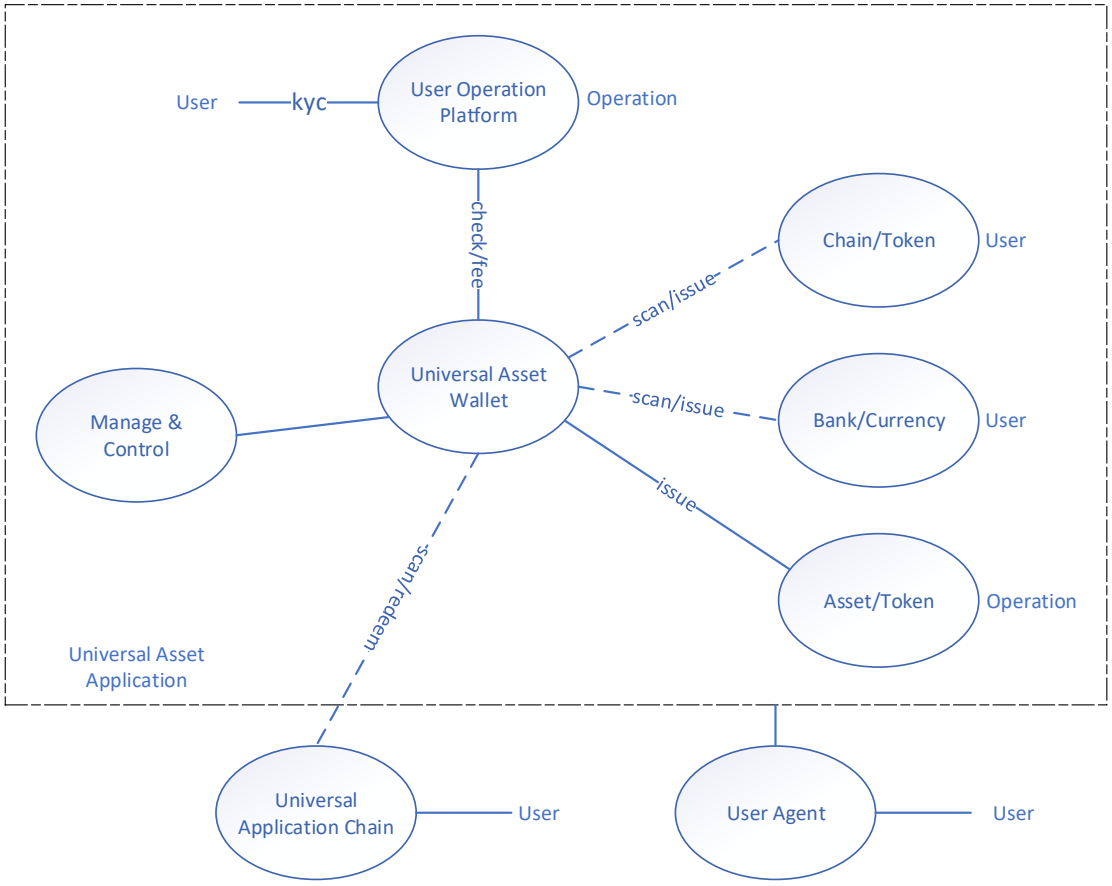
目录

UAA



Universal Application Chain（UAC）
基于 EOS 公链代码扩展的专用公链，增加了应用管理相关的特性。
UAC 公链核心代币符号 UAC，精度 4。

Universal Asset Application（UAA）
基于 UAC 公链实现的应用，提供代币跨链、法币 token 化、资产 token 化等功能。

Universal Asset Wallet（UAW）
与其他公链及各种平台连接，提供充值、铸造/赎回、token 保管等功能。

User Operation Platform（UOP）
提供用户注册，准入规则，收费规则等功能。

Manage & Control（U&C）
为 UAW 提供安全管控、风险管控等功能。

Chain/Token
公链及公链代币。

Bank/Currency
银行及银行账号。

Asset/Token
资产评估及资产 token 化。

User Agent
用户代理类似传统行业代理，具有自己的用户群和业务渠道。
代理向 UAA 充值获取 UAC 代币，向 UAA 赎回提现；
代理的用户向代理充值获取 UAC 代币，向代理赎回提现；
代理的用户不直接与 UAA 交互；

