



如何将8亿 Telegram 用户连接到主流区块链生态

cipher@joy.id

目录



扫码加入 Tg dapp 开发者群

Telegram 概况

Miniapp 开发入门

Telegram 对 Crypto 的支持现状

JoyID Passkey Wallet 简介

JoyID 的 Telegram dapp 解决方案

Telegram + 主流区块链 dapp 的畅想



Telegram 概况

- 8亿全球月活用户
- 可创建高达 20 万人的群组
- bot 对标服务号, miniapp 对标小程序
- 内置 Ton 钱包, 支持 toncoin, btc, usdt (trc20)
- 缺少‘朋友圈’、‘红包’等广受欢迎的微信功能
- 隐私起家但别深究
- 除了 crypto 用户外, Telegram 早已成为很多地方的主流应用
- 无须许可即可开始开发

Miniapp 开发入门



Miniapp 和微信小程序的区别和相似点

- Miniapp 直接使用外部URL, 无须官方托管
- 开发 miniapp 无须 KYC, 无须官方许可
- Miniapp 必须和 bot 关联
- Miniapp 中同样屏蔽了一些html 调用, 包括 deeplink、websocekt、webauthn 等
- Miniapp 中无法直接通过 html 保存浏览器状态(可通过其他方式绕过)



创建 miniapp

- 访问 <https://t.me/BotFather>
- 首先创建一个 bot, '/newbot'
 - 你会得到一个 access token: xxxxxx:xxxxxxxxxxxxxx
- 接着创建一个 miniapp, '/newapp'
 - 一个 bot 可以对应多个 app
- 唯一链接
 - `https://t.me/<bot>/<app>`



初始化 miniapp

- 引入 telegram-web-app.js
- 访问 `window.Telegram.WebApp`
- 校验 `initDataUnsafe`, 获取必要的上下文信息
 - 用户名
 - 群组名
 - 打开参数 `?startattach=command`
- 云端状态同步 CloudStorage



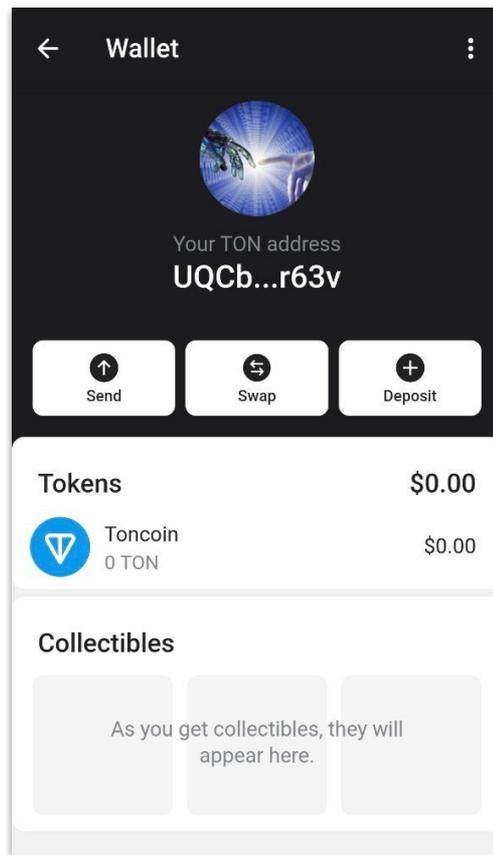
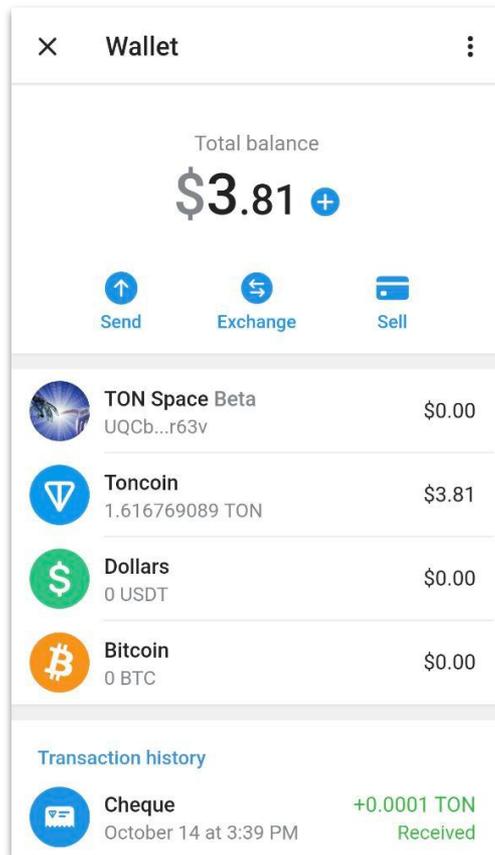
Miniapp 小技巧

