1、 云端矿池设计方案

1 需求

为了实现满足云端矿池的功能需求，编写此文档。

需求：

- 在FOGGIE-V的基础上，搭建云端矿池，让新版的foggie-desktop（尽快在移动端实现）接入矿池
- 云端矿池帮助移动端实现链上买单，链上达成共识的工作，形成闭环。
- 接入矿池的客户端数量用来衡量矿池得到的销售返点。
- 云端矿池用邀请码的形式来接收客户端
- 云端矿池的运营方（Fog Works）要有合理的收费模式来和矿池的拥有方（销售大使）来分享收益用来cover云端矿池的成本

2 功能设计：

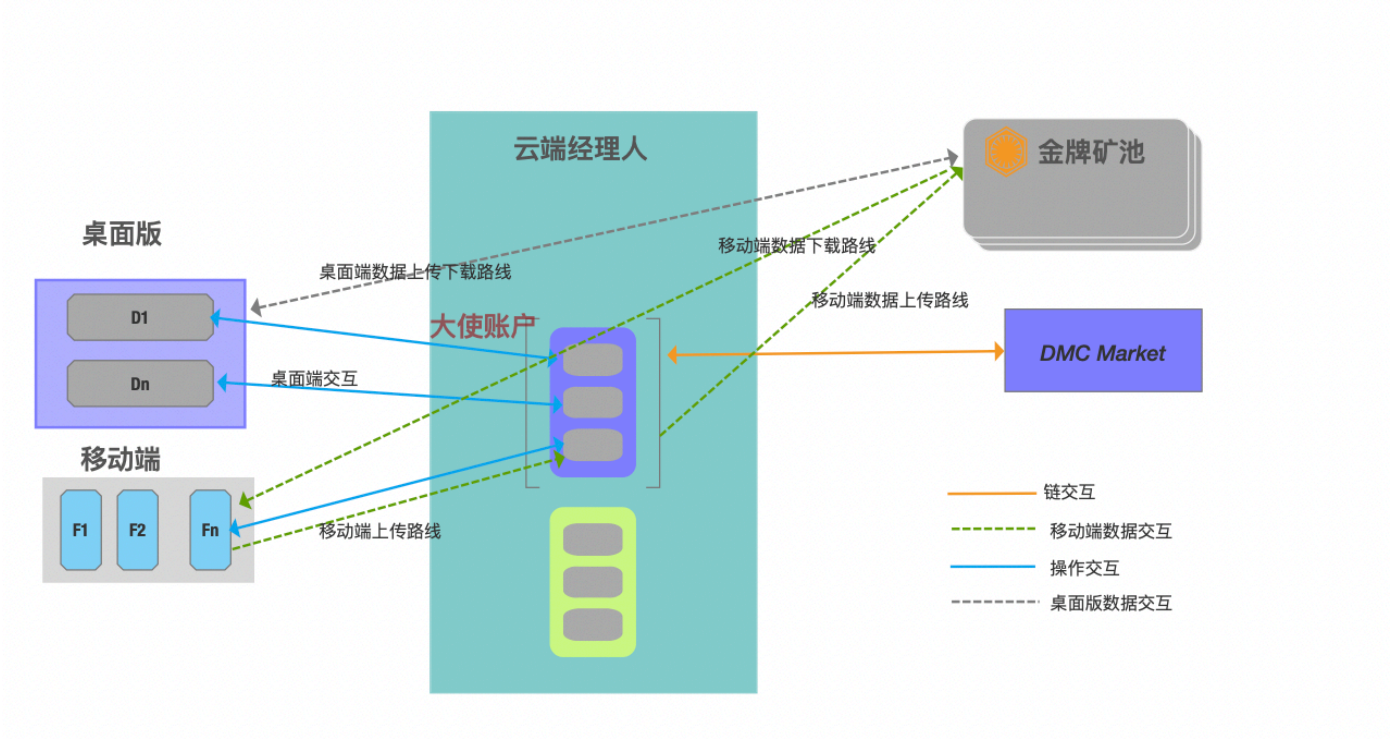
2.1 功能要点：

- 支持DeskTop客户端/手机端可以使用此功能完成上传下载需求
- 支持大使经理人模式完成挖矿必须的买单、达成共识、挑战等操作
- 大使需要购买经理人账户，并可以管理收益和分配，根据收益抽成和设置分配模式。
- 链上功能使用大使账户完成操作
- 购买官方指定矿池（金牌矿池）的订单操作

名词解释：

- AMB: 大使(Ambassador),对应名词云端经理人或平台。指负责代理处理链的人，所有操作归集为大使操作。大使拥有与链交互的DMC账户的轻权限私钥。可以对链发起买单，共识、挑战、抽取、获取分红奖励等操作。
- AMB Node：大使平台中，专门负责处理数据和链交互的节点。一个大使根据当前有效PST数目（订单在有效期内的）计算需要几个Node来提供服务。
- AMB Center：AMB 中心，是大使登录的管理平台，负责管理大使账户的资源、账户、收益等。

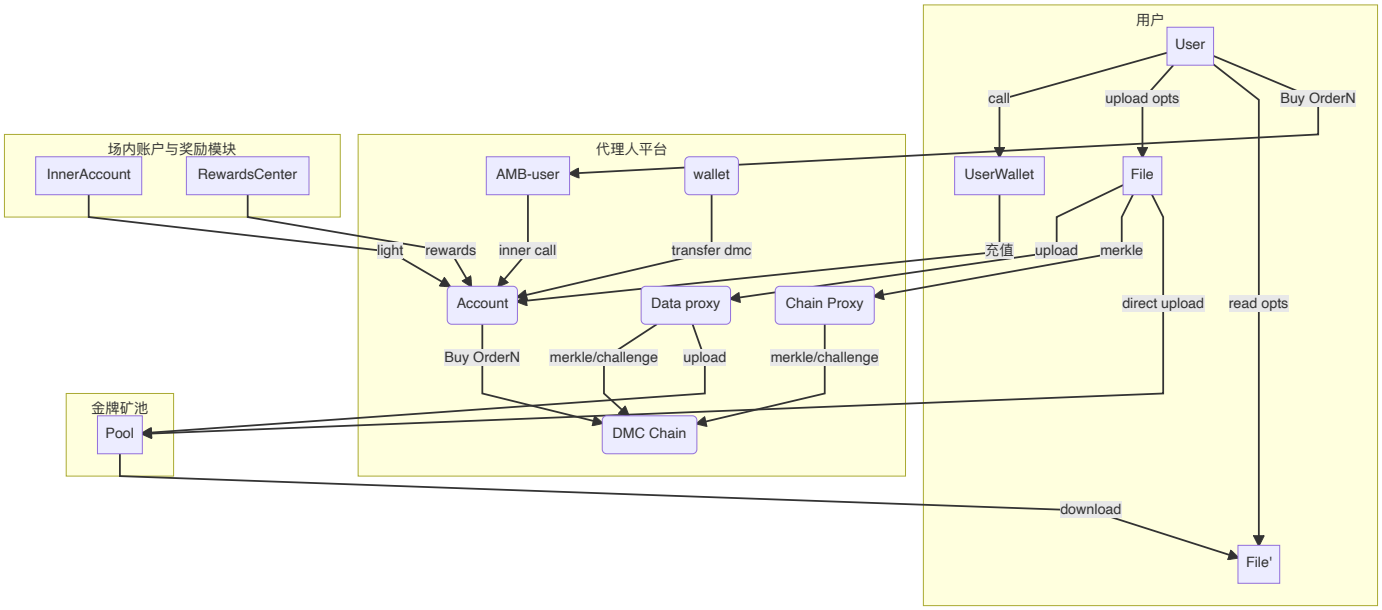
2.2 整体设计如下：



根据该设计有以下功能点：

- 客户加入云端经理人管理的云端矿池
  - 客户根据邀请码不同加入不同的云端经理人
  - 客户需要充值所需购买的空间大小、周期的DMC。
  - 客户可以管理和查看自己的DMC资产，包含提现、充值、购买等操作
  - 客户可以查看自己购买订单的收益和进度
  - 客户可以上传数据、下载预览和查看数据
  - 客户可以通过不同的客户载体访问订单。但移动端上传的数据的订单，不能在桌面版进行数据操作。反之亦然。
- 云端经理人
  - 批准加入云端矿池的客户群体，可以设置默认自动接收模式和手动批准模式。
  - ~~云端经理人要购买经理人账户（大使账户）~~ ***（通过社区/基金会购买，本功能不包含此功能）***。
  - 云端经理人可以查看订单信息和收益详情
  - 客户通过扣除自己账户的资金，委托经理人进行买单，取消订单操作。
  - 桌面客户端数据在本地计算merkle数据，并将merkle 提交到云端经理人，经云端经理人的大使账户提交共识。
  - 移动端数据可以直接将数据提交到云端经理人处，经云端经理人计算后，提交共识。数据有变化，24小时内自动提交merkel/
  - 桌面端用户可以自主提交挑战。
  - 移动端数据可以有经理人代为发起挑战。
- 金牌矿池
  - 云端经理人买单需要优先购买金牌矿池空间。待金牌矿池无空间后，云端经理人可以购买其他矿工数据。页面需要提示。