User
可以是自然人、交易所、机构、用户代理等各种参与者。

UAC 账号

用户可以向 UOP 申请或向第三方申请。

代币跨链

把其他公链的代币 1:1 映射到 UAC 公链，实现不同公链代币在 UAC 公链的流通。

以 BTC 为例，

接入
UAW 接入 BTC 公链，创建 BTC 充值地址；
UAW 在 UAC 创建 UBTC 代币；

铸币
用户从 UOP 确认是否被允许使用 BTC，只有被允许才能进行 BTC 充值；
用户从 UOP 获取 UAW 的 BTC 充值地址，按充值认定方法向充值地址转账 BTC；
UAW 扫描 BTC 充值记录，按充值认定方法确定充值用户；
UAW 向 UOP 验证用户是否被允许使用 BTC；
UAW 铸造等额 UBTC 代币并转入用户 UAC 账号；

使用
用户可以在 UAC 使用 UBTC 代币进行转账；

赎回

用户从 UOP 确认是否被允许使用 BTC，只有被允许才能进行 BTC 提取；
用户从 UOP 获取 UAW 的赎回地址，并向赎回地址转账 UBTC（携带 BTC 接收地址）；
UAW 扫描 UAC 赎回记录；
UAW 向 UOP 验证用户是否被允许使用 BTC；·
UAW 从 UOP 获取扣除费用后的实际转账数额，往用户 BTC 接收地址转账 BTC，从 UAC 赎回地址销毁实际转账数额的 UBTC；

隐私情况下，赎回记录中携带的接收地址可以是 UOP 注册时绑定的接收地址代号。
使用代号存在一定的转换风险。

用户从交易所提现 BTC 到 UAC 账号，
1，如果交易所在 UAC 有账号且有足够 UBTC，可以直接转账 UBTC 到用户 UAC 账号；
2，如果交易所支持备注/签名方法，则可以使用备注/签名方法提现到用户 UAC 账号；
3，否则，用户只能先从交易所提现 BTC 到支持备注/签名方法的钱包，再充值转账到 UAC 账号；

充值认定方法，
1，备注方法，支持部分币种，备注格式：uac:UAC_account
   a) BTC 系列，交易中包含一个 UAW 充值地址和一个 op_return，如果 op_return 满足格式，则认定向 UAW 的充值为 op_resurn 携带的 UAC_account 的充值；
   b) ETH 系列，只支持 ETH 充值，如果 data 满足格式，则认定向 UAW 的充值为 data 携带的 UAC_account 的充值；
   c) EOS 系列，如果 memo 满足格式，则认定向 UAW 的充值为 memo 携带的 UAC_account 的充值；
2，签名方法，支持各种代币，以 BTC 为例，
   a) 获取转账交易 BTC_txid；
   b) 使用 BTC 私钥 BTC_key 对 BTC_txid+UAC_account 签名，BTC_sign = sign(BTC_key,BTC_txid+UAC_account)；
   c) 在 UAC 发送绑定消息 bindtx(BTC_sign, BTC_txid, UAC_account)；
   d) UAW 扫描绑定消息，如果 BTC_sign 提取公钥能够验证 BTC_txid 转账记录，则认定为 UAC_account 的 BTC 充值；

钱包实现参考：

转账带备注
1，如果交易支持备注，则直接添加到交易中，
2，如果不支持备注，则使用签名方法，
  1）如果不是往 UAC 充值，则拒绝转账，无备注可能出现问题，
  2）使用《消息签名发送》流程，备注放入 bindtx 的 memo，

消息签名发送
1，转账交易签名时，同时生成和签名 bindtx 消息，一个交易中只能包含一个转账，
   a) bindtx: to,msg,msgSign，to 为转账交易的接收地址，msg+msgSign 为验证信息
   b) msg: chain,txid,prev,memo， chain 为公链，txid 为转账交易，prev 为输入数额（btc

系列），memo 为备注，

c) msgSign 转账交易的私钥对 msg 进行签名，btc 系列使用 prev 对应的私钥签名，

2，把交易 raw 放入 btc_transactions 表，把 bindtx 放入 bindtx_send 表，两者具有对应关系，raw 重建时 bindtx 也失效，

