让每一份付出都被看见：乡建数字身份（Semi）

南塘DAO · 技术详细版

官网摘要

乡建数字身份（Semi）是南塘DAO 的伙伴们一起做的开源工具。它给每一位乡村建设参与者，无论是返乡青年、实习生还是数字游民，一个属于自己的数字身份账户，用手机号或邮箱就能登录，不用懂技术。做饭、除草、画墙、写代码……每一份为社区出的力，都能以“ 社区积分 ”的形式被记录下来，写明做了什么，公开、可信、不会被悄悄改掉。它从南塘长出来，也欢迎更多村庄和社区一起使用。

技术上，Semi 由 Nuxt/Vue 前端和 Rails/PostgreSQL 后端组成，每个账户背后是一个基于 Safe 和 ERC-4337 标准的智能账户，链上手续费由平台代付；贡献备注通过智能合约写进区块链；同时提供 OAuth 2.0 统一登录，让任务系统“ 白（Bai） ”等社区应用共用同一个身份。

一、从一个村子说起

安徽阜阳的南塘村，是一个有“ 自己商量事 ”传统的村子。1998 年前后，村民们为了共同面对的难题自发组织起来；2003 年，老年协会和妇女文艺队相继成立；2004 年，大家在此基础上成立了南塘兴农合作社。从那时到现在，这里的人们在乡村协作上已经走了二十多年。

南塘还有一套很有名的“ 萝卜白菜规则 ”。它来自美国的《罗伯特议事规则》，一本专门讲“ 怎么好好开会 ”的厚书。2008 年，议事规则推广者袁天鹏来到南塘，和合作社一起把它精简成村民记得住的“ 南塘十三条 ”。村里的老人念不准“ 罗伯特 ”，就笑着叫它“ 萝卜白菜 ”，名字就这样传开了。

这十三条说的都是大白话：主持人只管流程，不发表意见，也不替大家“ 总结 ”；讨论的必须是一个具体、能落地的提议，“ 动议动议，就是行动的建议 ”；发言先举手，每人每次不超过两分钟，同一件事最多说两次；不许跑题，不许人身攻击，只能就事论事；赞成的人比反对的人多才算通过，打平就是没通过。村民们靠这套规则，学会了一件看似简单、其实很难的事：好好开会。合作社里的大事小情，就是这样一条一条商量出来的。在数字技术来到这里之前，民主和协作的种子早就埋在了这片泥土里。

2011 年，资深志愿者刘兵因为被南塘的民主实践吸引，来到这里做志愿者，从此和南塘结下了长久的缘分。后来，通过他的牵线，南塘结识了 SeeDAO、LXDAO 等线上社区的朋友。2024 年，一群关心公共事务、熟悉区块链的年轻人来到村里，和村民一起生活、一起做事。这一年 8 月，南塘DAO 正式成立。“ DAO ”可以简单理解为：一群人不靠老板发号施令，而是按照公开的规则，一起商量、一起做事的组织。此后，返乡青年、实习生、数字游民和远程参与的伙伴陆续加入，成了今天在南塘做事的主力。

这两条线能走到一起，是因为它们本来就很像：一边是合作社二十多年扎根乡土的协作传统，一边是线上社区开放协作、共同建设的新方式。它们都不相信由少数人自上而下决定一切，都希望更多人能参与进来。南塘DAO 也一直提醒自己：乡村为主，DAO 为辅。

二、我们遇到的问题

在一起做事久了，我们发现几个绕不开的难题。

第一，很多付出没人记得。有伙伴为大家忙了一早上的大锅饭，有人顶着太阳在地里除了一下午的草，实习生组织了一场村里的活动，远方的伙伴熬夜整理了文档、带了一期线上共学。这些事情温暖又重要，可在传统的账本里找不到位置，只能靠“人情”记着。人情用久了会累，愿意付出的人也会慢慢疲惫。

第二，记录容易丢，也不容易让人放心。写在本子上、存在某个人电脑里的记录，换了负责人、换了系统，就可能找不到了；一个人管账，其他人也难免心里打鼓。

第三，人来人往，大家缺少共同的“尺子”。过去在熟人社会里，谁帮了忙、谁出了力，大家心里有数。可今天在南塘做事的人，有的住上一年，有的只来两周；有的在村里，有的远在千里之外。大家背景不同、来来去去、彼此不熟，“心里有数”就不够用了。过去是“因为我认识你，所以相信你”；现在，我们需要的是“因为规则公开、记录可查，所以大家都能放心”。