根据以上功能整体模块设计如下：



名词解释：

User: 代表用户

UserWallet：代表用户的钱包，通过用户钱包可以进行充值操作

AMB-User：代表大使账户下的用户绑定账户。

Data-Proxy：数据代理处理，属于AMB-Node服务

Chain-Proxy: 链代理服务，属于AMB-Node服务

2.3 功能点

2.3.1 客户端

需要在Desktop端增加一款产品云端矿池。与目前foggieV/Storage 并列的产品。该产品不需要用户私钥，只需要用户名称12位地址。

需要IOS/Android端增加移动云端矿池功能。IOS有北京团队完成。

2.3.2 云端经理人

云端经理人需要功能较多，从操作人员分类： 云端经理人管理平台，云端经理人数据处理功能。

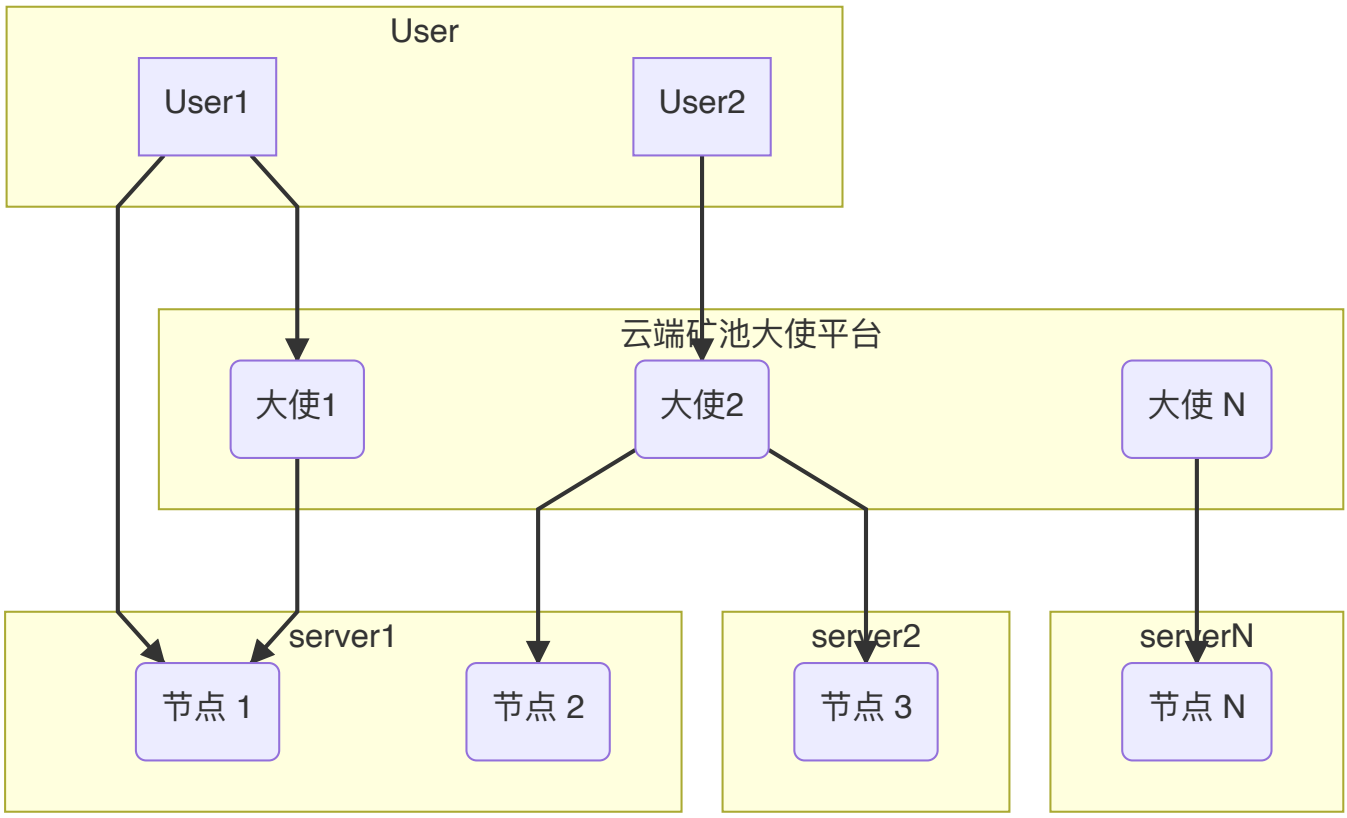
主要设计如下：

- 统一的管理平台；

  云端矿池管理平台：使用人员面向基金会管理人员，负责管理大使账户。

  云端矿池大使平台：AMB Center，使用人员为大使。

- 每台服务器可以支持多个云端经理人,或每个经理人可以管理多个服务器上。



云端经理人（大使）管理平台应包含以下主要功能：

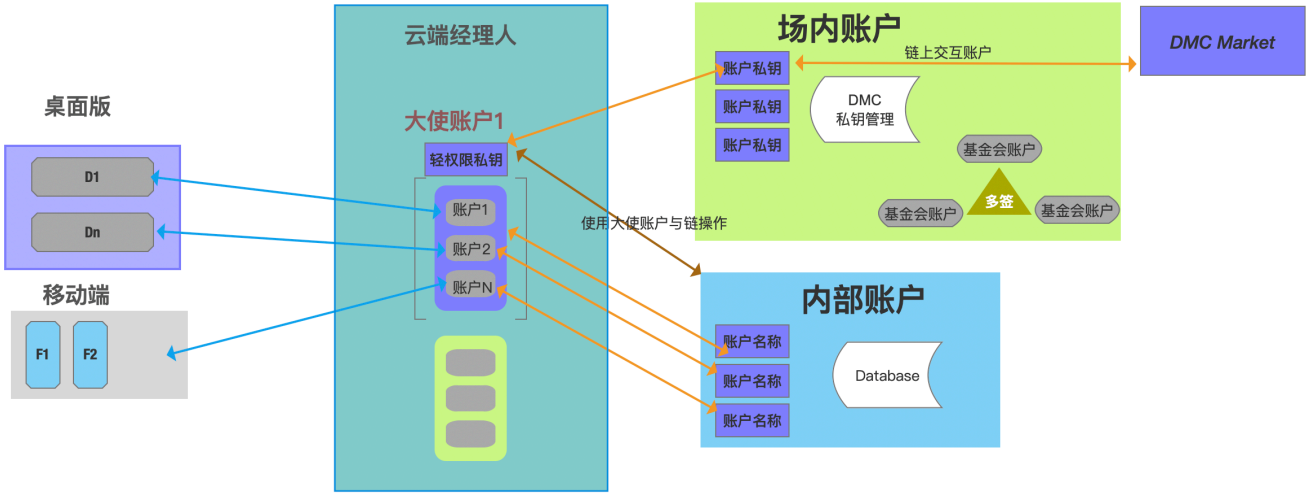
- 认证管理：
  - 平台使用JWT认证模块认证登录。邮箱注册与登录
- 资产管理
  - 可以查看经理人账户的资金收益记录、充值和提现功能。
  - 可以为加入用户进行抽水设置，并进行分红发放。
- 用户管理
  - 可以查看加入经理人的用户，并查看用户的订单信息、收益信息。
  - 可以审批用户管理和冻结用户。
- 数据管理
  - 可以查看经过经理人的数据处理的订单成交merkle信息。数据大小。不能查看数据详细内容。
- 云端经理人数据处理功能：
  - 为了满足移动用户使用矿池的需求，需要辅助用户完成数据的共识操作，
  - 要求移动端数据更新后，24小时内更新一次merkle。
  - 链挑战功能：客户端发起挑战VS 经理人发起挑战；~~支持链下挑战功能。一周内每个订单需要完成线下挑战不少于一次，链下挑战不正确，需要进行链上挑战。~~
  - 订单完成后，需要清理挑战需要的敏感数据。
  - 移动端数据做完merkle后，要删除用户数据。
  - 用户上传的敏感数据需要安全存储
  - 与链交互的私钥使用轻权限模式。