3，钱包定时发送 bindtx 到 UAC，不需要稳定块确认，使用专用的 UAC 账号，

4，钱包扫描 UAC bindtx 记录，用发送 UAC 账号过滤，标记 bindtx 发送成功，

5，转账与 bindtx 不需要完全同步，接收方应该在两者都到达后才会进一步处理，

集中充值接收

1，钱包把集中充值地址加入 bindtx_address 表，

2，钱包扫描 bindtx 放入 bindtx_recv 表中，过滤 to 在 bindtx_address 中，

3，钱包把 bindtx_address 的充值放入 incoin_pendtx，其他的放入 incoin_transactions，

4，钱包定时扫描 bindtx_recv，与 incoin_pendtx 进行匹配验证，

5，匹配完成的充值放入 incoin_transactions 中，

6，从 API 接收的 bindtx 与从 UAC 扫描的相同处理，

法币通证

把银行账号的法币按 1:1 映射到 UAC 公链，实现法币在 UAC 公链的流通。

以 USD 为例，

接入

在银行开设账号，UAW 接入银行账号。

铸币

用户从 UOP 确认是否被允许使用 USD，只有被允许才能进行 USD 充值；

用户从 UOP 获取 UAW 的 USD 账号，向 USD 账号转账；

UAW 扫描 USD 账号记录，确定充值用户；

UAW 向 UOP 验证用户是否被允许使用 USD；

UAW 铸造等额 UUSD 代币并转入用户 UAC 账号；

使用

用户可以在 UAC 使用 UUSD 代币进行转账；

赎回

用户从 UOP 确认是否被允许使用 USD，只有被允许才能进行 USD 提取；

用户从 UOP 获取 UAW 的赎回地址，并向赎回地址转账 UUSD（携带 USD 接收银行账号）；

UAW 扫描 UAC 赎回记录；

UAW 向 UOP 验证用户是否被允许使用 USD；·

UAW 从 UOP 获取扣除费用后的实际转账数额，往用户 USD 接收银行账号转账 USD，从 UAC 赎回地址销毁实际转账数额的 UUSD；

隐私情况下，赎回记录中携带的银行账号可以是 UOP 注册时绑定的银行账号代号。
使用代号存在一定的转换风险。

资产通证

资产评估通证化后，把资产通证映射到 UAC 公链，实现资产通证在 UAC 公链的流通。

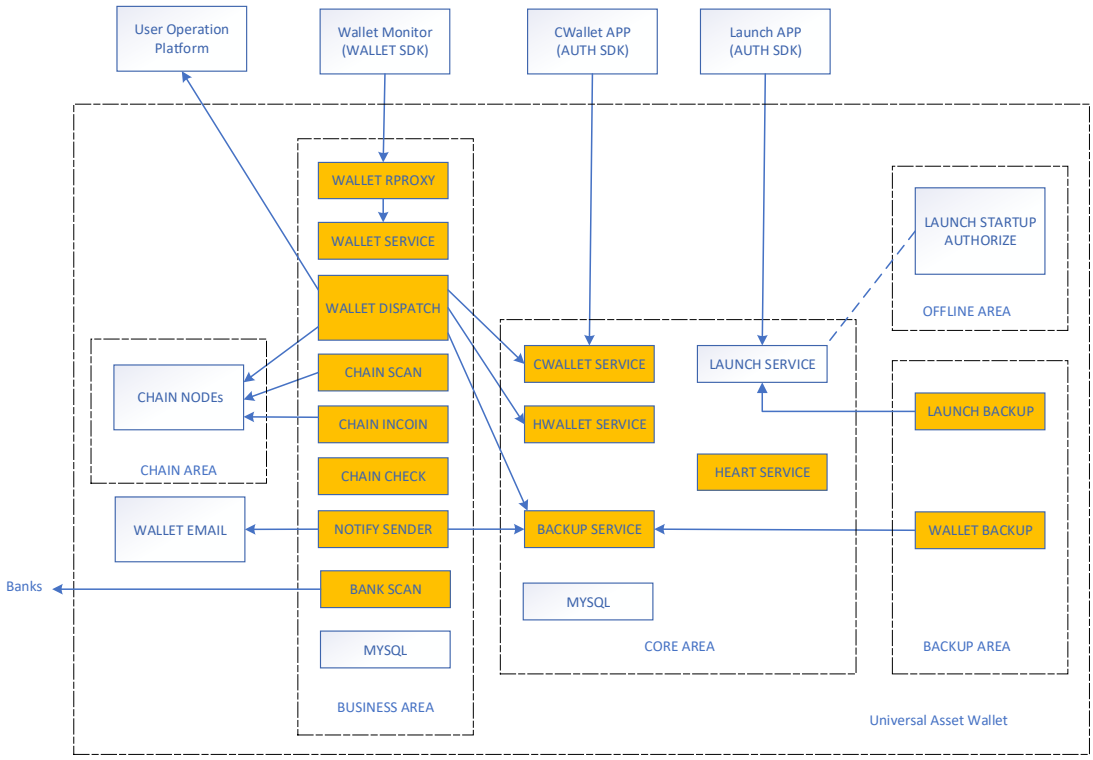
以鞋子为例，

铸币
运营有 10 双耐克鞋子，每双评估 1000USD，运营可以在 UAC 发行 10000 个 NAIKE 代币，每个 NAIKE 代币初始 1USD，1000 个 NAIKE 代币可以兑换一双鞋子。

