术说明　挂单锁是一个 P2TR 输出，有两条花法：平台钥匙走密钥路径，随时能花；卖家的取回公钥走脚本路径，锁确认满 1,008 块才能用。平台花掉锁，只拿得到锁里那点聪（官方中继建锁放 330 sats，协议不限金额）；作品要靠取回签名才回到卖家手里，取回密钥由卖家的种子和这次挂单的作废码算出，平台算不出来。

05 交易

挂单公开什么，平台能做什么

NAKA 挂单要公开编号、价格和收款地址，作品的去向从此由一把锁决定。锁的钥匙在平台手里：平台能随时关掉挂单，却拿不走作品，也拿不走货款。

图中

1. 价签：编号和价格写进区块，谁都看得到。
2. 挂单锁：装着 330 sats 的比特币输出，钥匙挂在平台牌子上。
3. 买家：标价付给卖家，2% 平台费另付（最低 1,000 sats）。
4. 沙漏：锁确认满 1,008 块，卖家不用平台，自己花锁取回。
5. CLOSED：锁花掉却没成交，挂单关闭，卖家签取回才拿回作品。

挂单（LIST）的信封交出卖家票据的作废码，同一笔交易建好挂单锁。索引器认下以后，这张票据就花不了了，作品暂时挂在锁上：锁怎么被花，决定新票据归谁（下一页从头走一遍）。

收款地址可以是金库里的新地址、连接的钱包，也可以手输，bc1p、bc1q、3 开头的线上都成交过；标价不能低于这种地址的粉尘限额。

购买（BUY）的交易要花掉这把锁，同一笔里付清货款，新票据由买家自己生成。花锁要平台签名，协议文档写明平台只签付款正确的交易：标价 1,000,000 sats，卖家要收到不少于 1,000,000，平台不少于 20,000，少一样索引器就不认。

撤单（CLAIM）是平台签名花锁、卖家用取回密钥签取回，两样可以放进同一笔交易。平台不配合，卖家等锁确认满 1,008 块，自己花锁取回。锁要是被花掉又没成交，挂单就关了，卖家随时能签取回，不用再等 1,008 块。

