# UNIPASS

Universal Passport for Internet and Metaverse

知县 @ Lay2

# 红包第一弹

# 用户体验
# 技术实现


邮件恢复资产
邮箱 + 密码登录
指纹 / 扫脸签名
微信内即开即用
链上社交恢复体系
Subtle Crypto 密钥基础设施
WebAuthn 密钥基础设施
基于离线授权的双层密钥体系
基于密码学的邮件链上验证系统
Nervos CKB

# 前菜

- 底层支撑 - Nervos CKB 的两大特性
- 已经铺好的道路 - SubtleCrypto 和 WebAuthn
- 让区块链看懂邮件 - DKIM 简介

# 底层支撑 - Nervos CKB 的两大特性

- 自定义密码学
  - 举例：P-256 在 ETH / EOS / CKB 上的支持方式
  - PW-SDK：「白嫖」ETH / EOS / Tron / Near 等公链基础设施
    - ETH：Secp256K1 + Keccak256
    - EOS：Secp256K1/P-256 + SHA-256
    - Tron：Secp256K1 + Keccak256
    - Near：Ed25519 + SHA-256

# 底层支撑 - Nervos CKB 的两大特性

- 底层账户抽象 - 所有 CKB 地址都是智能合约钱包地址
  - CKB 地址格式 - RFC
  - 模拟各公链钱包签名格式
    - https://pay.lay2.dev
  - 自定义任何解锁逻辑
    - 根据行为解锁 - Anyone Can Pay
    - 基于离线授权的代理签名

# 已经铺好的道路 - SubtleCrypto 和 WebAuthn

- SubtleCrypto
  - 原 Web Crypto API
  - 可以在浏览器中生成由底层管理的 CryptoKey 对象，生成非对称密钥对时可将私钥设置为不可导出
  - 只有在 Secure Context 环境下可以调用
  - 支持 RSA / P-256 等签名算法，不支持 Secp256K1

# 已经铺好的道路 - SubtleCrypto 和 WebAuthn

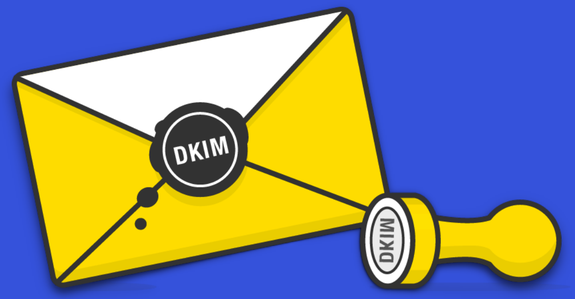
- WebAuthn
  - 全称 Web Authentication
  - 可以在浏览器中调用 FIDO 协议验证器进行密钥生成和签名
  - 支持环境：
    - Mac Touch-ID / iOS Touch-ID & Face-ID
    - Android Fingerprint
    - Windows Hello
    - Yubikey / Titan
  - 支持 RSA / P-256 等签名算法，不支持 Secp256K1