2.3.3 DMC账户与经济模型

- 场内账户

  提供场内账户体系

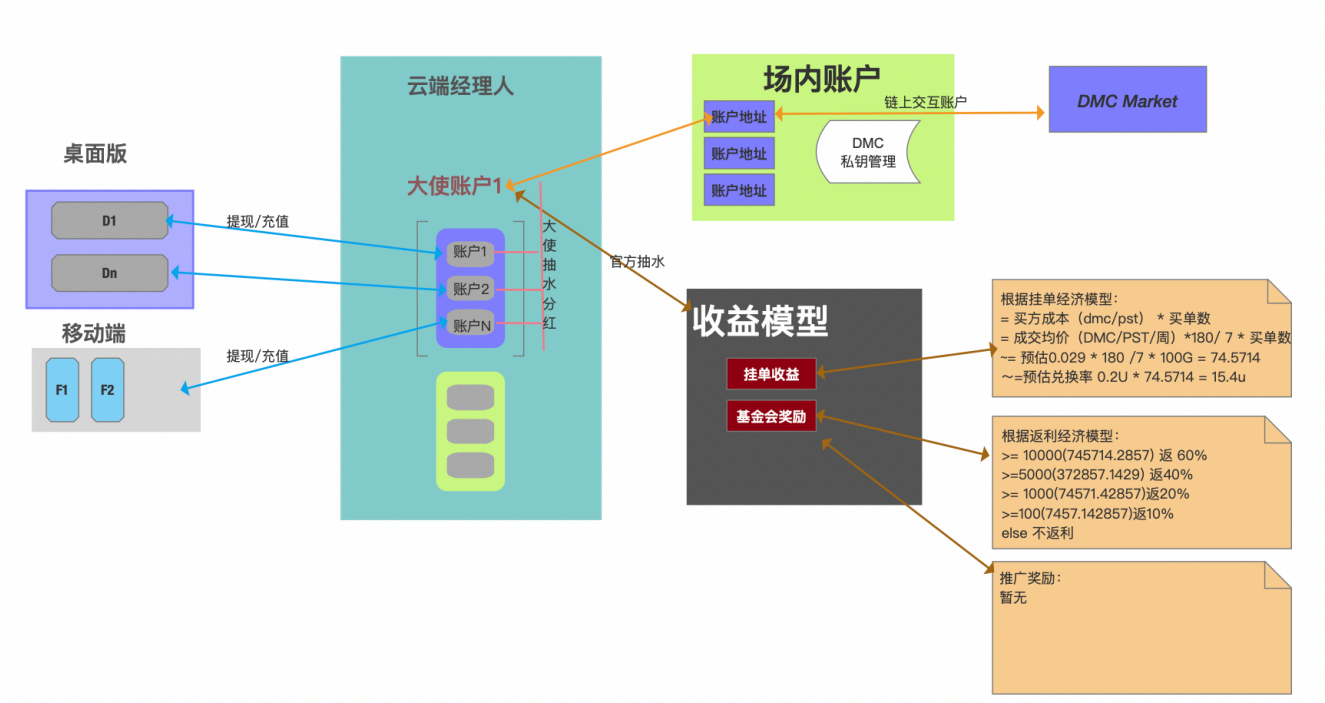
  - 提供场内账户系统，每个账户派生出轻权限私钥。
  - 转账功能有场内账户统一管理。
  - 买单、共识、挑战操作有轻权限账户操作。
  - 轻权限账户运行在所在节点的服务上。
  - 基金会账户有多签功能保护，主要用户基金会给场内账户提供奖励资金
  - 场内账户负责官方抽水，抽水限定为提现的***（5%，暂定）***的抽成。
  - 场内账户防止链回滚，最后一笔金额到账***5分钟内***不能提现。
  - 场内账户提现每天最多10000DMC(1万DMC，可配置)。
  - 场内账户提现会确认链回滚的场景（后期）
- 基金会账户
  - 负责给云端经理人(大使)账户激励dmc的账户。
  - 账户通过多签方式进行管理。3个账户，每个权重为1，2/3满足可以发起提案；



- 经济模型

  根据基金会奖励模型设置的经济模型有2种。一是挂单收益，二是基金会奖励

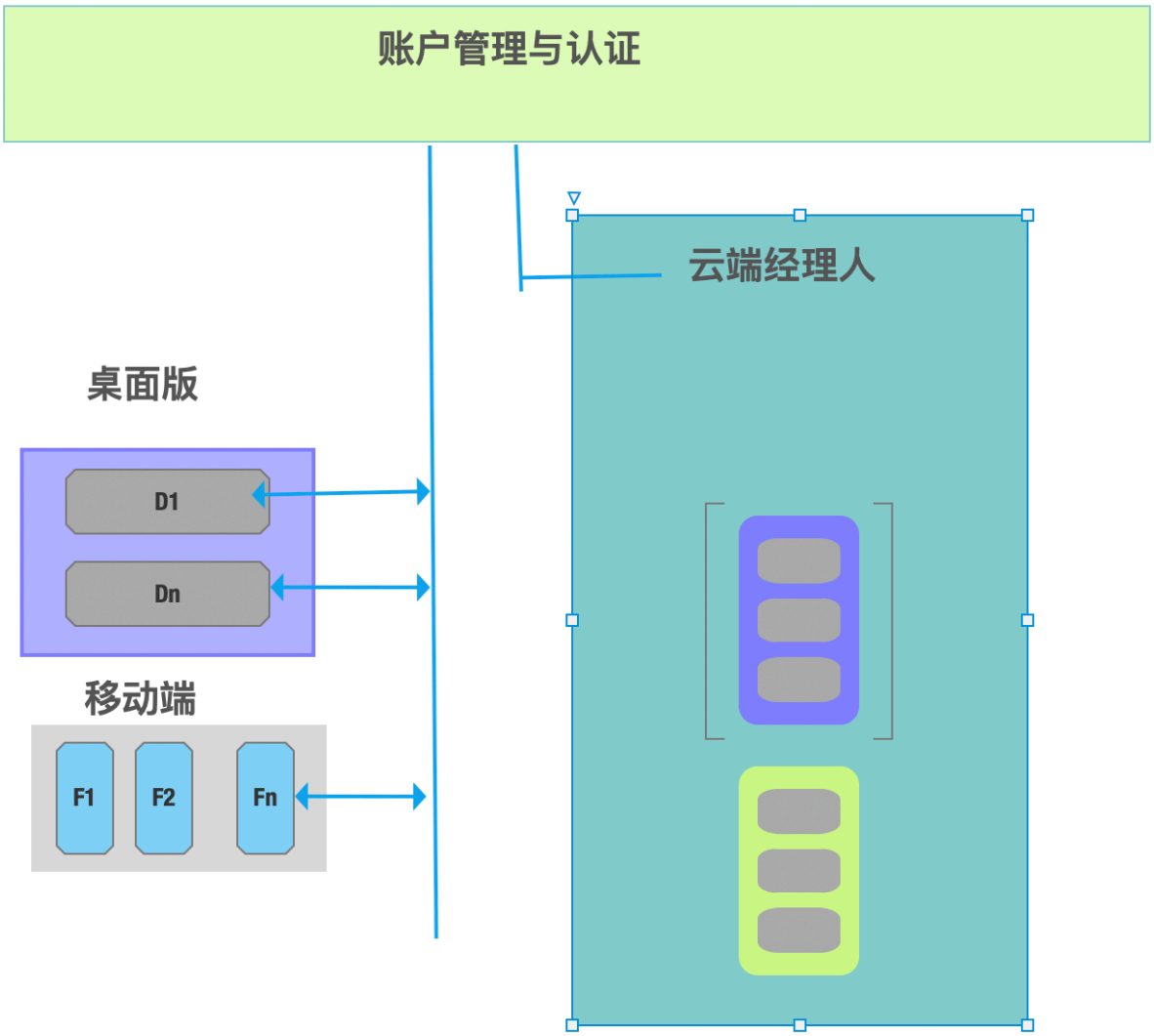
  经济模型：***基金会奖励功能目前有基金会通过管理平台人工负责***。



2.3.4 账户管理模型

- 账户登录体系

  要求用户通过不同设备接入后，查看用户挂单信息。



3 详细设计

3.1 经理人(大使)平台

3.1.1 帐号管理

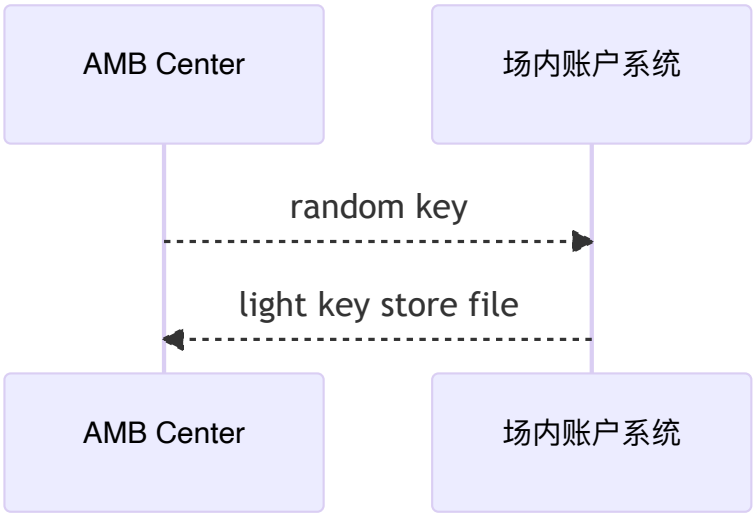
- 帐号注册
  - 社区提供二维码，社区大使扫描后登录/注册。注册填写申请信息。二维码包含邀请信息和登录注册地址
  - 经理人通过“邀请码”注册账户。邀请码通过市场或销售获取，邀请码与经理人注册一对一。
  - 注册信息需要使用经理人帐号，邮箱，邮箱验证码，密码进行注册；
  - 注册后，需要经理人绑定自己的DMC钱包地址。
  - 简化登录：钱包登录流程。