误解　BTC 付款确认了，购买就成功了。

事实　**付款进了区块，索引器再按挂单验收；验收通过、金库里出现新票据，这笔才算成交。**

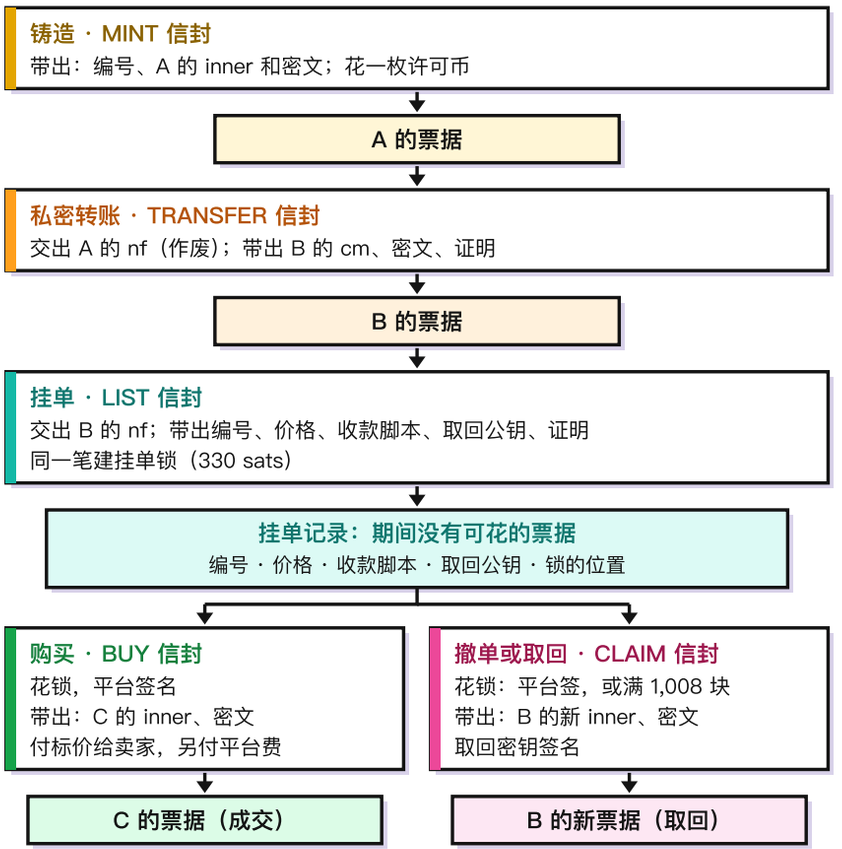
所有权流转

交易和信封

> **上一页讲了一张挂单的三条出路。这一页把 #4 从铸造到成交完整走一遍：每一步交出什么、带出什么；信封在内存池里谁都读得到，为什么改不了；一笔购买上链前，谁能叫停。**

这里按 NAKA 的链上挂单讲。其他合集已改成链下挂单（官方叫即时挂单），成交时才上链；项目方 10 月 27 日说 NAKA 保持原样。

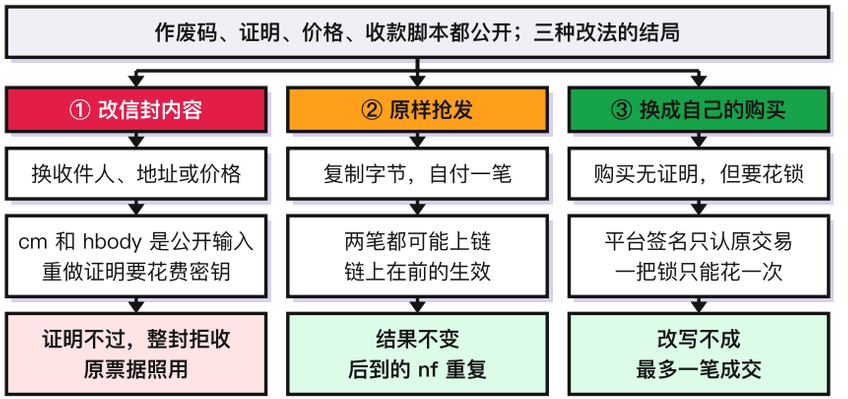
流程图 01 #4 从铸造到成交：每一步的交易和信封



锁被花掉而没有有效购买：挂单关闭，卖家再补一封 CLAIM

挂单编号就是挂单时交出的 nf；锁本身不记所有权

流程图 02 内存池里的信封：谁都读得到，为什么改不了



改不了：重做证明要花费密钥，签 CLAIM 要取回密钥，都只在持有人的金库里

转账、挂单、取回信封可原样搬走；购买、铸造的平台签名只认原交易

一笔购买上链前，谁能叫停

谁	怎么叫停	结果
买家	确认前用同一个输入再发一笔手续费更高的交易（RBF）	新交易先确认，购买就上不了链，挂单照旧；买家只付新交易的矿工费
平台	抢先用平台钥匙花掉挂单锁	花锁的交易先确认，购买就上不了链，买家不花钱；挂单关闭，卖家签取回
卖家	锁满 1,008 块前叫停不了，撤单要平台签名；满了以后能自己花锁，和购买抢先	谁先确认算谁：卖家先，挂单关闭、取回；购买先，成交
其他人	改不了这封信（见上图）；要抢同一单，得另有一笔平台签过的购买	一把锁只能花一次，最多一笔购买成交
矿工	不打包这笔购买	其他矿工仍可能打包

06 证明

证明持有，各要交出什么

证明在金库里生成，票据和密钥都留在本机。三种用法差在交给谁、票据动不动：投票交给投票服务，点“证明”交给官网，票据都原封不动；领基础奖励写进比特币链，旧票据换成一张新的。