使用
可以在 UAC 使用 NAIKE 代币进行转账；
可以转到交易所交易；

赎回
用户在收集到足够的 NAIKE 代币后，可以兑换成鞋子；
用户从 UOP 确认是否被允许使用 NAIKE，只有被允许才能进行 NAIKE 提取；
用户从 UOP 获取 UAW 赎回地址、UAW 收费地址、NAIKE 收费，在同一笔交易中向赎回地址转账 NAIKE，向收费地址转账 UAC；
UAW 扫描 UAC 赎回记录、收费记录；
UAW 向 UOP 验证用户是否被允许使用 NAIKE；·
UAW 向 UOP 验证收费，从 UAC 赎回地址销毁 NAIKE，通知运营赎回用户及赎回数量；

UAW



工作区

1，BUSINESS AREA，业务工作区，实现 UAW 的业务功能逻辑，
   a) WALLET RPROXY，反向代理和负载均衡，保持 UAW 的平滑升级和稳定在线。
   b) WALLET SERVICE，实现 UAW 接口。
   c) WALLET DISPATCH，实现 UAW 功能调度。
   d) CHAIN SCAN，区块链数据解析。
   e) CHAIN INCOIN，区块链充值入库。
   f) CHAIN CHECK，检测区块链状态。
   g) NOTIFY SENDER，UAW 运行通知。
   h) BANK SCAN，银行账号扫描。
   i) MYSQL，存放数据，采用主从模式。
   j) 该工作区网络只允许白名单 INPUT，白名单 OUTPUT。
2，CORE AREA，核心工作区，管理 UAW 关键数据及相关逻辑，
   a) CWALLET SERVICE，实现冷钱包的私钥管理和交易签名。
   b) HWALLET SERVICE，实现热钱包的私钥管理和交易签名。
   c) LAUNCH SERVICE，模块的启动和配置授权服务。
   d) BACKUP SERVICE，模块的业务数据异地备份服务。
   e) HEART SERVICE，模块的心跳监测服务。

f) MYSQL，存放数据，采用主从模式。

g) 该工作区网络只允许白名单 INPUT，禁止 OUTPUT。

3, BACKUP AREA，备份工作区，

a) LAUNCH BACKUP，模块配置数据的异地备份客户端，在不同地区不同运营商构建备份节点。

b) WALLET BACKUP，模块业务数据的异地备份客户端，在不同地区不同运营商构建备份节点。

c) 该工作区网络禁止 INPUT，只允许白名单 OUTPUT。

4, CHAIN AREA，区块链工作区，存放区块链接入节点。

a) 节点 API 端口使用内网地址，数据端口使用外网地址。

b) 该工作区网络只允许白名单 INPUT 到节点 API 端口，禁止 OUTPUT 到其他工作区的机器。允许 INPUT 到数据端口，OUTPUT 到外部机器。