    经理人可以通过dmc钱包进行登录和注册。当使用DMC钱包登录后，建议用户绑定邮箱和密码。
    - DMC 钱包验证流程：使用dmc钱包插件进行进行签名，将签名信息+钱包名称发给平台
    - 后台通过获取该钱包的公钥进行验签，成功后，用户可以登录。

        - 登录后，用户账户右上方提示黄色感叹号！建议邮箱绑定，便于找回账户和方便其它方式登录。
        - 使用邮箱注册的用户，可以使用绑定的钱包账户一键登录。

          没有绑定邮箱，或者第一次注册的钱包作为新账户启用。
    - 账户注册后，会分配场内账户，详见dmc账户管理
    - 没有邀请信息的可以提请申请。申请后需要主动联系社区，页面提示需要联系社区的方式。
    - DMC账户绑定后，账户右上方提示红色感叹号！，需要提示：***你的DMC钱包不受安全保护，需要设置2FA！***（即开启google 验证码验证）
- 账号管理
    - 登录/退出
        - 支持云端经理人登录/退出平台
    - 注册经理人展示：帐号，邀请码，邮箱等信息展示；
    - 展示最后一次登录的时间。
    - 邮件激活账户。
    - 用户可以上传个人头像。
- 认证管理：
    - 支持JWT认证方式。
    - 访问采用HTTPS证书。证书Let'Encrypt 申请；
    - 登录使用经理人帐号/密码进行登录，5次失败后锁定1天；
    - 密码找回功能。通过邮箱确认码找回，更新密码后才能登录。
    - 密码修改功能：通过邮箱发送确认码，更新密码后页面要强制退出。
    - 页面退出功能：退出后，清理用户登录token。
    - 登录Agent信息管理：当前token只能允许当前用户浏览器登录。超时要自动更新证书。
- 邀请码管理：
    - 云端经理人注册时同步生成邀请码。（该邀请码信息用来供客户端使用注册）。
    - 一个邀请码可以供多人使用。
    - 邀请码时效设置，在指定失效内有效，过期提示邀请码过期，无法使用。
    - 邀请码可以多次生成。有记录可以查询。邀请码最低有效期7天，最长1年。
    - 第一个邀请码免费生成，新生成的邀请码按次收费。1次10DMC收费。
    - 多个邀请码同时生效。
    - 用户注册后，可以展示邀请码的来源。
    - 邀请码提供链接和邀请码二维码图片可以下载。如有用户头像，邀请码的二维码中包含用户头像。
    - 关于经理人发展下线人员邀请的规则：**一期暂不考虑**
        - 邀请码分为普通邀请码和下线经理人邀请码。

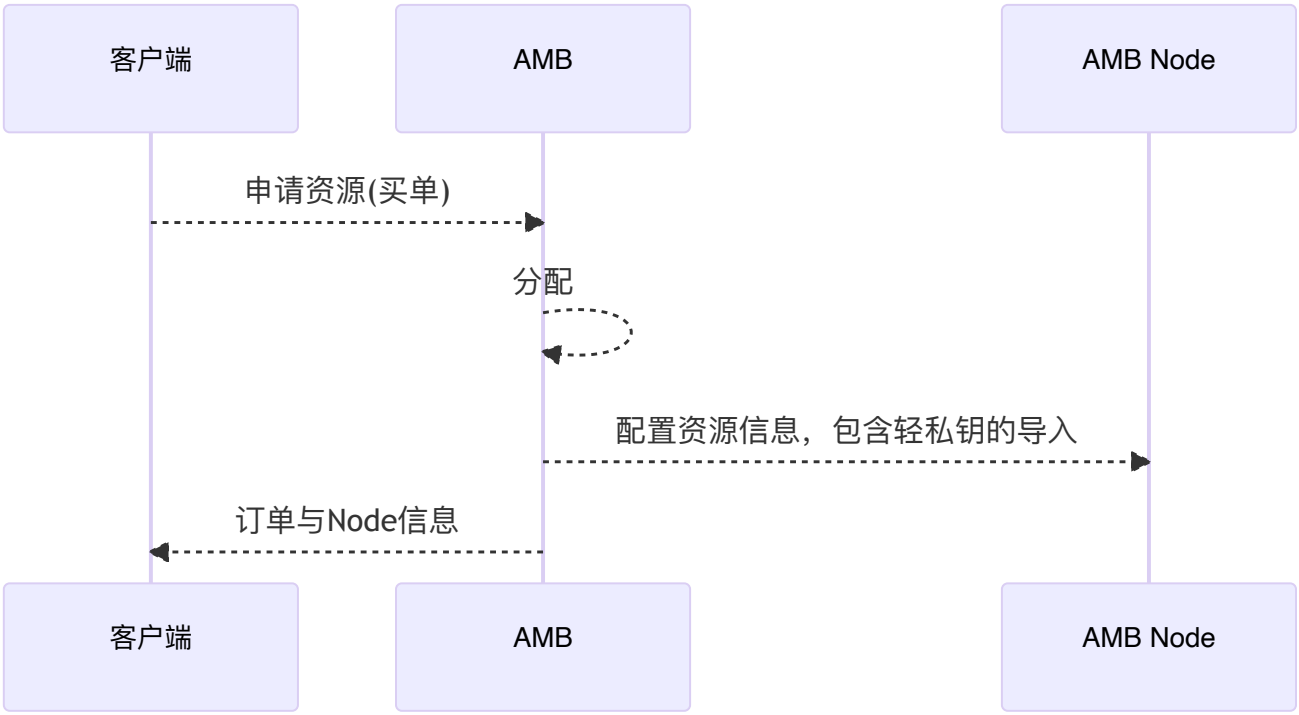
        - 下线大使邀请码人员使用邀请码可以登录经理人平台，需经管理员批准才能有效。
        - 下线大使邀请码带来的收益对上线的奖励有管理员进行核算和奖励。
- 成员账户管理：
    - 详见成员管理
- DMC 账户管理：
    - 查看DMC帐号信息，DMC资产信息。详见资产页面。只能看到账户名称，看不到私钥信息。
    - 大使拥有一个内部账户。该账户记录大使的利润和奖励数据和记录。
    - 获取轻权限账户
        - 通过场内账户获取轻权限账户。
        - 生成随机密钥和AMB经理人唯一信息请求场内账户，场内账户会利用该密钥生成加密后keystore文件返回给经理人。
    - 账户获取



3.1.2 节点管理

- 查看节点分配
    - 系统根据配置的分配策略默认分配访问的server Node
- 节点扩容/缩容
    - 当节点用户购买有效PST总数(手机端)达到上限时，自动扩容。
    - 当节点有效PST少于PST下限时，新买订单优先使用既有节点。
- 节点分配调度管理：

  调度资源依据当前***有效PST数***进行调配。并分发轻权限私钥。私钥要安全管理。



3.1.3 成员管理

- 用户管理
  - 注册加入
    - 新用户注册帐号时输入云端经理人邀请码进行注册
    - 提供扫描二维码，用户用手机扫描二维码实现注册和绑定。
    - 后台对用户输入的邀请码是否合法进行校验，不存在的邀请码或者已超过邀请时限的邀请码禁止加入；
    - 成员的唯一ID不能是钱包地址。
    - 用户登录平台后，绑定DMC钱包地址后，才可以加入云端经理人。
    - 加入云端经理人之前，用户端邀请码可以更换。加入后不能更换。
    - 如果是旧的邀请码，延续旧的邀请策略。
    - 云端矿池邀请码，对购买foggie收益奖励同样有效。
  - 老用户加入
    - 对已存在的客户帐号支持绑定云端经理人，同理，根据输入云端经理人邀请码进行绑定
  - 账户销毁
    - 暂不支持
  - DMC账户对应：
    - 需要dmc账户。可以修改。修改DMC账户后，历史dmc账户信息保留。查询历史记录时，包含历史所有账户。
    - 修改账户收取DMC费用。1DMC 一次，首次不收费，1DMC直接打入官方账户。（防止用户频繁修改账户）
  - 对应关系：

        - 支持一个用户绑定一个云端经理人；
        - 一个云端经理人支持多个用户绑定。
    - 用户审批
        - 审批策略
            - 自动接收模式和手动批准模式，系统默认为自动接收模式

              如果是自动接收模式，客户加入云端经理人时，只要符合后台策略即可加入，客户加入状态自动更新为审批通过状态，如果设置手动批准模式，客户加入云端经理人时，处于待审批状态，当云端经理人批准后，状态更新为审批通过。
        - 用户权限管理：
            - 账户封锁：
                - 可以对指定的用户进行封锁和解封。封锁的账户不能买单、提现操作。
            - 黑白名单
                - ~~黑名单：对处于黑名单的用户帐号或者DMC帐号限制加入~~ （暂不支持，意义不大）；
                - 白名单：仅限白名单用户可以加入。
    - 用户信息查询：
        - 支持查看当前云端经理人绑定的用户信息，（包含不限于邮箱，DMC帐号等）
            - 当前资产信息（summary）
                - 收益总数。归档年/月/周收益
                - 订单信息：当前（订单笔数，PST数，质押总数） 累计数。
                - 纯利润：收益数据要扣除抽水的收益数据；
            - 详情：
                - 空间大小
                - 订单周期
                - 订单金额
                - 订单进度
                - 订单收益
                - merkle/挑战信息