区块链恰好能帮上忙。说得简单一点，它是一本大家共同保管的公共账本：每一条记录写上去之后，所有人都能查看，谁也不能偷偷修改或删除。它的特点就是公开透明、不可篡改，是一种可信的记录方式。

可问题也来了：区块链用起来太难了。来南塘的年轻人里，很多人并不熟悉区块链，要记一长串英文单词（助记词），要懂“私钥”“手续费”这些专业概念，一不小心还可能弄丢账户。我们曾经只能由管理员在后台替大家操作，这又回到了“一个人说了算”。

乡建数字身份（Semi），就是为了解决这个“好东西用不上”的问题而做的。

三、它是什么

乡建数字身份（Semi），是一个给乡村建设参与者使用的个人数字身份账户。

你可以把它想象成一本“社区护照”加一本“贡献记录本”：

- 护照，证明“你是这个社区的一员”；
- 记录本，记下“你为社区做过什么”。

它的背后用的是区块链，但使用的人完全不需要懂区块链。就像我们用电不需要懂发电原理一样。对住在村里的年轻人来说，它是随手记下自己付出的小本子；对远方的伙伴来说，它是和这片土地保持联系的一扇门。

它虽然从南塘长出来，但不只属于南塘。任何一个村庄、合作社或社区，都可以用它来记录和认可自己成员的付出。

四、它现在能做什么

1. 用手机号或邮箱就能拥有自己的身份。 输入手机号或邮箱，收到验证码就能登录。第一次使用时设一个 6 位数的“ 支付码 ”，系统就会自动为你建好一个属于你自己的账户。不用记复杂的密码，也不用抄写一长串英文助记词。

2. 记录社区积分，而且每一笔都“ 有话要说 ”。 这是 Semi 最想让大家看到的地方。社区积分在成员之间发放和转交时，可以附上一句备注，比如“ 2 月 13 日，完成合作社老墙绘画 ”“ 周六帮厨，做了二十人的午饭 ”。这句备注会和记录一起写进区块链，成为永久、公开的贡献证明。

所以，一条记录不只是一个数字，它讲的是一件具体的事：谁，为社区，做了什么。 很多年以后再翻看，这些记录依然在，不会因为换了负责人或换了系统而消失。

3. 社区徽章。 参加了一次共创营、完成了一项长期任务，社区可以为你颁发一枚数字徽章，作为纪念和认可。你确认接收后，它会一直留在你的个人账户里。

4. 公共事务多人共同确认。 社区可以设立公共账户，由几位成员共同管理。涉及公共事务的操作，需要达到事先约定的人数确认才能生效，不让任何一个人单独说了算。这也正是“ 萝卜白菜规则 ”精神在数字世界的延续。

5. 社区可以设立自己的社区积分。 不同的村庄、不同的社区，可以按照自己的规则，设立属于自己的社区积分，用来记录本地成员的贡献。

6. 一个身份，进入多个社区应用。 Semi 是“ 身份入口 ”。比如我们的社区协作助手“ 白（Bai） ”，大家在“ 白 ”里发布和认领社区任务，登录用的就是 Semi 的身份。在“ 白 ”里完成一项任务，对应的社区积分和备注就会记录到 Semi 账户里，任务和贡献记录一一对得上。其他社区和开发者做的应用，也可以接入 Semi，让大家不必到处注册新账号。

五、它是怎么做到的（技术篇）

这一部分写给对技术感兴趣的朋友。不熟悉技术的读者可以跳过，只需要记住一句话：复杂的事情交给系统，用的人只需要手机号、验证码和一个 6 位支付码。 下面提到的内容，都能在 GitHub 上公开的代码和文档里找到。