图中

1. 证明卡：#46 交出去的只是这张卡，票据留在脚边的保险箱里。
2. 核对单：SNAP（在本轮快照里）、VALID（证明有效）。
3. 投票箱：选项连同证明交给投票服务，不上链。
4. 标签板：投票服务公开的标签记录，每票一行。
5. 挂单牌：#4 后来挂单，作废码上链，就和板上红的那行对上。

投票按快照算：快照那一块持有的 NAKA 每件一票，之后卖掉也算数。证明借用私密转账那套电路（花费电路），只是什么都不花。也正因为是这套电路，证明里带着作废码，投票服务公开每一票时都附上由它算出的标签，计票谁都能核。投票当时标签对不上任何票据；票据日后花掉、作废码上链，才对得上，那次若是挂单，编号也公开。

没有 NAKA 也能用 Snickets 投票。这种票不用证明，金库签个名交给平台就行，投出去的 Snickets 不退（附录 I06）。

领基础奖励就要上链了：奖励信封把旧票据换成一张新的，外加一个 SHNAKAS 钱袋；链上看得到作废码和新承诺，看不出是哪一件。加成得另发一封信封，签名亮出编号（补领、批量领取见附录 I06）。

“证明”按钮走另一套电路，叫持有证明：证明交给官网的验证接口，申领人是你的钱包地址，公开的只有树根、活动标识和去重标记，连作废码都不露。它证明的是票据在记录树上，不检查是否已经卖出：卖掉的票据叶子一直在树上，用最新的树根照样能证明。

误解 投票、点“证明”都会花掉我的 NAKA。

事实 **这两样都不花票据，也不上链。领基础奖励会花掉旧票据，同一笔就换回新的，挖矿的周数照样接着算（第 07 章）。**



技术卡 06 三种用法，各交出什么

官网投票 花费电路	证明什么	快照时持有一张合格票据
	交出去的	选项和证明（公开输入含作废码），交给投票服务
	票据怎样	不花，不上链
	边界	**票据日后花掉，公开的标签就对得上它投了什么**
领基础奖励 花费电路	证明什么	资格树上有一张整周持有的票据
	交出去的	上链的奖励信封：作废码、新承诺、证明
	票据怎样	正常领取时，旧票据换成新的
	边界	**不亮编号，作废码公开**
持有证明 Holder 电路	证明什么	知道树上某张票据的数据和密钥
	交出去的	证明和申领人地址，交给官网（“证明”按钮）
	票据怎样	不花，不上链
	边界	**不检查是否已花：旧叶子仍在新树根里**

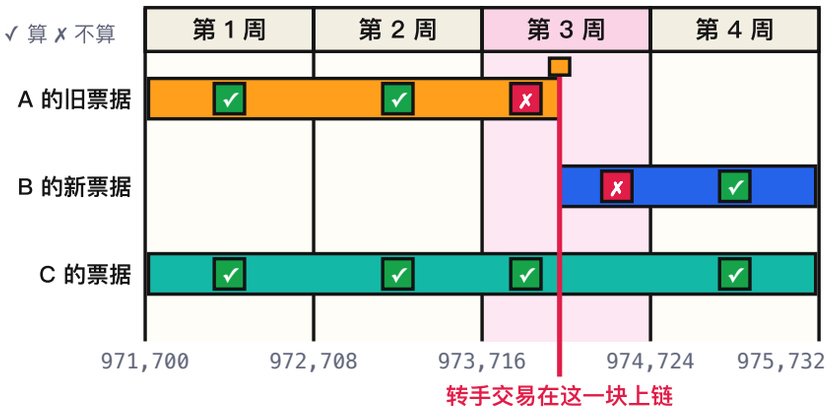
领加成另发一封 BONUS 信封：用签名，不用证明，编号公开

票数和标签对得上公开记录；证明没公开，资格只能抽查

技术说明 持有证明的去重标记是 Poseidon(作品秘密 s, 活动标识, 13)。活动标识由合集、用途和申领人一起算出，所以同一件作品在一个活动里只能证明一次；申领人也在里面，别人抄走这份证明也用不上。投票的标签是另一回事，由作废码和主题、轮次算出，前面说的“对得上”就出在它身上。