3.2 经理人(管理员)平台

3.1.1 帐号管理

- 申请：
    - 批准经理人申请。
- 邀请码管理：
    - 生成邀请码（经理人使用的邀请码，1对1的。）。
    - 邀请码被使用后，标记已激活。可以看到邀请人的账户信息。快捷方式可以查看当前账户信息
- 账户信息

    - 汇总信息：
        - 大使账户总数，挂单总数；PST累计/当前总数；质押总数；当前账户余额总数；
        - 查看每个大使账户下的挂单总数，PST累计/当前总数，质押总数，当前账户余额总数。
    - 可以查看所有大使账户信息，资产信息，挂单数，质押数，成员等详细信息
    - 管理平台(Admin)可以对账户进行封锁账户，封锁转账等功能设置
- 激励管理
    - 可以根据奖励计划对经理人进行激励
    - 激励信息记录和归档展示
    - 奖励操作需要管理员平台向场内账户发起转账请求。
- 节点管理
    - 添加节点服务器信息
        - 超级管理员注册服务的server节点信息

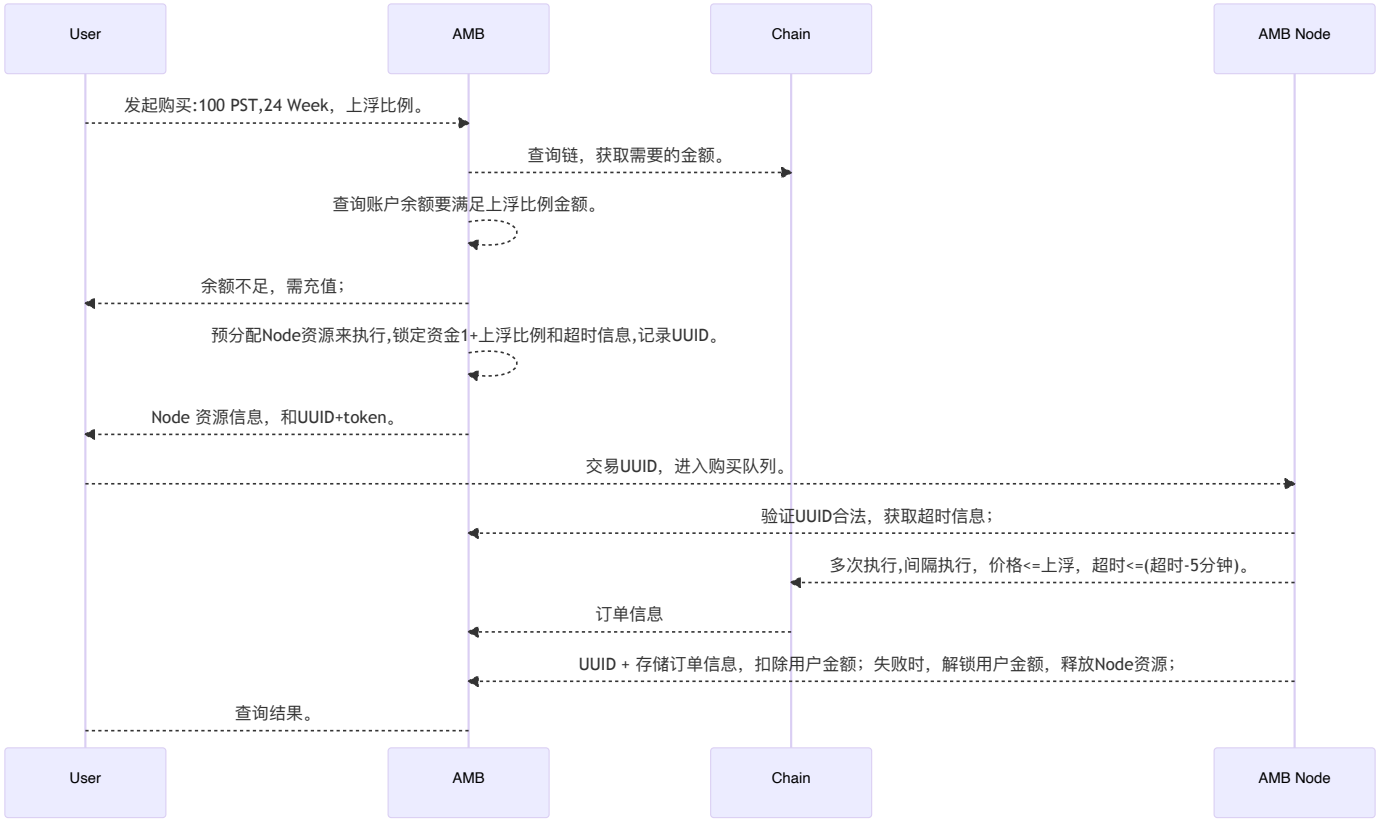
          （包含不限制于访问地址，名称，区域等）
        - 节点分配：
            - 超级管理员配置（支持修改）云端经理人server分配策略配置

              比如默认1:1，即每个加入的云端经理人默认分配一台server

              可以配置N；1或者1:N，即多个云端经理人共同分配一台server，或者一个云端经理人分配多个server

3.3 用户买单操作

3.3.1订单购买



【核心流程】

- 1.客户提交购买空间大小和周期，设置上浮比例。
- 2、发起购买订单请求。
- 3、云端经理人核查该用户购买DMC需要的金额是否满足当前价格的上浮比例。
- 4、如果满足，发起资源分配。告知客户。如果不足，需要用户充值。

- 5、用户发起购买请求购买；
- 6、Node 节点验证信息后，根据需求执行买单，买单执行结果反馈给AMB。
- 7、购买成功扣除费用。需要提供到用户购买的订单信息，交易ID及其他详细信息。
- 8、如果购买失败，需要释放资源。
- ***锁定金额不支持其它操作***；