1. 整体结构：三层分工

Semi 由三部分组成：

- 前端 semi-app：用 Nuxt 4 和 Vue 3 写成的单页网页应用（打开网页就能用，不用下载 App），界面用 Nuxt UI 和 Tailwind CSS，状态管理用 Pinia，支持中英文。所有和区块链打交道的操作都用 viem 这个库完成。Nuxt 自带的服务端（Nitro）只承担少数必须放在服务端的事，比如徽章上链。
- 后端 semi-backend：用 Ruby on Rails 8 写成的纯接口服务，数据存在 PostgreSQL 数据库里。它负责登录、账户资料、交易记录、多人确认的提案和签名收集，以及统一登录（OAuth）。用户和账户的编号用的是按时间排序的 TSID。
- 区块链核心 semi-core：从前端代码里专门抽出来的一个独立模块，负责智能账户、密钥、手续费代付和多人签名这些“ 算错就出事 ”的逻辑。它不依赖 Semi 后端，网页端和服务端共用同一份代码，并配有单

元测试，以及在真实链上状态的复制环境（fork 测试）里跑通的测试，验证账户地址的推算和交易执行与真实合约一致。

2. 登录：只要手机号或邮箱

登录只有两种方式：手机短信验证码和邮箱验证码，没有密码登录。短信通过阿里云发送，邮件通过 Resend 发送。

验证码是 6 位随机数，15 分钟内有效；同一个手机号或邮箱任何时候只有一个有效的码，每个码最多试 5 次；发送频率也有限制，防止被人刷短信或反复猜码。验证码不会写进日志。登录成功后，后端发给浏览器一个登录凭证，之后每次请求都带上它。

3. 账户是怎么“自动建好”的

很多人以为“区块链账户”一定要自己保管助记词。Semi 的做法是把这件事藏到幕后：

1. 第一次登录后，设一个 6 位支付码。浏览器会在本地生成一组密钥（技术上是标准的 12 词助记词，按 BIP-39/BIP-44 规范推出一把签名私钥），用户不需要看到它，也不需要抄写。
2. 用支付码把密钥锁起来。浏览器用支付码对密钥加密（PBKDF2 进行 10 万次运算推出加密钥匙，再用 AES-GCM 256 位加密），得到一个加密包（keystore）保存到后端。支付码本身只在你的浏览器里使用，从不发给服务器，所以服务器保存的只是一个它自己打不开的“上了锁的盒子”。
3. 给你一个智能账户。你在链上的账户不是一把裸露的私钥，而是一个 Safe 智能账户。Safe 是区块链上被广泛使用的开源账户合约，Semi 用的是 1.4.1 版，配合 ERC-4337 标准（一种“账户抽象”标准，让账户可以由程序来定规则，例如由别人代付手续费）。账户地址用 CREATE2 方式提前算出来：你一注册就有了确定的地址，可以先收下积分和徽章，账户合约等到第一次真正操作时才部署上链。
4. 证明“这把钥匙是你的”。绑定账户时，浏览器会用这把私钥签一句固定的话，后端验证签名，并复算 Safe 地址确实由这把钥匙推出。一个账户只能绑定一次，一把钥匙、一个地址也只能属于一个账户，别人没法冒充。

以后每次要在链上做事，比如发放社区积分，只需输入支付码，浏览器在本地解开密钥、签好名再提交。需要的话，用户也可以在设置里导出私钥，自己保管。

4. 手续费：用户感觉不到

在区块链上写入记录，本来需要支付一笔“手续费”（gas），这是普通人最大的门槛之一。Semi 借助 ERC-4337 的两个角色解决它：

- 打包服务（bundler）：把用户签好的操作（叫 UserOperation）提交到链上；
- 代付服务（paymaster）：由平台替用户支付手续费。

这两项服务都接入了 ZeroDev，链上节点和查询服务用的是 Alchemy。在 Optimism 和 Arbitrum 两条链上，手续费由南塘自己预存的代付额度支付，每个账户有一定次数的免手续费操作。整个过程中，用户不需要知道什么是手续费，更不需要自己去准备。

5. 链上备注：一句话是怎么写进区块链的

这是 Semi 和“白（Bai）”配合最紧密的地方。

备注合约。链上有一个专门存备注的智能合约（RemarkLogicV1，部署在 Optimism 上，外面套了一层可升级的代理合约 Proxy，方便以后修 bug 而不改地址）。它只有一个写入功能 saveRemark，接收四样东西：任务池编号、任务编号、一条公开备注、一条完成任务的人写的感想。合约会把这两句话按“任务池 + 任务”存起来，记下写入时间，并发出一条 RemarkSaved 事件，方便以后按任务检索。它只负责“存证”，不处理别的事。备注最多 32 个字。