5, OFFLINE AREA，离线工作区，

a) LAUNCH STARTUP AUTHORIZE，授权 LAUNCH SERVICE 启动和配置。

b) 该工作区禁止连网。

模块结构

1, SECURITY BASE，基础安全工具，

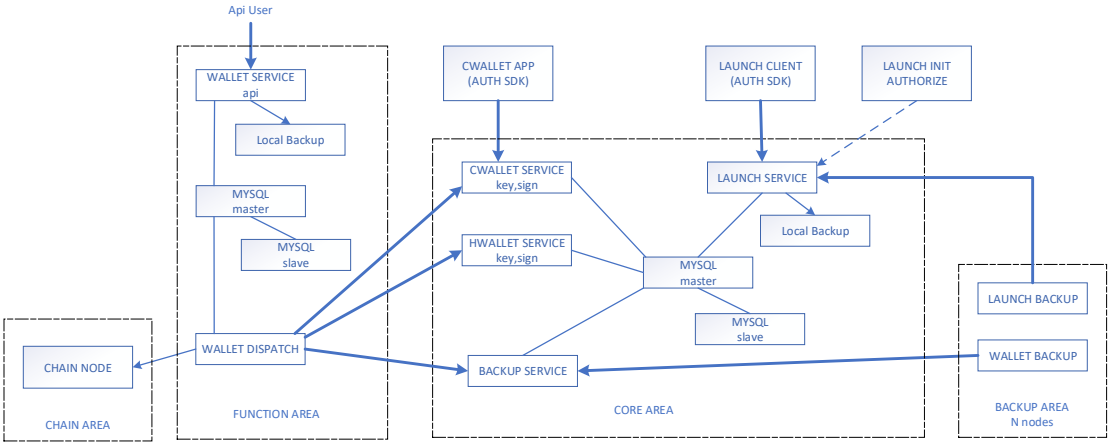
a) SO，包括运行时加密、持久化加密、启动验证逻辑等，采用指令级混淆编译。

b) BASE SDK，基于 SO 的安全增强工具包。

2, SECURITY SDK，应用授权、应用加密、数据库等安全增强工具包。

3, APPLICATION，基于 SECURITY 工具包实现应用模块。

安全设计



运行安全

1，安全开发库
    a) 多种安全防护开发工具，
    b) 运行时关键数据始终处于加密状态，
    c) 运行时内存及时清理防护，
2，验证授权机制
    a) 代码验证、密码验证、多次确认等多种方法，确保仅对可信的应用授权运行，
3，配置系统，
    a) 关键数据封闭管理，管理员和关键数据分离，管理员不可见关键数据，
    b) 关键配置集中管理，代码和关键配置分离，开发人员不可见关键配置，
    c) 关键数据集中管理，代码和关键数据分离，开发人员不可见关键数据，
    d) 根据安全性不同要求，管理员、关键配置、关键数据、应用分区管理，
4，运维安全，
    a) 操作系统安全扫描，
    b) 约束网络访问权限，
    c) 约束软件安装，

通信安全

1，模块之间的通信采用 AES256 加密和谷歌验证码校验，
2，模块之间的访问采用授权配置，
    a) 仅允许被授权的用户访问，
    b) 仅允许被授权的机器访问，
    c) 仅允许访问被授权的接口，
3，运行时授权配置隐藏在授权框架内，应用代码与通信加解密及授权验证分离，
4，各模块与数据库通信全部采用 ssl 加密，

数据安全

1，关键数据全部加密，
    a) 配置管理系统的各种数据由 5 个加密键加密，
        i. 2 个由系统提供，
        ii. 3 个由配置授权管理员提供，
    b) 热钱包私钥由 5 个加密键加密，
        i. 由配置管理系统生成并封闭加密管理，人工不可见，
    c) 冷钱包私钥由 5 个加密键加密，
        i. 2 个由加密键由配置管理系统生成并封闭加密管理，人工不可见，
        ii. 3 个由冷钱包管理员提供，
2，地址私钥存储，

a) 核心区数据库主从，
b) 异地多备份，
c) 在异地 2 备份后才可使用，

3，配置系统存储，
a) 核心区数据库主从，
b) 异地多备份，
c) 键值和变量等核心数据在异地 2 备份后才可使用，

4，数据签名验证，
a) 各模块产生数据时，对数据做签名并一起存储，用于验证数据正确性，
b) 各模块备份数据时，发送端对数据做传输签名，接收端验证传输签名，确保数据传递的正确性，

接入安全

1，区块链用户的操作来源于区块链节点记录扫描，并加了一定的确认块验证，
2，银行用户的操作来源于银行账号记录扫描，
3，用户操作完全由用户签名发起，表达用户真实操作，

总结

1，采用封闭管理和封闭运行机制，在 UAW 内部拦截网络、扫描系统、伪造请求、修改数据等可能性大大降低，
2，采用多种备份机制，重要数据的丢失或篡改可能性大大降低，
3，采用多种多重加密机制，通过窃取私钥盗取资产可能性大大降低，

M&C

安全管控

1，CWallet APP，冷钱包授权客户端。UAW 保管的各种 token，在累积到一定数额时会自动归集到冷钱包中，提供更安全的存储，只有多位冷钱包管理员共同授权才能动用冷钱包保管的 token。
2，Launch APP，启动授权客户端。UAW 各模块的配置均由 LAUNCH SERVICE 加密管理，LAUNCH SERVICE 需要多位管理员共同授权才能启动，确保 UAW 由多位管理员共同管理。

风险管控

Wallet Monitor，UAW 监控平台。设置 UAW 阈值、查看 token 进出、余额平衡状况等。

UOP

用户注册

使用 UAA 的用户必须通过 KYC。

准入规则

从不同地区接入的用户，需要遵守当地的规定，使用 UAA 的部分功能。

收费规则

进入 UAA 一般免费，从 UAA 赎回/提现需要收取一定费用。