说明：

购买订单设置异步任务，设置多种状态，支付中/购买成功/购买失败等；

校验用户账户的DMC不足以购买时，不支持购买订单

如Node节点挂掉，金额持续未解锁，大使可以人工解锁，以达到闭环。

购买订单时候：需要在memo中指定邀请码。***官方矿池会核对邀请码，才能达成共识。***

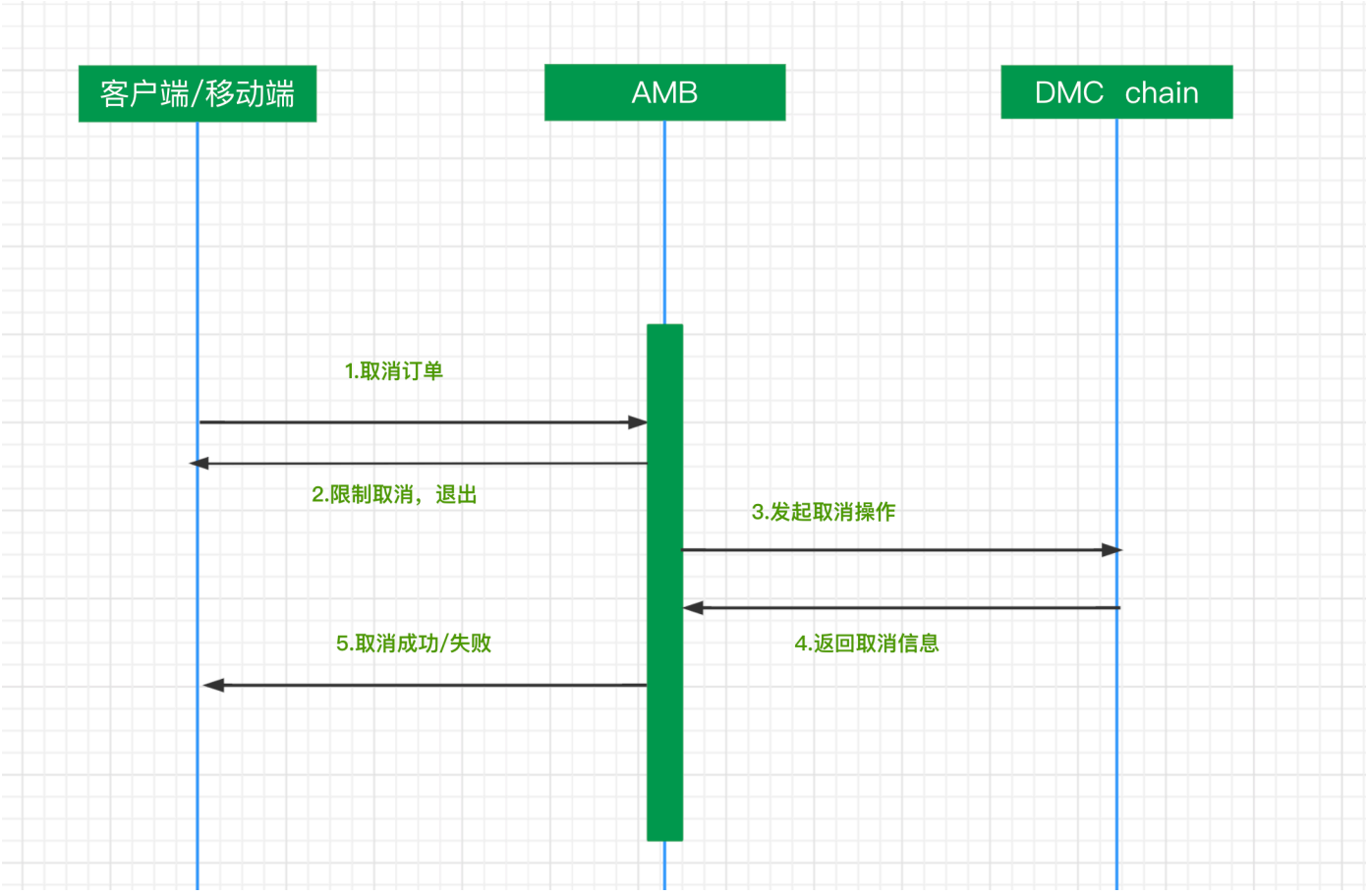
3.3.2订单管理查询

3.3.2.1查询订单信息

- 区分进行的订单和完成的订单
- 订单信息进行归档。
  - 完成的订单按照月份归档，比如7月xx单（xxpst/xxxdmc），点击后查询详细

3.3.2.2订单取消

- 可以取消用户订单（AMB操作细则参考买单）

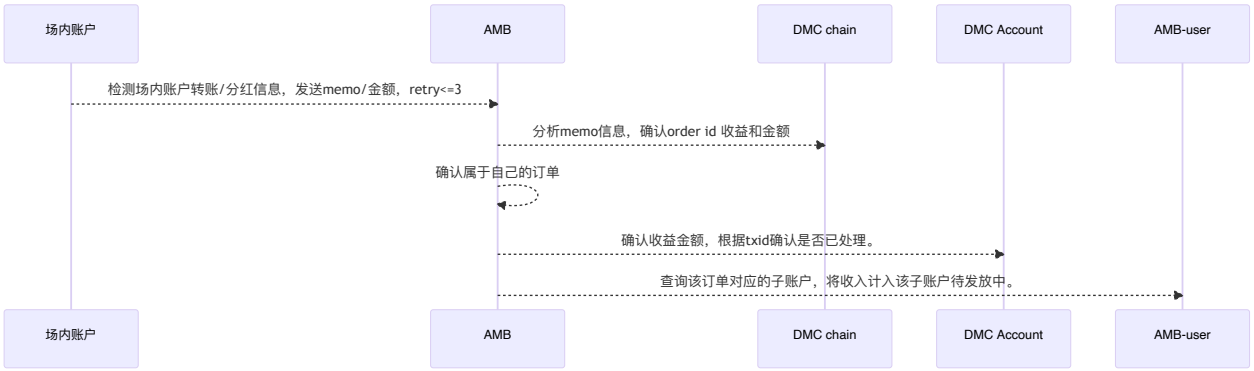


【核心流程】

- 1.客户发起取消操作；
- 2.云端经理人进行取消操作；
- 3.返回取消状态；
- 取消订单记录和金额纪录

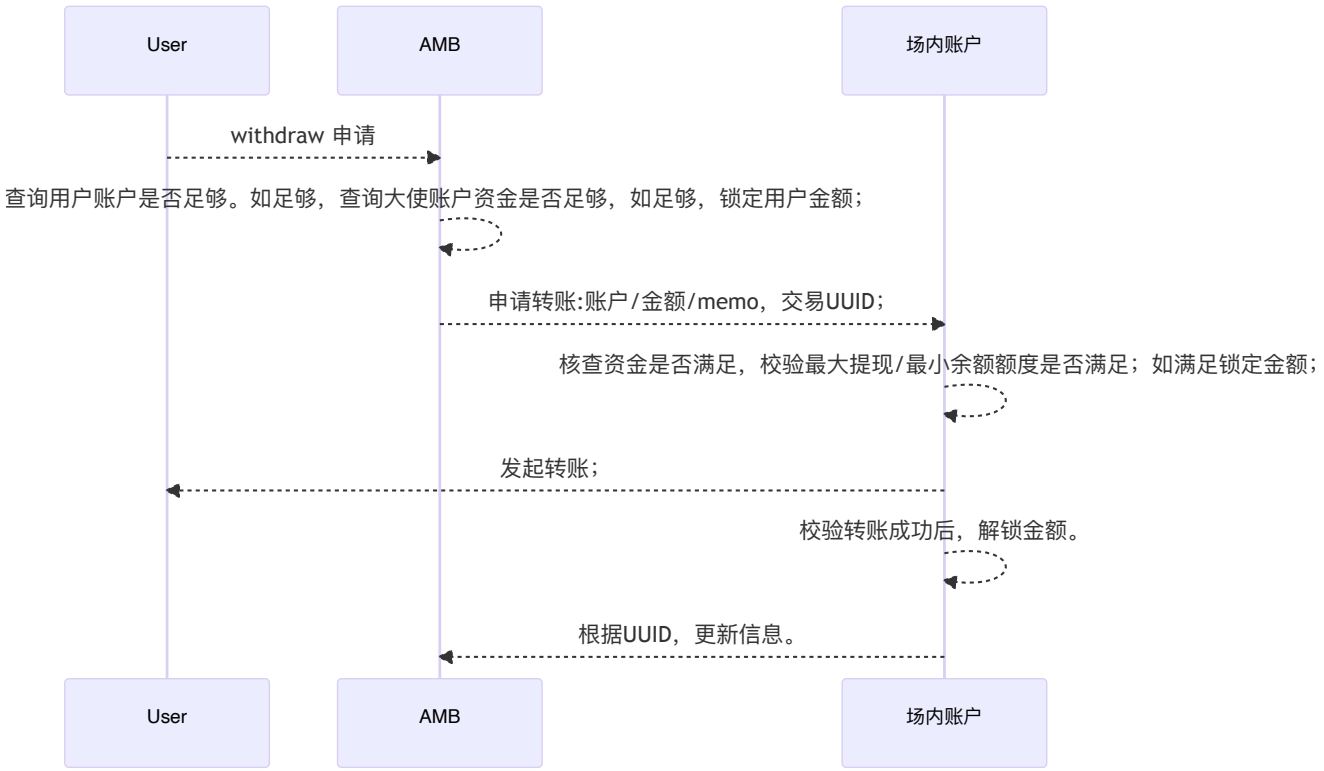
3.3.3资产管理

- 收益管理
  - 收益总数。以及归档年/月/周收益
  - 订单信息：当前（订单笔数，PST数，质押总数） 累计数
  - 纯利润：收益数据要扣除抽水的收益数据；
  - 设置抽水比例：
    - 抽水比例设置
  - 收益获取



  - 分红策略：
    - 收益展示：
      - 根据每个账户的收益信息，减去抽成数据后，展示给用户。
    - 自动分红： 根据每个账户的收益纯利润进行分配。
      - 从代发放账户中，自动将数据转给用户。