和社区积分一起，一次写入。发放社区积分时，Semi 把“发放积分”和“写入备注”这两个动作放进同一笔链上操作（同一个 UserOperation）里一起提交：要么都成功，要么都不发生，积分和它对应的那句话永远绑在一起。

和 Bai 的任务对上号。流程是这样的：

1. 伙伴在“白”里认领任务、提交完成凭证，可以顺手写一句感想；
2. 发布任务的人在“白”里审核通过后，点击发放社区积分，“白”会跳转到 Semi 的发放页面，并把任务池编号、任务编号、一条默认备注（例如“任务：《任务标题》+ 时间”，可以修改）和那句感想一起带过去；
3. Semi 把“白”里的任务编号经过 keccak256 哈希换算成链上用的数字编号，发放人输入支付码确认后，积分和备注一起上链；
4. 之后，“白”的后端可以按任务编号到链上查找对应的 RemarkSaved 事件，把这次发放和备注找回来，和任务对应起来。

不是从“白”过来的普通发放，也可以写备注，Semi 会为它生成一个随机编号。

记录可以核对。发放完成后，前端会把这条记录同步给后端，用于在双方的历史里展示。后端不会照单全收：它会去链上读这笔操作的回执，确认发起方真的是这个人的智能账户、接收方确实出现在这笔操作里，手续费和成功与否也以链上数据为准。

6. 社区徽章与纪念品展示

徽章建立在一套徽章合约之上：先由社区创建“个人档案”（Profile Registry 合约），再创建一类徽章，然后为成员颁发。颁发后徽章先处于“待接收”状态，成员自己确认接收后才会上链铸造，也可以拒绝。

徽章上链需要一个管理账户签名，这把管理私钥只保存在服务端，不会进到网页里；而用户发起颁发或接收时，会用自己的钥匙签名证明身份，服务端只验签，永远拿不到用户的加密包和支付码。为了防止网络中断导致重复铸造，服务端在铸造前会先查链上是否已经存在这枚徽章。

个人页面还会集中展示账户里的数字藏品，包括徽章和纪念品。展示数据通过 Alchemy 的索引服务读取，图片和说明信息可以来自 IPFS、Arweave 等分布式存储，音乐类的纪念品还能直接打开播放链接。

7. 多人共同确认：把“萝卜白菜规则”写进代码

社区的公共账户本身也是一个 Safe 智能账户，只是它有多位成员，并设定一个“门槛”：比如 3 位成员里至少 2 位同意，操作才能生效。

- 发起提案：任何成员都可以发起一项操作，后端把它放进待确认的队列里。
- 各自确认：每位成员用自己的支付码，在自己的浏览器里对这项提案签名（EIP-712 标准的结构化签名，签的内容一目了然）。后端收集签名，并逐个验证签名确实来自对应的成员。
- 达到门槛后执行：签名数量够了，任何一位成员都可以把它提交上链执行。手续费同样可以由平台代付。
- 看到的就是签下的：为了防止“页面上显示的是一回事，实际签的是另一回事”，前端在签名前会根据页面展示的内容重新生成一遍操作，和待签内容逐字节比对，不一致就拒绝签名；后端在收到提案和签名时也各核对一次。而且每项提案只允许包含一个操作，不能夹带别的东西。
- 成员变动也要大家同意：增加、移除成员或调整门槛，本身也是一项需要多人确认的提案。

这正是“萝卜白菜规则”里“少数服从多数、一个人说了不算”的精神，换了一种技术形式来执行。

8. 社区自己的社区积分

Semi 里有一个“合约工厂”：社区可以在页面上填写积分的名称、简称、图标，以及由哪个账户负责发放，一键部署一份属于本社区的积分合约。这份合约采用以太坊生态里通用的 ERC-20 标准，这是一种记录“谁有多少积分”的标准技术格式，任何支持这个标准的工具都能读取。目前这一功能部署在 Optimism 上。新建的积分默认只有创建者自己看得到，要由管理员审核后，才会出现在所有人都能看到的公共列表里，防止有人冒用别的社区的名义。

9. 一个身份，多个应用：统一登录

Semi 后端内置了一套 OAuth 2.0 授权服务。这是大家熟悉的“用微信登录”“用 GitHub 登录”背后的同一种标准，并提供了 OpenID Connect 风格的配置发现地址和公钥地址，方便其他应用自动对接。