技术卡 07　一周 1,008 块



某一周算你的：这周开始时已经拿着，一直拿到这周结束

例外：领奖励换出的新票据，当周照样算

每周 1,008 块、266,640 枚，共 78 周；轴上是分界块，第 3 周即 973,717–974,724 块

技术说明　资格只看两个区块高度：创建票据的区块不晚于周起点，花掉它的区块晚于周终点（没花也算）。权重每块按当时的挂单重算，所以属性地板价一变，加成跟着变。每周的区块区间见附录 E。

07 挖矿

拿着 NAKA 就在挖 SHNAKAS，转手为什么断

> **SHNAKAS 按整周发：每 1,008 个区块算一周，一张票据从这周开始拿到这周结束，这一周的份额才算它的。份额先记在账上，可以攒着一起领，领了才变成钱袋。**

图中

1. 钟柱：每 1,008 块一根，两根之间就是第 3 周。
2. 转手：A 的信写进第 3 周中间的一块，B 的新票据从这一块才有。
3. 打叉的代币：第 3 周的份额，A 和 B 都领不到。
4. C 和宝箱：另一件整周没动，第 3 周的份额照算，领了才到手。

图里是第 04 章那次转手，转账在第 3 周中间上链：A 的旧票据在那一块花掉，没拿到周末；B 的新票据从那一块才有，不是从周初拿起，所以第 3 周两人都不算。之前的周不受影响，A 拿满的第 1、2 周照领；B 接着拿下去，从第 4 周开始算。

挂单、撤单、转给自己（给作品加中继额度就是一次）同样会断掉当周，因为它们都花掉了旧票据。领基础奖励也花掉旧票据，不过同一笔交易就把这件换回你的金库，索引器把新票据补进当周的资格树，所以挖矿不断。领加成、改价、投票、持有证明不动票据，不影响。

资格决定一周能不能领，权重决定能领多少。每件从 100% 起算，属性地板价高、编号小的另有加成，封顶 400%；规则写在链上的铭文里，谁算都一样（附录 I07），每件每周多少，用浏览器插件 Naka Sigil 看。挂单中和没铸的作品也占份额，这份谁都领不到。

份额不用每周领，可以攒着一起领。只领基础的 100% 不用亮编号，要领加成就得亮出编号。奖励算到第 1,050,324 块为止，之后再留 52 周来领，第 1,102,740 块截止；怎样变成钱袋，见下一页。

误解　一挂单或卖掉，以前拿满的周也没了。

事实　**拿满的周照领，卖掉以后还能补领。挂单期间每周都不算，取回后从下一周恢复。**

挖矿原理

从蚀刻到钱袋

> **上一页攒下的份额，领了才变成钱袋。SHNAKAS 在 SHORD 里是一个合集，装的不是作品，是一个个有编号、记着数量的钱袋；2,100 万枚符文在蚀刻时全部给了 NUMS 地址，一直停着不动，钱袋也兑不回去。流程图 03 跟着一次领取走一遍。**

流程图 03　一次领取：份额怎样变成钱袋



钱袋兑不回 NUMS 上的符文：那 2,100 万枚领不领都原样不动

图里是正常领取；卖掉以后补领、一次领好几周，见附录 I07

总量怎么算

流程图只走了一次领取。把所有领取加起来，和上限、规则摆在一起，就是下面这张表：上限是蚀刻时定的，每周发多少写在链上的规则铭文里，已发行是把官网账本里的钱袋逐个加起来。