# 让区块链看懂邮件 - DKIM 简介

- DKIM - DomainKeys Identified Mail
- 主流邮件服务商会对邮件关键信息进行签名

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=twitter.com; s=dkim-201406; t=1627030779;
bh=Rk6d9VIajGPyKz4kz9NAYoemyhjAdxJzKvpF2zXT7wE=; h=Date:From:To:Subject:MIME-Version:Content-Type:List-Unsubscribe:
        Message-ID; b=rd78IeUn/Gw0IsogWSl13UGhUenN5Zs1ZRKLr7u0DbO+wOKTalHQbFuc+G/UjrfT8
        qicxW6xNoFg8trZB84BIKIZYK2+YUL1lLXK9/IpvmvaRS4cF+jo2k77xUY7wvy6du0
        UQBGrhb3iWrSPJl6m9qg9OhabkgDGFvPp5sCqB6ebwCFXhfWRM4qgZIET4dJ+I6rm6
        BP97XR9dmPPeL+nq/CCTYptcTWTfmQIfdyTwTXhuCS5D2C4s2Ea5dxq95Bw1pBmY3n
        vEHWlhGAXs/8iOO5f1RMtaWIihgpkUody6e4Z8cLkqadZWt1vuuLXPpmohnQDZ1hct
        T53BPcKZNpahA==
```

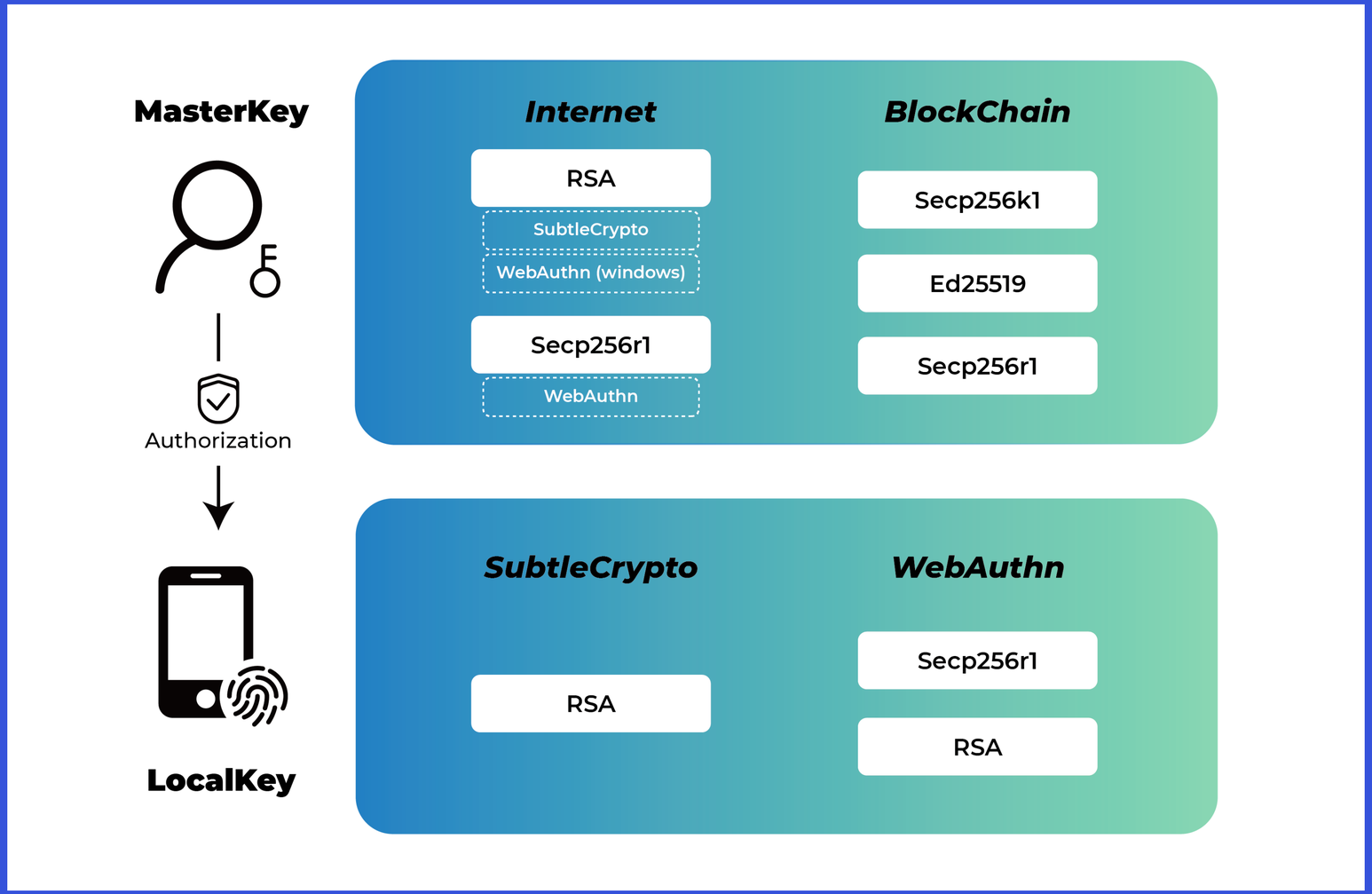
- DKIM 公钥公开可查
  - dig TXT dkim-201406._domainkey.twitter.com



# 正餐

- UniPass 的双层密钥架构
- 链上社交恢复

# UniPass - 双层密钥架构



# UniPass - 双层密钥架构

- MasterKey
  - 对应地址，承载资产
  - 注册时由前端生成或由外部提供（如 MetaMask / Ledger）
  - 加密：用户密码 —KDF(2^18)—> 强密码 —AES256—> Pem / KeyStore
  - 存储：UniPass 存储 / 第三方云存储 / 导出后自行保存
- LocalKey
  - 新环境登录时生成（多种格式），不可导出
  - 用于日常操作，需要配合 MasterKey 签发的授权使用
  - 登录时解锁 MasterKey 签发授权，之后本地只有 LocalKey 和授权存在

# UniPass - 双层密钥架构

- 多设备统一
  - 所有环境统一使用 MasterKey 对应的地址
  - 每个环境的 LocalKey 对应一个 MasterKey 的授权
- 不容易泄露
  - MasterKey 日常操作环境中不存储、不出现
  - LocalKey 使用环境安全性高，且不可导出
