

ENGAGE 手机 App 使用说明书

适用版本：ENGAGE 移动钱包（Flutter / Android · 鸿蒙兼容，含 PoE 移动挖矿、链下加密聊天）
最后更新：2026-09
本文档面向普通用户，介绍如何使用 ENGAGE
移动钱包进行日常操作：资产管理、移动挖矿、区块浏览器、DApp
与链上青春、质押、治理、链下加密聊天等。
本次更新要点：① 默认节点池现仅保留官方节点；② 提交提案的销毁额为 1000 ENGA（投票仍为 1 ENGA）；③ 链上青春的留言 / 昵称 / 告白费用是上缴合约方、不是销毁、留言也不是给作者；④ 发帖现由合约强制最低 1 ENGA；⑤ 新增「交易签名确认（防盲签）」章节；⑥ 设置页新增聊天图片缓存管理。

1. 主界面与五个标签

App 底部为 5 个标签，无「设置」标签（设置是钱包页右上角齿轮进入的独立页）：

图标	标签	内容
	钱包	余额、收款、转账、交易记录、账户切换、安全/设置入口（右上角图标）
□□	挖矿	PoE 移动挖矿开关、挖矿统计，并集成质押 / 链上治理 / 任务解锁 入口
	区块浏览器	全网状态（高度/持币人数/同步/供应），最新区块、余额排行、最新交易，搜索
□	DApp	默认集成「链上青春」（青春档案 / 青春榜 / 告白墙）
	聊天	链下端到端加密聊天（会话、通讯录、群组、备份）

切到后台不会立即锁定；App 按「无操作时长」自动锁定（详见 4.3）。
所有上链操作（转账、投票、合约调用、开始挖矿等）在签名前都会弹出确认框，由 App 在本地解码交易内容后展示给你核对，并需再次验证身份（详见 4.4）。

2. 第一次使用（创建 / 导入钱包）

2.1 创建钱包

- 1 进入「创建钱包」，输入钱包名称（仅本地标签，默认 **My Wallet**，可随手填写、与聊天昵称无关）。
- 2 选择助记词长度：12 词 或 24 词（校验位不同，恢复时须一致）。
- 3 点「生成」后离线抄写助记词（顺序错乱/漏词将导致无法恢复，请妥善保管，切勿截图联网保存）。
- 4 进入备份确认页：按顺序点选助记词完成校验，方可继续。
- 5 若尚未设置应用锁，会强制进入设置密码页（见 4.1）；设置后钱包创建完成。
- 6 （可选）填写邀请码：由设备 ID 确定性派生（**sha256(deviceId)** 前 12 位），一机一码——同一台手机上创建的所有钱包共享同一个邀请码，重装后也不变。用于后续任务解锁换积分（详见 5.2）。

说明：创建流程没有「同意条款」勾选框，无需勾选即可生成。

2.2 导入钱包

- 支持两种方式：助记词 或 私钥。
- 通过私钥导入的钱包不显示助记词（仅可导出私钥）。
- 导入时可填写钱包名称（默认 Imported Wallet）。

3. 钱包主页

钱包页顶部含：账户切换（头像）、余额与地址、安全盾牌图标（进入安全页）、设置齿轮图标（进入设置页）。下方有 收款 / 转账 快捷入口、活动记录（区块奖励 / 转入 / 转出）。

3.1 余额与地址

- 显示可用余额与锁仓余额（挖矿锁仓奖励、质押锁仓等）。
- 地址为 eg1... 格式（主网）。收款页可切换查看 主网透明地址 与 屏蔽地址（隐私地址）。

3.2 收款

进入收款页：显示二维码与地址，可一键复制；支持透明地址 / 屏蔽地址切换。把地址或二维码发给对方即可收款。

3.3 转账

- 1 填写收款地址（eg1...）、金额、备注（可选）。
- 2 页面显示预估网络费：PoE 链上无传统 Gas，普通转账费用约 0（以页面显示为准）。
- 3 点「Review & Send」→ 弹出签名确认框：列出交易类型、付款方、收款方与金额（内容由 App 本地解码得出，不采信节点返回的描述）→ 身份验证（生物识别或应用锁密码）→ 确认后签名广播（详见 4.4）。