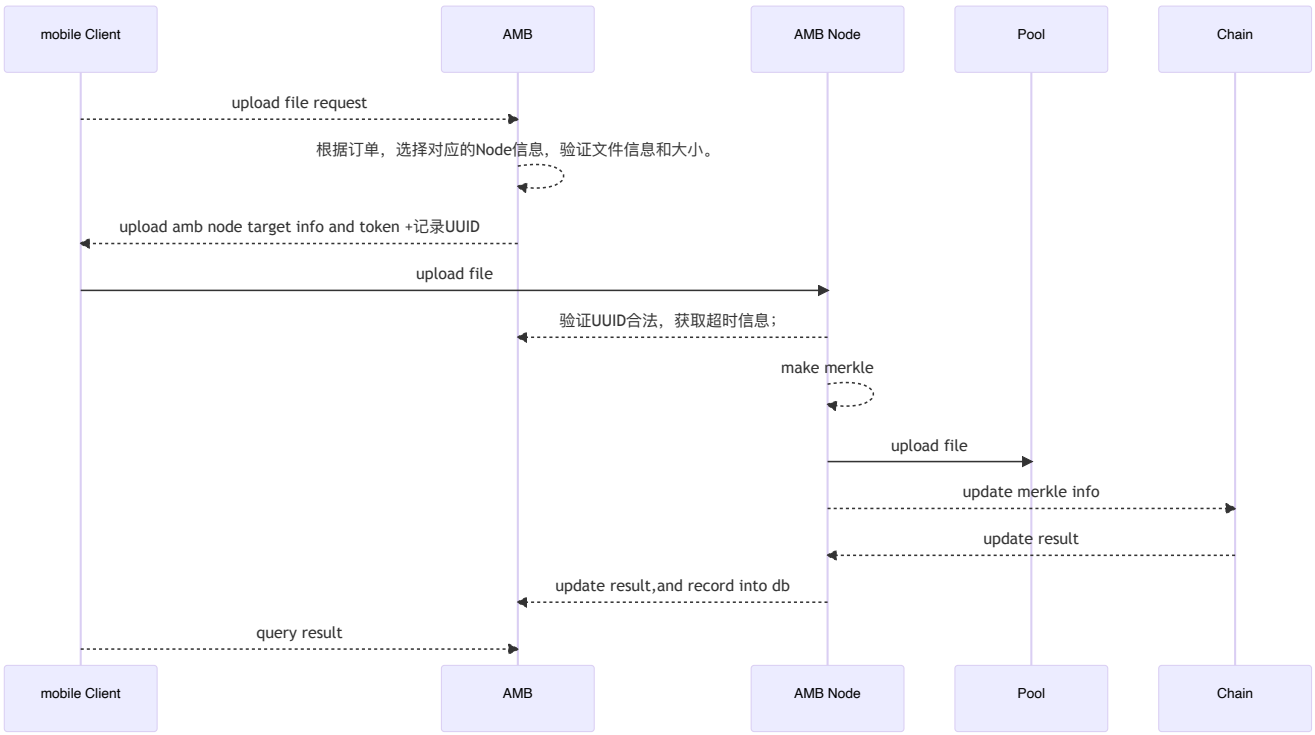
        - 手动分红：经理人可以给指定成员进行分配利润。
            - 从代发放账户中，将数据转给用户。
    - 抽水管理：
        - 抽水只在用户提现的时候进行抽水。
        - 用户请求提现，需扣除(经理人)大使的抽水额度后，进行提现。
        - 抽水数据记录经理人(大使)自己的内部账户上。
        - 用户端需要展示抽水比例。
    - 资产流动表
        - 收入：
            - 购买记录
            - 充值记录
            - 用户收益收益记录
            - 奖励记录
            - 用户抽水记录
        - 支出
            - 官方抽水记录
            - 提现记录
            - 分红发放记录
            - 收益发放激励
        - 归档： 按照年/月/周进行归档
    - 提现管理
        - 大使提现只能提现大使自己的内部账户（利润与返点）账户。
        - 提现需要有记录
        - AMB与场内账户通过Token认证
            - token 认证方式 :hash（获取轻权限时的密钥+金额+时间戳+目标账户）
        - 用户提现：ss
            - 用户只能提现自己内部账户的余额。（包括收益和分红）



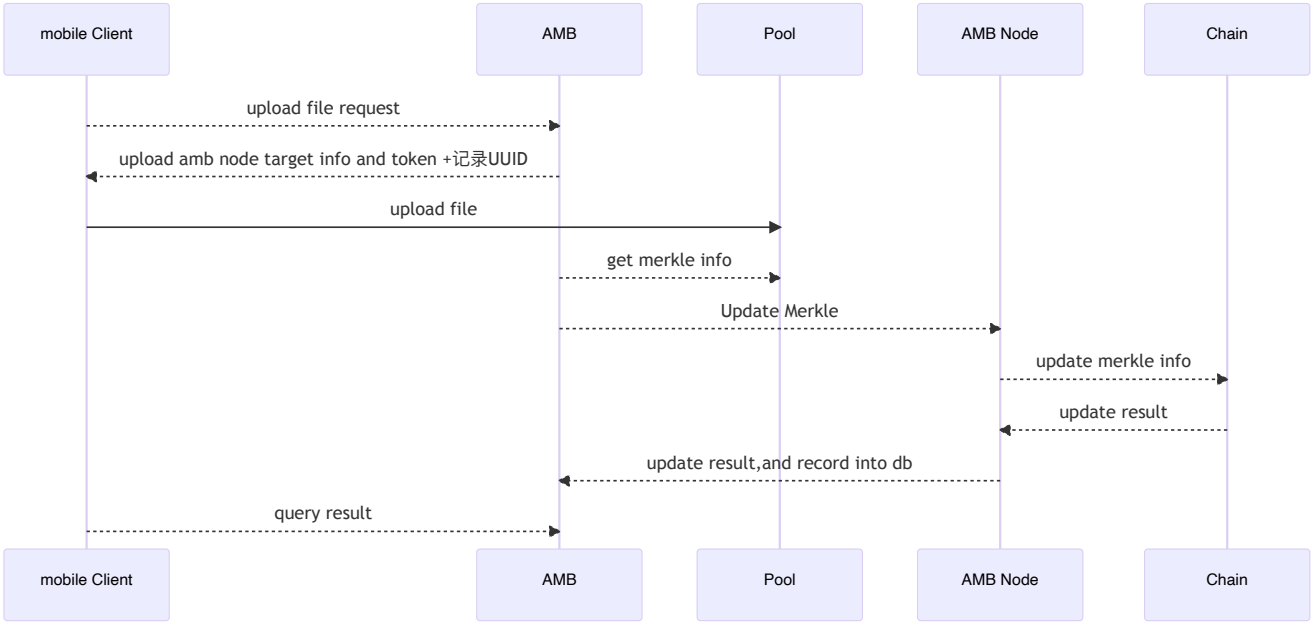
3.3.4数据管理

- 提交共识：
  - 当登录用户是桌面版本用户时，平台接收用户计算的merkle 数据，并进行提交
  - 当登录用户是移动端数据后，平台接收用户的数据，并计算merkle后提交。
- 查询merkle 信息
  - 客户端：具体订单提交过的merkle 数据
  - 云端经理人平台：支持查询绑定该经理人的用户提交过的merkle 数据
- 上传数据
  - 只有移动端数据经过Node（链服务上传）
  - node 节点需要记录：密码本数据、merkle db信息。
  - amb 需要存储共识记录

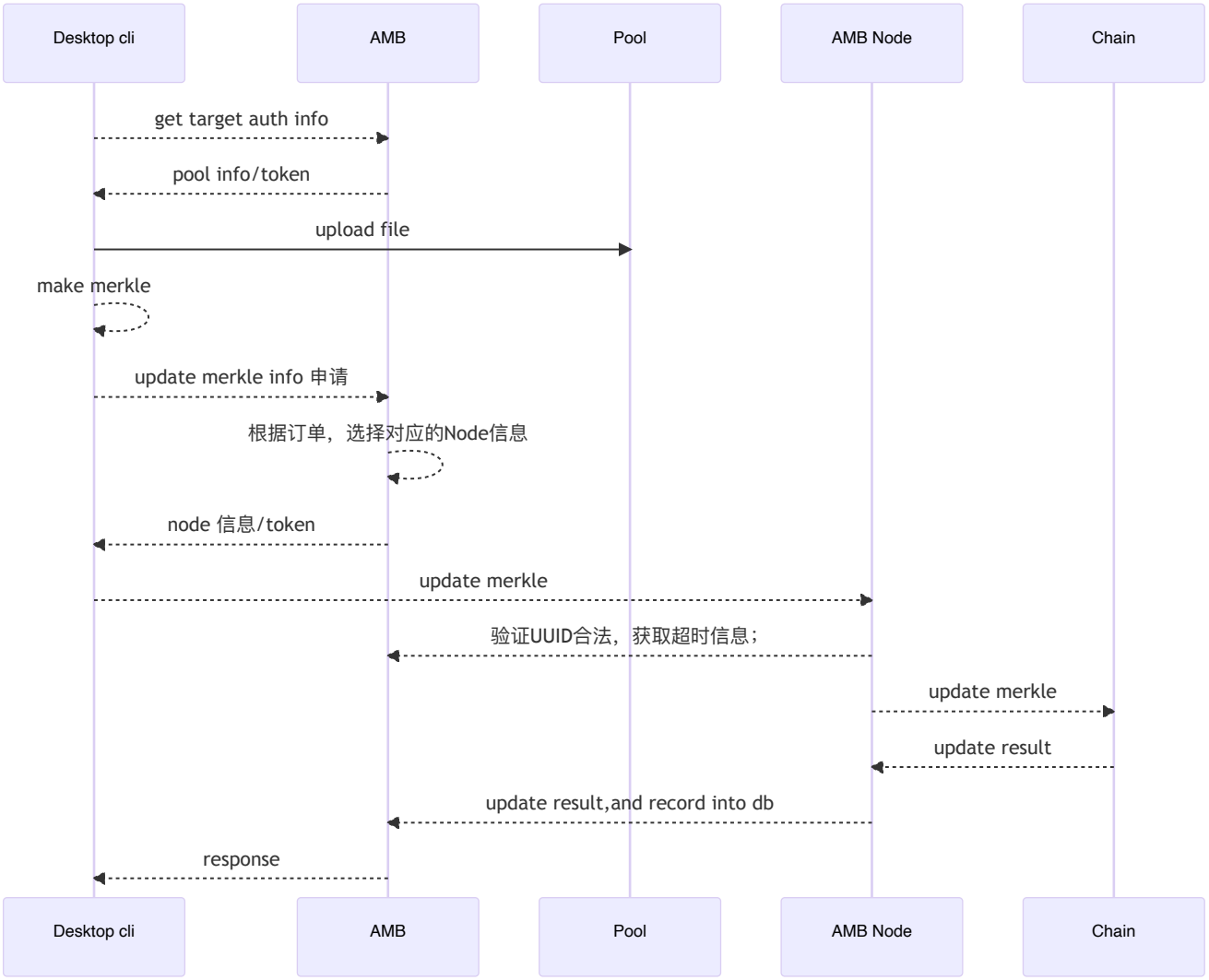
  移动端方案A


mobile Client
AMB
AMB Node
Pool
Chain
upload file request
根据订单，选择对应的Node信息，验证文件信息和大小。
upload amb node target info and token +记录UUID
upload file
验证UUID合法，获取超时信息；
make merkle
upload file
update merkle info
update result
update result,and record into db
query result
mobile Client
AMB
AMB Node
Pool
Chain