- 半高/全高切换
- 将 miniapp 打开按钮放在 bot 菜单位置
- 可配置背景/按钮样式
- 注意 API 的 quota

Telegram 对 Crypto 的支持现状

Ton Wallet

- 托管钱包 + 非托管钱包
- 支持币种十分有限
- 非托管钱包门槛较高
- 内置 on/off ramp、swap
- Dapp 调用钱包需要跳转 @wallet 小程序
- 开发了 Cheque 功能, 但尚未正式发布





第三方钱包

- Miniapp 不支持 websocket, 不支持 deeplink, 因此无法与外部钱包直接连接
- 少数钱包通过二维码方式关联, 用户体验极差
- Unibot 等主流的 telegram dapp 使用中心化托管钱包, 用 telegram 账号 + 密码方式管理用户资产

JoyID Passkey Wallet 简介



什么是 Passkey

- 有 FIDO 联盟发起的用户侧安全登录协议
- 基于硬件的非对称加密进行身份认证
- 网页、Native app 均可访问
- 允许云端加密同步
- 支持 RSA / secp-r1 两种签名算法



Passkey 的普及度

- iOS 14.5 + (JoyID 要求 16.0 +) with iCloud, 支持同步
- Android 7.0 + with GMS, 支持同步
- MacOS with fingersensor, 支持同步
- Windows 10 + (JoyID 要求 Win11 22H2+), 不支持同步
- Linux with external authenticator (JoyID 暂不支持)

JoyID 的产品特征

- 无须密码、无须助记词、无须用户名、无须邮箱、无须手机号
- 10s 完成账户创建, 使用生物识别鉴权
- 非托管, 服务器不保存任何用户私钥或私钥分片
- 自动 Passkey 备份, 设备丢失可自动恢复
- 支持多设备、跨操作系统备份
- 无须安装, 即开即用, 支持PWA 安装到桌面, 支持离线签名
- 去中心化, 不依赖任何中心化组件
- 支持多链、多应用场景
- 安全性介于软件钱包和硬件钱包之间



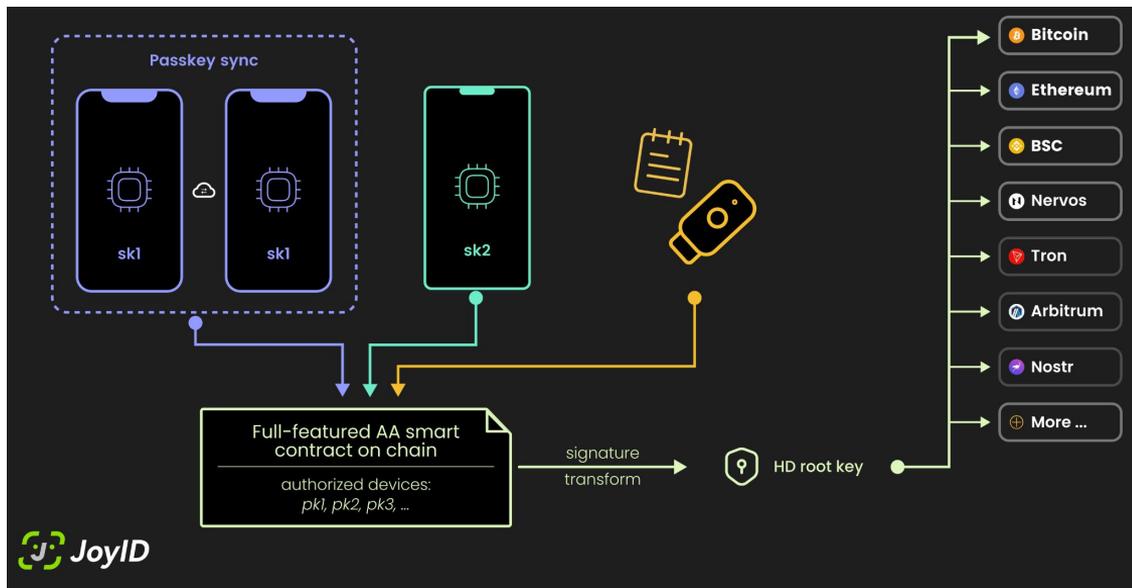
Joy.id



Demo time

JoyID 技术概述

- 使用 AA 账户管理多设备鉴权与密钥协商
- Signature transform 利用安全芯片提供稳定熵计算 HD wallet
- 对外表现为一个 EOA 钱包
- 单设备使用时 AA 账户无须付费
- 第三方可直接与智能合约 & 设备关联, 不需要依赖我们的中心化服务