3.4 交易记录

- 钱包页「最近活动」有四个筛选标签：全部 / 区块奖励 / 转入 / 转出，默认展示最新 5 条。
- 时间窗口随筛选变化（容易误解）：
 - 「全部」与「区块奖励」→ 仅最近 3 天（出块频繁，避免列表被奖励刷满）；
 - 「转入」/「转出」→ 最近 180 天。
 - 因此切到「转入」却看不到几天前那笔，多半是曾停留在「全部」的 3 天窗口下。
- 收录的类型不止转账：注册验证者、罚没、活跃提交、合约部署 / 调用、Gas 燃烧、分红、解锁等任何改变可用余额的动作都会归入「转入」或「转出」（区块奖励单独一列）。
- 点「查看全部」进入交易记录页，点单条查看交易详情（金额、对手地址、区块高度、类型、备注）。

3.5 多账户

通过账户切换入口进入账户列表（独立页，底部有导航）：

- 创建新账户（生成/导入）、切换当前账户、重命名、删除（删除需二次确认）。
- 删除账户会移除本地密钥与缓存，请先确保助记词/私钥已备份。

3.6 安全入口

钱包页右上角盾牌图标进入安全页（见第 4 节）。

4. 安全：应用锁密码与生物识别

安全页由钱包页盾牌图标进入，包含：应用锁密码、生物识别开关、自动锁定说明、查看助记词 / 导出私钥。

4.1 设置 / 修改密码

- 进入安全页「应用锁密码」→ 进入密码设置页，可创建或修改应用锁（6 位及以上，纯数字或字母数字）。
- 修改密码需先通过现有生物识别/密码验证。
- 同一密码页用于首次设置与后续修改（未设密码时创建，已设时修改）。

4.2 生物识别

- 开启后可用系统指纹/面容（含鸿蒙设备能力）替代密码解锁与授权转账。
- 生物识别仅作解锁便利，密码仍是终极恢复手段；关闭生物识别不影响密码。

4.3 自动锁定

- 采用 **LockManager**：10 分钟无任何操作后自动锁定（任意点击/滑动都刷新计时）。
- 切到后台不会立即锁定；只有累计无操作达到时长才锁。
- 锁定后需生物识别或密码解锁，期间不泄露资产操作能力。

4.4 交易签名确认（防盲签）

任何需要你签名的上链操作（转账、投票、提交提案、质押 / 解押、链上青春发帖 / 点赞 / 留言 / 昵称、开始挖矿等），App 都会先做两件事：

- 1 本地解码：App 自己解析待签名的交易字节，把「交易类型、付款方、收款方与金额」显示出来供你核对。这些内容不取自节点返回的摘要——节点给的描述一律不采信，以防被劫持的节点用“A 提示、B 内容”骗你签名。
- 2 身份验证：确认框弹出前需再次通过生物识别或应用锁密码（与导出助记词同级的二次验证）。

因此：

- 若 App 无法解析该交易内容（字节流非法或截断），或该类型属于系统交易（出块奖励、分红派发、活动上报等，本就不该由钱包签名），会直接拒绝签名并说明原因，绝不会让你签一个看不懂的东西。
 - 若确认框显示的内容与你实际要做的操作不符，请立即取消，并检查是否连到了来路不明的节点（见 11.2）。
-

5. 挖矿（PoE 移动挖矿）

挖矿是可选的开关，属 PoE 主链共识的一部分。

5.1 开启挖矿

- 在「挖矿」标签点「开始挖矿」开关：需已连接主网节点。
- 开启时需要用该钱包的私钥签名一次挑战：App 把签名随请求一起发给节点，节点校验签名确实由该地址派生。这样别人即使能访问公开的 RPC，也无法把你的地址登记成矿工、把你的挖矿份额转走。
- 机制：所有连接任意主网节点的手机矿工，平分每个区块的 App 挖矿份额（按地址均分，非按设备）。
- 一台手机通常对应一个挖矿钱包（由构建期标志 `ENFORCE_ONE_WALLET_PER_DEVICE` 控制，发行版默认关闭以便测试；开启后同一部手机同时只允许一个钱包挖矿）。