名称	怎么来的	数量（枚）
上限	蚀刻时全部给到 NUMS 地址；官网叫“上限”，永远不会超过的数量	21,000,000
规则最多发	3 个固定钱袋各 80 枚，加 78 周、每周 266,640 枚；剩下的 201,840 枚规则里没有安排	20,798,160
已发行	到 974,323 块领成 987 个钱袋：基础 506 个共 74,989.91 枚，加成 481 个共 92,265.79 枚；3 个固定钱袋还没铸	167,255.70
不会发行	挂单期间和没铸编号的份额没人能领；截止以后还没领的，也不再发	本文没统计
已销毁	烧成 Snickets 的钱袋转进花不出的地址；账本认不出是哪几个	看官网代币页
流通量	已发行减已销毁，官网代币页这样算	看官网代币页

为什么叫上限

蚀刻时那 2,100 万枚全部给了 NUMS，符文协议管这叫预挖（Premine）。但 NUMS 谁也花不动，这份预挖不归任何人，只给钱袋总量划了个上限，所以本文照官网叫它“上限”。

误解　没人领的份额被销毁了。

事实　**销毁是已经发出的钱袋再也花不出去，比如烧成 Snickets。没人领的份额从来没变成钱袋，账上本来就没有它；官网的说法是“从未领取的部分永不发行”。**

08 核验

账是谁记的，能不能自己核

账是索引器照规则从比特币区块里算出来的，官网的账也一样。要核，就用自己的索引器把区块重算一遍，在同一块上和官网比摘要。只是公开代码还追不上官网的规则，眼下核不全。

图中

1. 区块按顺序开过来，车厢上写的是高度。
2. 两台索引器，一台是官网的，一台是你自己跑的。
3. 规则一样、读到同一块，摘要就一样（9F3A 是开头几位的示意）。
4. 吐出的纸带：每台机器自己存的账和检查点。

索引器逐块读区块，按规则验收每封 SHORD 信封，过了才记账。验收不看时钟，也不问哪台服务器，所以规则和验证参数一样，谁来跑结果都一样。

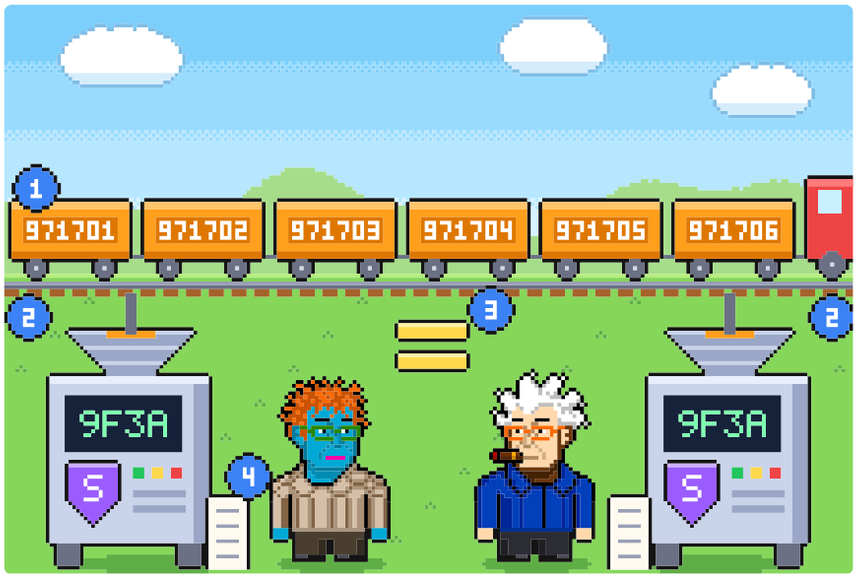
这本账存在每台索引器自己的机器上，隔几块存一份检查点。重启时从最新一份能用的接着读，都用不了才从起始区块重算。

对账就比同一块上的状态摘要。10 月 11 日用公开代码从头重放到 970,879 块，摘要和官网一模一样。眼下官网的规则比公开代码新：公开代码只能认出六类消息，官方线上后加的奖励、链下挂单和拆分还没公开，现在记录树和官方有差异，差多少见附录 H。