- 开发者可以在 Semi 的开发者页面登记自己的应用，设置回调地址和允许申请的权限范围；
- 登录采用“授权码 + PKCE（S256）”方式，即使授权码在传输中被截获，也换不到登录凭证；
- 权限是分开授予的：基本资料（profile）、链上账户地址（wallet）、积分查看（token:read）等，用户在授权页面上看得清清楚楚，之后也可以在 Semi 里随时查看和撤销已授予的应用；
- 授权页禁止被其他网页嵌入，防止“点击劫持”。

“白（Bai）”就是这样接入的：大家在“白”里点击用 Semi 登录，完成授权后，“白”会按 Semi 的用户编号找到或创建对应的用户，同一个人在两个系统里就是同一个身份，积分发给谁也就不会出错。

10. 支持哪些区块链

Semi 目前支持四条链，在页面上可以随时切换：

- Optimism：日常使用的主力，手续费代付、备注合约、徽章合约、社区积分合约工厂都在这里；

- Arbitrum One：支持智能账户和多人确认，手续费同样代付；
- 以太坊主网：支持智能账户和多人确认，但手续费不代付，需要账户自己承担，所以日常一般不用；
- Sepolia 测试网：给开发者测试用。

Safe 的官方合约在这些链上是同一批地址，所以同一个人在不同链上算出来的智能账户地址也是同一个。

11. 其他村子怎么自己部署

Semi 的前后端都提供了 Docker 镜像构建文件，可以部署在自己的服务器上：

- 后端需要一个 PostgreSQL 数据库，以及自己的短信和邮件发送账号；
- 前端需要配置区块链节点服务（Alchemy）和打包、代付服务（ZeroDev）的密钥，以及后端地址。所有链相关的配置都集中在一个地方读取，配错时会在启动阶段就明确报错，而不是等到用户操作时才出问题；
- 如果要让本地的协作工具接入，只需在 Semi 里登记一个 OAuth 应用。

“白（Bai）”同样开源：前端是 Nuxt/Vue，后端是 Node.js/Express 加 Supabase，备注合约等智能合约用 Solidity 编写、Hardhat 部署，也放在 GitHub 上。

六、我们为什么这样看待“积分”

在南塘，社区积分不是奖金，也不是商品，它更像一本大家共同的贡献记账本：有人为大家煮的一锅饭，远方伙伴写的一行代码，都能在这本账上被公平地看见。它想做的，是让贡献从少数人的记忆变成大家共同的记录；在南塘，这份记录也是大家参与社区事务讨论、共同做决定时的重要依据。

这一想法，借鉴了国际上关于“贡献会计”和社区互助的思路。比利时学者 Michel Bauwens 是 P2P 基金会的创办人，长期研究共享与协作。他和同伴们提出：好的记录方式，应当记下每个人的各种贡献，而不只是市场愿意付钱的那部分劳动；照顾、陪伴、互助这些“看不见的工作”，同样值得被记录。同时我们也提醒自己：记录是为了让人与人的关系更好，而不是把人变成一串冷冰冰的数字。

在“身份”这件事上，我们也受到日本山古志村的启发。这个只有几百位居民的山村，邀请世界各地关心它的人成为“数字村民”，与村庄建立长期的联系。我们同样希望，来过南塘、或远远关心着乡村的人，都能有一个“属于这里”的身份。

乡村建设不只是修路盖房，更是一群人共同创作一种生活。真正的难点从来不在技术，而在人和人的共同生活里。每一份付出被看见，是这种共同生活的开始。

七、开源，欢迎一起来

乡建数字身份（Semi）是社区一起写出来的开源项目，代码公开在 GitHub 上（github.com/nantang-dao），包括前端 semi-app、后端 semi-backend 和任务系统 Bai，任何人都可以查看、使用和参与改进。无论你是返乡青年、数字游民、乡建团队，还是愿意写代码、做设计的朋友，都欢迎一起把它变得更好用。

- Semi 网站：semi.ntdao.xyz
- 社区协作助手“白（Bai）”：bai.ntdao.xyz
- 代码：github.com/nantang-dao
- 微信公众号：南塘DAO

如果你所在的村庄或社区，也有很多“没被记下来的付出”，欢迎来找我们聊聊。