5.2 锁定奖励与任务解锁（AP）

- 挖矿收益以 `LOCK_MARKER`（锁仓奖励）形式记到该地址，需解锁后才能流动。
- 「任务解锁」入口（见 5.4）进入 AP 活跃积分页：
 - 步数任务：步数只能来自设备运动传感器，不支持手动填写（节点侧也拒收手填数据）。需先授权健康 / 运动权限并点「刷新获取运动步数」。每设备每日一次，且仅限本设备首个上报的地址；节点同时按步数直接解锁锁定币（每步 ≈ 1 ENGA，受锁仓余额与凭证上限约束）。
 - AP 兑换：用 AP 按实时汇率将锁仓奖励释放为流动 ENGA。
 - 邀请：邀请码为设备级（一机一码，本机所有钱包共享）。他人使用你的邀请码后，点「上报」即可换 AP——上报本身不需要签名、不发链上交易；一天内可多次上报（每邀请到新人即可再报一次）。上报时 App 会顺带把链上累计计数清零（该步需邀请码登记人签名）。
 - 每日上限：所有行为（步数、签到、邀请、发帖、点赞、留言等）共享同一个每日额度，每地址每日上限 50,000 AP。

注意：不是「保持 App 活跃就持续累积锁仓」——锁仓奖励来自挖矿区块收益，靠步数任务 / AP 兑换解锁。

5.3 后台与恢复

- 约 6 小时在后台无心跳后，挖矿会暂停，需手动恢复（点开关重新开启）。
- 挖矿统计展示：余额、链高度、锁仓奖励等链上数据。

5.4 挖矿页快捷入口

「挖矿」页集成三个入口，便于直达深层功能：

- 质押（见第 9 节）
- 链上治理（见第 10 节）
- 任务解锁 / AP（见 5.2）

6. 区块浏览器

「区块浏览器」标签展示全网状态与检索：

- 网络卡片：当前高度、持币人数（holders）、同步进度、总供应（最大 / 已铸造 / 已销毁），以及当前生效节点与 peer 数。
- 三个子页：

- 最新区块（高度、时间、出块地址、交易数）
- 余额排行（按余额排序的地址榜）
- 最新交易（类型、金额、地址、时间）
- 搜索：支持 区块高度（数字）、地址（eg1...）、交易哈希（0x... 或 64 位 hex）/ 区块哈希。
- 特殊地址带徽章：金库（treasury）、团队、燃烧（burn）、Gas 燃烧、分红等。

说明：区块浏览器没有「验证者列表」，仅展示持币地址与节点 peer 信息。

7. DApp 与链上青春

「DApp」标签默认集成 链上青春，含三个子页：青春档案 / 青春榜 / 告白墙。

7.1 青春档案

- 成长值 与 等级：21 级（萌芽 → ... → 混沌），升级成本随等级递增（ $25 \times L^2 + 75 \times L$ ）；不同等级对应不同称号。
- 链上昵称：首次设置 10 ENGA、修改 100 ENGA（全局唯一，重名被拒）。
 - 该昵称是链上唯一的同一份：链上青春与加密聊天共用它，并非两套独立昵称；在一处修改，另一处同步生效。
 - 费用性质为上缴合约方（开发者费池），不是销毁。
- 我的青春宣言：发布至链上，文案上限 500 个字符；合约强制最低 1 ENGA，不足会被拒绝（费用上缴合约方，非按字数计费，另需网络费）。
- 可「发布 / 重新发布」宣言；另有「告白墙」发布入口。

7.2 青春榜

- 浏览他人宣言，按 热度 / 时间 / 昵称 排序，可搜索、可只看「我的」。
- 点单条进入详情：可点赞、留言。
 - 点赞：免费（附带的链上 value 原样退回，仅耗网络费），作者不因此得币。
 - 不能给自己点赞：点自己的宣言会直接提示「不能给自己点赞」，不会发起交易、不扣任何费用。
 - 留言：消耗 0.5 ENGA + 网络费。该费用上缴合约方（开发者费池），不是给宣言作者；作者获得的是成长值补偿。

7.3 告白墙

- 独立子页，按 热度 / 最新 排序，可只看「我的」。
- 发布：默认匿名，可 @目标（昵称或地址），消耗 2 ENGA（上缴合约方，非销毁）。
- 给告白留言：消耗 0.5 ENGA（同样上缴合约方）。
- 点赞免费，但不能给自己的告白点赞（会直接提示，不发起交易）。