中继替人发的信，不跑索引器也能核。10 月 29 日起它改用新钱包代发（bc1pr5vsx…5hcp73），官网状态接口列的就是它，在区块浏览器里能看到它发的每一封信。规则里的收款地址见附录 I08。

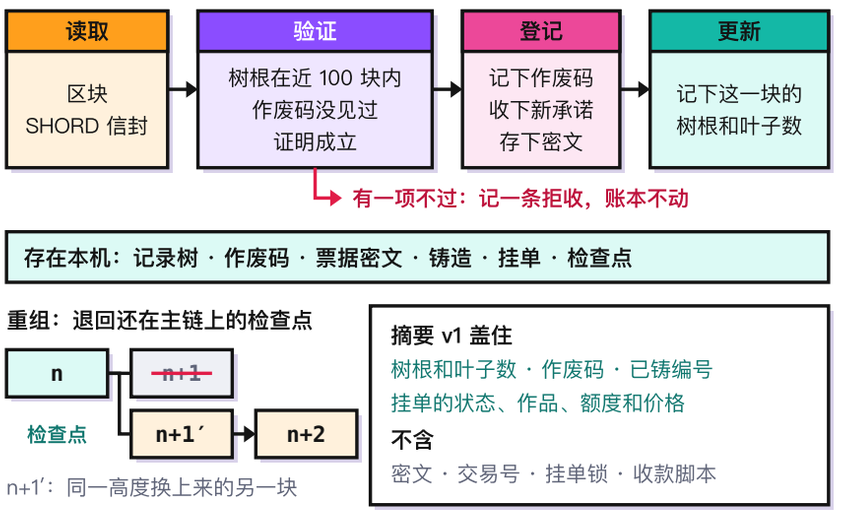
误解　索引器记着全部的账，知道每件作品在谁手里。

事实　**索引器只记承诺、作废码和密文，私密转账以后看不出哪张票据是哪件、归谁。密文只有收件人的金库解得开。**



技术卡 08　索引器验什么，摘要盖住什么

以私密转账为例：核对证明只用公开的数据和验证参数，不用任何人的私钥



两台对账：在同一块上比完整的摘要，高度和区块哈希都一样

前提：同一条比特币链、同一套规则和验证参数、同一个起始高度

技术说明　有了检查点，重启就不用从头读。可它也许是旧规则下存的、被改过，或者最后几块已被重组换掉，所以用之前先核三样：规则和验证参数的哈希，用存下的承诺重建出来的每块树根，最后 12 块还在不在主链上。有一样不对就换更早的一份。遇到重组也退回还在主链上的那份重读，追上最新区块之前对外仍用旧账。

快问快答

常有人问、正文又没细讲的十件事，先讲转账，再讲钱、钱袋和钥匙的安全。按主题排的完整问答见附录 K。

问 01 私密转账多久能到？对方怎么知道收到了？

答 交给官方中继，它会把一段时间里的信攒成一批再发，然后等交易进区块、索引器验收。自己付矿工费就不用等这一批。到了不会有通知，对方打开金库同步，看到新票据就是到了。

问 02 私密转账转错了地址，能撤回吗？

答 不能。信封上链、作废码记下，旧票据就作废了。隐私地址没有校验位，抄错一个字符多半仍是“合法”地址，作品就转给了一个谁也打不开的地址。地址要复制粘贴，转前核对首尾。