    - SubtleCrypto 为原生应用级安全
    - WebAuthn 为系统及或硬件级安全

# UniPass - 链上社交恢复

- 社交恢复简介
  - 用预先登记的邮箱(一个或多个)进行身份验证,由「见证人」对邮件内容进行的审核,利用超级权限进行密钥重置或资产转移
- 为什么需要社交恢复
  - 对普通用户来说,管理私钥或者助记词非常困难,用户很容易丢失甚至泄露自己的密钥。社交恢复给了用户一种在丢失密钥的时候能够通过自己的邮箱或者亲友的邮箱来证明所有权,进而重设密钥或恢复资产的途径
  - 社交恢复降低了用户的使用成本,但是也因此损失了用户的自主权,因为拥有超级权限的见证人总是能够转移用户资产,用户需要信任这个第三方权威

# UniPass - 链上社交恢复

- 链上社交恢复
  - 通过在链上用合约直接确认邮件真实性，以及解析邮件内容，做到去中心化地社交恢复逻辑
- UniPass 的链上社交恢复流程
  - 用户注册时，MasterKey 对注册邮箱进行授权（签署加密遗嘱），后续可继续添加更多灾备邮箱，以及设置恢复逻辑（如 2 of 3 多签）
  - 用户忘记密码时，MasterKey 无法解锁，需要通过注册邮箱将加密遗嘱和资产转移的目的地址按照一定格式填写在邮件中并发出（收件人可为上链机器人或者自己另外的邮箱），并将邮件报文上链（多签则需要凑够发件邮箱的数量）
  - 合约验证邮件的 DKIM 以及加密遗嘱，如果两部分签名都正确，就授权将用户的资产转移到邮件中制定的新地址，此过程会经历约 48h 的时间锁

# 红包第二弹


NFT 谜语红包
- 看谜题，猜谜底，抢红包 -
「UniPass 是一套去中心化 __ __ 系统」
长按领取至钱包
抢 NFT 红包，玩加密新社交

# 甜点

- UniPass 红包原理简介
- 思考🤔：能否去掉密码？能否保持地址不变？

# UniPass 红包原理 🧧

- 目标
  - 接收方不需要提前向发送方提供地址，甚至可以领红包时再生成
  - 全程只需要一笔链上交易
  - 去中心化：除了收发红包的两个人，任何第三方无法冒领红包

# UniPass 红包原理 🧧

- 方案（以 A 给 B 发红包为例）
  - 在 KeyA 本地生成 KeyX，并用密码（也就是口令）加密
  - KeyA 签发红包 Cell 的花费权给 KeyX
  - 通过链接（二维码）将加密的 KeyX、授权、红包信息一起传递给 B
  - B 打开链接，前端获得 KeyB 对应的地址（没有就注册），用输入的口令解锁 KeyX，再用 KeyX 签交易将红包转给 KeyB 的地址，广播上链

# 思考🤔：能否去掉密码？能否保持地址不变？

- 密码来源于对 MasterKey 的依赖，如果没有 MasterKey 呢？
- 地址是否可以不对应 MasterKey 的公钥？
- 地址是否可以不对应任何公钥？


# Thanks

# Q&A

我们会邀请提问的小伙伴进入 UniPass 硬核群

知县 @ Lay2