8. 链下加密聊天

「聊天」标签为端到端加密聊天（中继转发，服务器无法解密；昵称唯一性由链上费用背书）。

8.1 连接与界面

- 进入聊天自动连接中继（默认 <ws://180.76.117.98:8770/ws>）；图片走图床（默认 <http://180.76.117.98:8780>）。
- 两个地址均为 App 内置默认值，当前版本无修改入口。
- 会话列表右上角：备份、新建群组、通讯录。右下「+」发起新会话（私聊按地址 [eg1...](#)，或群/频道按作用域+频道名）。

8.2 昵称（与钱包名无关）

聊天昵称与「创建钱包时填的名称」完全无关。钱包名只是本地标签；聊天昵称须显式设置并支付链上费用后才生效，默认空。

它也与链上青春昵称是同一份（见 7.1）：共用同一条链上记录，任一处修改另一处同步生效。

- 首次为空时按钮显示「设置」；设置过显示「修改」。
- 设置 10 ENGA；修改 100 ENGA（全局唯一，重名被拒）。费用为上缴合约方（开发者费池），不是销毁。
- 设置/修改会同时发布你的 E2E 加密公钥，好友方可向你发加密消息。

8.3 加好友与聊天

- 通讯录点「添加」：输入对方地址（[eg1...](#)）或昵称；昵称由中继解析到地址（无昵称则提示「昵称不存在」）。已是好友会提示。
- 发起聊天后消息经 X25519 / NaCl box 端到端加密，仅收发双方可解密。
- 发送图片：先传图床得公开链接，再以加密文本消息发送，对方自动加载。

8.4 群组与通讯录

- 通讯录含：好友请求（待确认/待接受/已发出/已拉黑）、好友（备注、拉黑、移除）、群组（邀请/已加入）。
- 可创建群组、接受/拒绝群邀请；对好友可设备注、拉黑、移除。
- 会话支持置顶、免打扰、删除。

8.5 备份与隐私

- 聊天消息不存链上，仅中继转发；本地记录可在聊天备份页导出/恢复。
- 图床附件存于服务端可长期访问；昵称索引重启后由你重新发布昵称自动重建。

9. 质押（Staking）

入口：挖矿页「质押」，或经挖矿页快捷入口。

- 质押将 ENGA 锁仓以获得 ve(ENGA) 治理权重。锁仓时长决定链上 ve 时间因子（严格阶梯）：
 - [< 6,000,000 块](#)（≈1 年）→ [1×](#)
 - [6M-12M 块](#)（≈1-2 年）→ [2×](#)
 - [12M-18M 块](#)（≈2-3 年）→ [3×](#)
 - [≥ 18M 块](#)（≈3 年+）→ [4×](#)（封顶）

- 治理权重 = Σ (各笔锁仓金额 $\times$ 该笔自身的 ve 时间因子)；分批质押各自计权后加总。
- 锁仓时长可自由输入（默认 10000 块，App 提示「约 10000 块 = 1 天」起算；阶梯按锁仓块数自动判定）。
- 可看到：锁仓数量、解锁高度、进度、已存批次、可提取金额等；链上按区块高度结算，已过锁定期的批次可提取。
- 锁仓的 ENGA 同时作为治理投票权重（见第 10 节），投票期间会被冻结。

10. 治理 (Governance)

入口：挖矿页「链上治理」。

- 社区金库 (treasury) 由治理掌控；可提交提案与投票。
- 投票选择：0=反对 / 1=赞成 / 2=弃权；权重 = 你为本次投票锁定的 ENGA（投票期间冻结，需 ≥ 1 ENGA）。
- 费用（销毁）：
 - 提交提案：销毁 1000 ENGA（门槛远高于投票，用于防止垃圾提案）。
 - 投票：销毁 1 ENGA + 锁定的投票权重。
 - 两者都需钱包预留足够的 UTXO 覆盖「销毁额 + 锁定权重」，App 会先校验并在不足时提示。
- 提案门槛：从区块高度 210,000 起，提案需 余额 $> 10M$ ENGA 且 票数 $\geq 5\%$ 流通量；团队专属类（金库/拨款/团队）仅限创始团队地址。
- 提案执行前有 100 块锁定窗口，避免临近结算被篡改。
- 投票后锁定权重约在投票结束 + 缓冲后自动解冻（约 1 小时量级）。