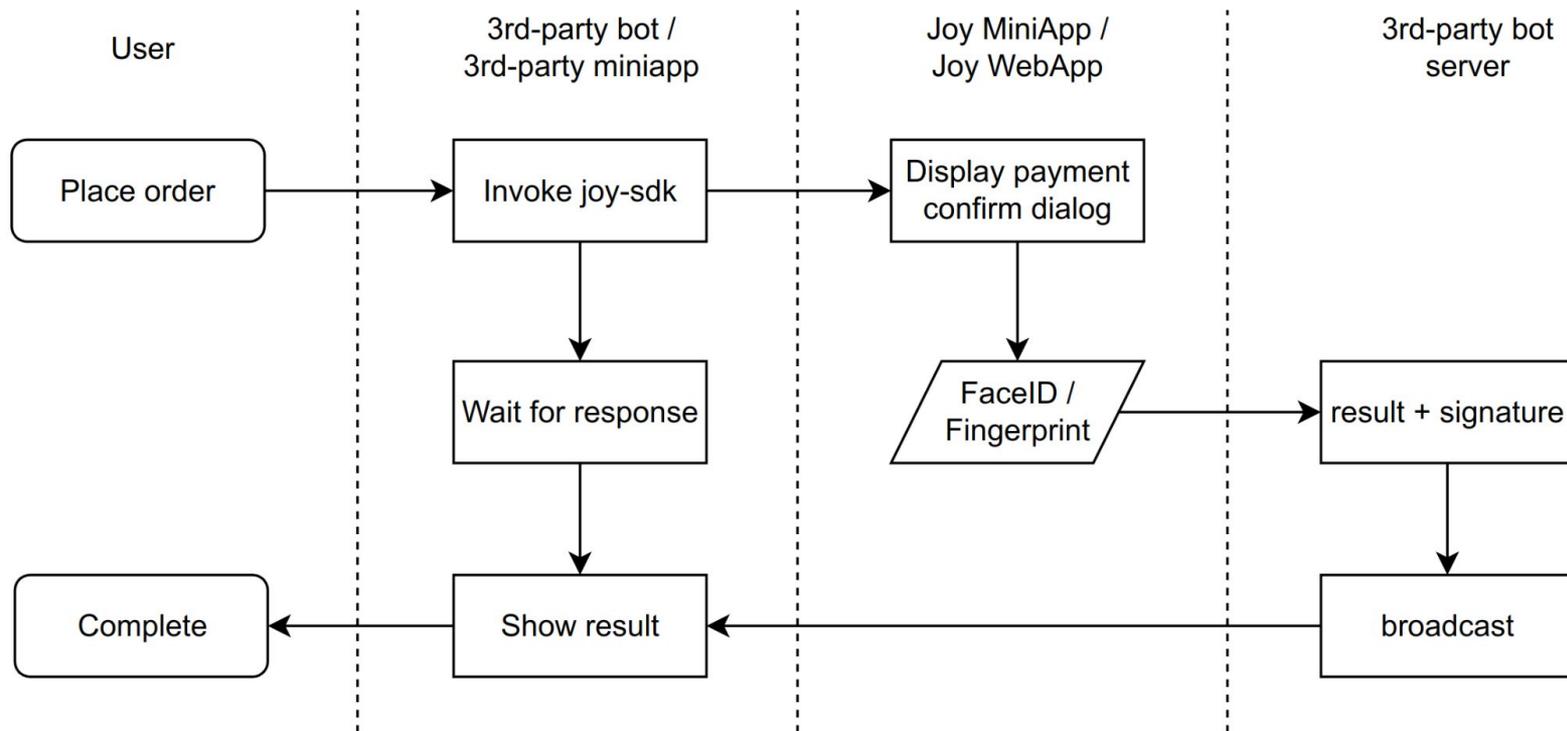
JoyID Passkey Wallet 针对 Telegram miniapp 的解决方案



Tg miniapp + web3 wallet 的主要问题

- 内置钱包不支持主流区块链
- Miniapp 不支持 walletconnect
- Miniapp 不支持跳转第三方 app
- Miniapp 支持跳转网页, 但网页跳回 miniapp 体验不好
- 如何解决 miniapp 和外部钱包的通讯问题?
- 如何解决主流用户的 onboarding 问题?

业务流程





Dapp 需要做什么

- 用户在 miniapp 操作时生成业务 id
- 调用 joyid-tg-sdk 生成跳转 URL + 业务id
- 后端监听回传的用户动作
- 更新前端页面



Demo time

Telegram + 主流 dapp 的畅想



Tg dapp 的切入点

- 全球最 crypto 的 8 亿人, 远超 metamask 3000万基础用户
- 必须低门槛
- 用好社交
- 提供‘降维打击式体验’



Tg 能带来的新的功能

- Token-gated 群 & 问答
- Token-incentive 社交裂变
- 反女巫空投
- Bot + miniapp 私域流量 + 消息推送
- 轻应用, 为主应用引流
- Crypto 支付/社交电商
- AA bot + JoyID



Thanks

Website: <https://joy.id>

Docs: <https://docs.joy.id/guide>

Demo: <https://t.me/JoyIDBot>

Github: <https://github.com/nervina-labs>



扫码加入 Tg dapp 开发者群