问 03 把 BTC 或别的铭文直接转到 NUMS 地址，能变成隐私资产吗？

答 不能。普通转入不会生成 SHORD 票据，转过去的东西没人有私钥，拿不回来。

问 04 复制一份票据数据，或者两台设备同时打开金库，能花两次吗？

答 不能。同一张票据只有一个作废码，索引器只认第一笔，后到的不算。后到的那笔要是用另一份 BTC 付了费，照样能上链，矿工费白付。

问 05 卖出后的 BTC 在哪里？

答 在挂单时选的收款地址。选“隐私地址”的，钱在金库的比特币页里，从那里提到任何地址；选连接的钱包或手输地址的，钱直接到那个地址。

问 06 领到的 SHNAKAS 能进普通符文钱包或市场吗？

答 不能。领到的是 SHORD 账本里的钱袋；2,100 万枚符文在蚀刻时给了 NUMS 地址，谁也花不动，钱袋也兑不回符文。钱袋能做什么见附录 I07。

问 07 作品锁在 NUMS 地址上，我还要保管什么？

答 锁住的是作品所在的比特币输出；持有权记在 SHORD 账本里，跟着金库的钥匙走，要保管的就是这把钥匙（第 01、03 章）。

问 08 解锁签名泄露了，重新签一次、换个 PIN 有用吗？

答 没用。同一钱包、同一地址签出的总是同一套钥匙。要换，就用另一个钱包地址开新金库，把票据私密转过去。

问 09 查看密钥泄露了会怎样？

答 对方能解开写给你的密文，看到你收过哪些票据，以后发给这把钥匙的也一样。没有花费密钥，动不了它们。

问 10 可信设置是什么，会影响我的作品吗？

答 生成证明密钥用的一次性随机数。NAKA 这份由官方单方生成，拿不走你金库里的作品；下一个合集计划改用多方仪式（附录 D）。

交易和保管提醒

> **在 SHORD 里，你的钥匙说了算，每一步上链就作数。动手之前对着下面几条核一遍，资产就稳稳在你手里。**

01 从收藏的官网入口进，看到签解锁文字的签名框先核对网址。这份签名只在官网用，任何人都不能给。

02 付款后，BTC 确认、索引器验收、金库里出现新票据，三步都到了才算成交。

03 私下买卖时，BTC 和票据分两笔走，没有挂单锁替双方担保，只和信得过的人做。转完让对方在金库里确认收到，担保方怎么核对见附录 K。

04 费用看合集：NAKA 平台费 2%，最低 1,000 sats，买家另付，没有版税。Trollbox 等合集是 1% 平台费加 1% 版税。

05 想领哪一周的奖励，那一周就别挂单、撤单、转手，也不能自己转给自己。

06 网页金库靠钱包打开，同一个钱包和付款地址总打开同一个金库，要保管好钱包的助记词。手机 Shielded Vault App 另有 24 个词，和 UniSat 等钱包的不是一套，抄在纸上别截图。

07 作品和钱袋用隐私地址收，BTC 用比特币页的地址收，别往比特币地址转铭文或符文，会被当成 BTC 花掉。搬金库到手机的二维码和链接就是金库，别拍照、别外发；别人发来的金库链接别打开，那是对方的金库，存进去的都归对方。

08 官网另卖的预付中继只存在买它的浏览器里，换设备、清数据前先用完；票据里的中继额度跟着作品走，卖出时归买家。



出场作品：A 是 #2，B 是 #0，买家 C 是 #21，#4 是被买卖的那一件；#12、#14、#42 是观众，#15、#1、#3 是博物馆里的作品，#7 是来铸造的人，#46 是出示证明的人，#37、#49 运行账本机。

扫码打开网页版

ordinalser.github.io/naka-sigil/learn/shord

在线阅读，下载中英文 PDF。

扫码加入 Naka Telegram 中文交流群

t.me/+fRT4yVcxZ6VlNTBl

提问、交流和交易。

本版 2026 年 11 月 3 日。线上数据截至 10 月 28 日，中继 11 月 2 日复核，项目方在 X 上的说明核到 11 月 2 日，官网金库、市场和游戏 11 月 3 日逐页核过；代码依据公开仓库提交 3cdbdfdf（10 月 12 日）和官网客户端（SHA-256 57457629…，10 月 28 日读取，11 月 3 日复核未变）。规则以后的变化见资料页的版本记录，每条说法的出处和复核日期见资料与复核，完整的操作和术语见网页版的附录（PDF 不收附录）。摊位上的 Ord Dropz 标志照官网图标画成了像素，后窗里那双眼睛是本指南自己画的。