11. 设置（语言 + 节点连接池 + 聊天图片缓存）

设置由钱包页齿轮图标进入，含三项：

11.1 语言

- 支持 简体中文 / 繁体中文 / English，单选即时切换。

11.2 主链节点连接池

- 默认节点池只有一个官方节点：<http://124.221.244.124:8545>（主网）。
- 可添加节点（格式 <http://host:port>，端口默认 8545）、设为默认（移到首位）、测试连接（显示高度 / peer / 同步%）、移除（至少保留一个）、重置为默认池。
- 连接具备故障转移：首选不可达时自动往后尝试池中的其它节点。

注意：节点池里只添加你信任的节点。App 虽然会在签名前本地解码交易（见 4.4），但连到恶意节点仍可能拿到被篡改的查询余额与历史记录。

11.3 本地聊天图片缓存

- 显示聊天图片在本机占用的空间（如 **0.12 GB**），可一键清理。
- 清理只删除本地副本，不影响已收到的图片内容——需要查看时会从图床重新拉取；对方发送的图片仍存于服务端。

说明：设置页不含质押、治理、安全、聊天中继等入口（它们分别在挖矿页、安全页、聊天内）。

12. 常见问题（FAQ）

Q1：聊天昵称为何一开始是空的、按钮显示「设置」？

聊天昵称与「创建钱包时填的名称」完全无关——钱包名只是本地标签，绝不会自动变成聊天昵称。新用户昵称默认空，需在通讯录显式设置（10 ENGA，上缴合约方）；设置过才显示「修改」（100 ENGA）。昵称全局唯一、重名被拒，且与链上青春昵称是同一份。

Q2：聊天消息安全吗？会被服务器看到吗？

消息经 X25519 / NaCl box 端到端加密，中继只能转发、无法解密。昵称唯一性由链上费用背书；图片走图床以加密文本发送。消息不存链上。

Q3：挖矿是「保持 App 活跃就持续累积」吗？

不是。挖矿是可选开关，收益来自平分区块 App 份额（记为锁仓奖励），靠「步数任务 / AP 兑换」解锁为流动币；后台超约 6 小时需手动恢复。

Q4：出块大概多快？

约 5 - 9 秒/块；App 提示「约 10000 块 = 1 天」用于估算锁仓周期。

Q5：链上青春各项操作要花多少？

发布宣言最低 1 ENGA（合约强制，不足会被拒绝，非按字数计费）；点赞免费；留言 0.5 ENGA；发布告白 2 ENGA；给告白留言 0.5 ENGA；链上昵称首次设置 10 ENGA、修改 100 ENGA。以上费用均上缴合约方（开发者费池），不是销毁，也不会给内容作者（作者获得的是成长值）；另需少量网络费。

Q6：默认连接哪个节点？

默认节点池只设置了一个官方节点 <http://124.221.244.124:8545>（RPC 端口 8545）。可在设置中自行添加 / 设为默认 / 测试 / 移除 / 重置；只添加你信任的节点。

Q7：切到后台会丢币或断连吗？

不会。余额与挖矿状态持久化在节点；切后台不立即锁屏，按 10 分钟无操作计时自动锁定。

Q8：发表的宣言、点赞数为什么过几秒才变？

链上操作需等交易进块（约 5 秒一块）。App 会轮询确认是否上链；若迟迟未生效会提示失败，而不是假装成功。

Q9：为什么每次操作都要弹确认框、还要再验证一次身份？

这是防盲签保护。App 会在本地解析待签名交易，把类型、付款方、收款方与金额显示给你核对，且不采信节点返回的任何描述；确认前还要再做一次生物识别 / 密码验证。若交易无法解析或属于系统交易，App 会直接拒绝签名，绝不让你签看不懂的内容（详见 4.4）。

Q10：为什么「开始挖矿」也要我签名？

节点会校验签名是否由该钱包地址派生。这样即使有人能访问公开的 RPC，也无法把你的地址登记成矿工、把本该属于你的挖矿份额转走。

Q11：为什么我给自己点赞会提示不能点赞？

链上合约禁止给自己的宣言 / 告白点赞。App 会先在本地拦截并提示，不会发起交易，也不扣任何费用。

ENGAGE —— 让每一次参与，都变成链上的资产。