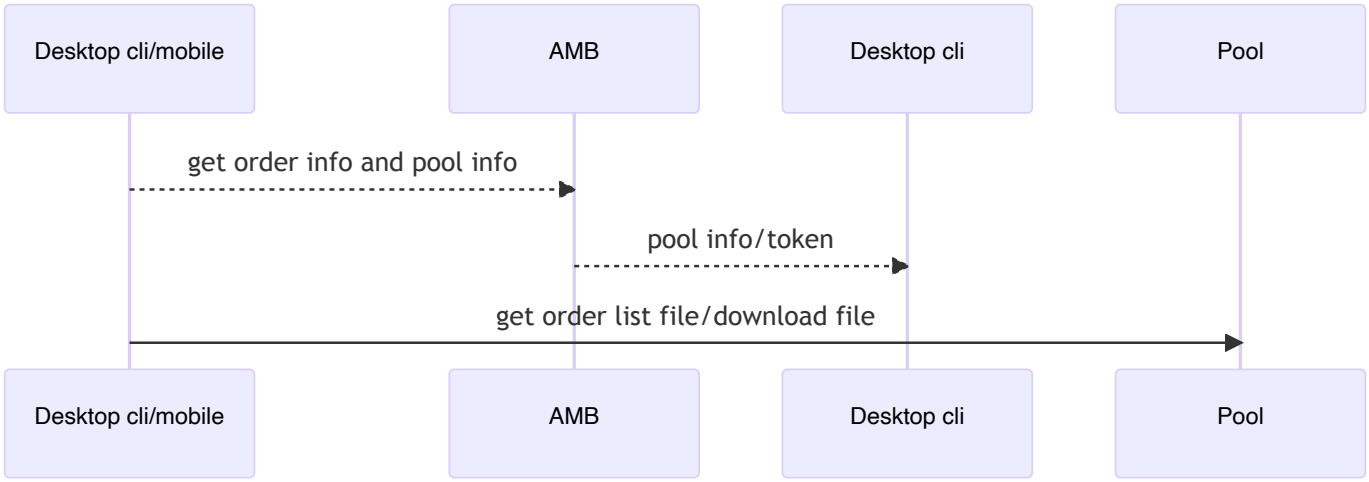
移动端方案B



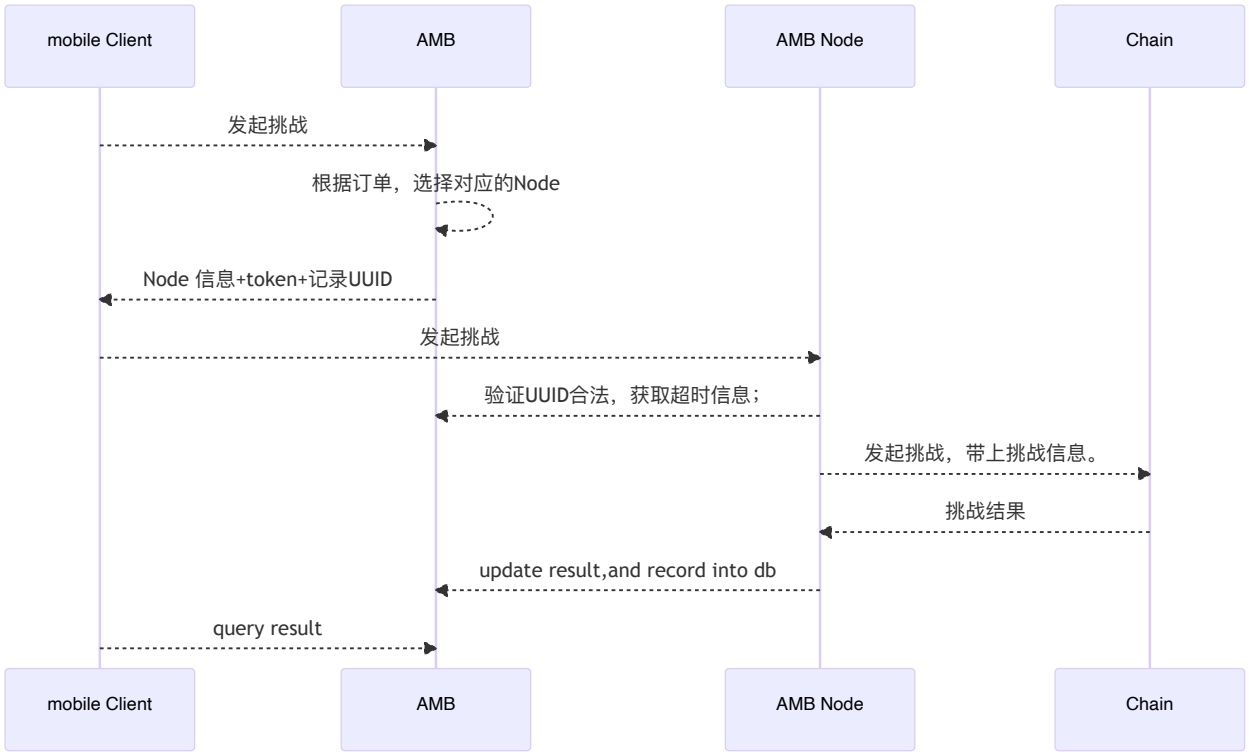
- 桌面版本客户端获取认证信息后，直接上传数据。


Desktop cli
AMB
Pool
AMB Node
Chain
get target auth info
pool info/token
upload file
make merkle
update merkle info 申请
根据订单，选择对应的Node信息
node 信息/token
update merkle
验证UUID合法，获取超时信息；
update merkle
update result
update result,and record into db
response
Desktop cli
AMB
Pool
AMB Node
Chain

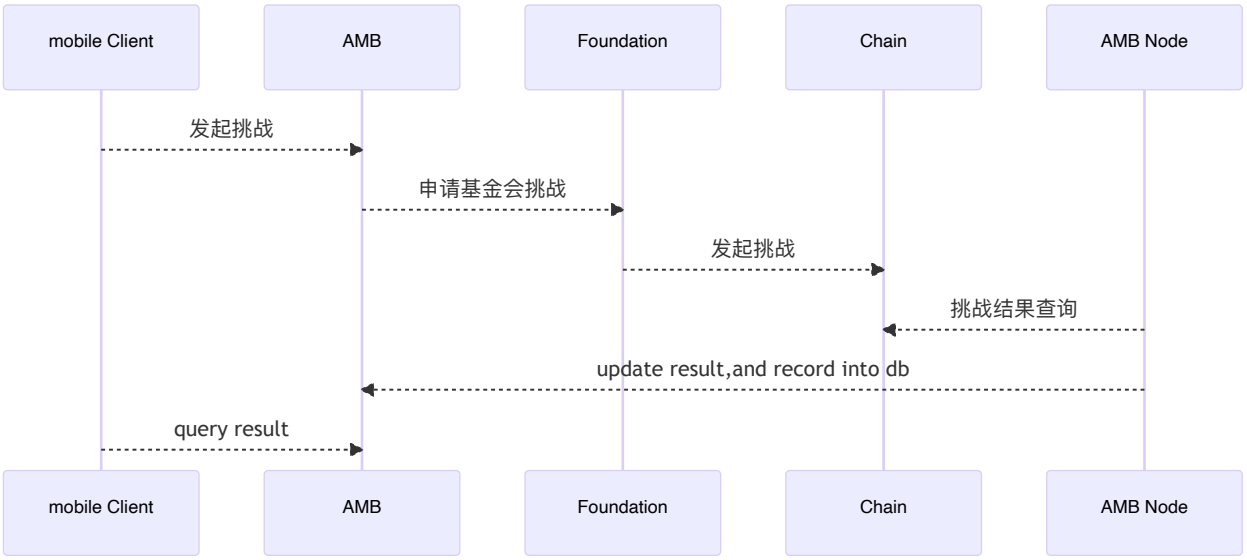
- 展示/下载



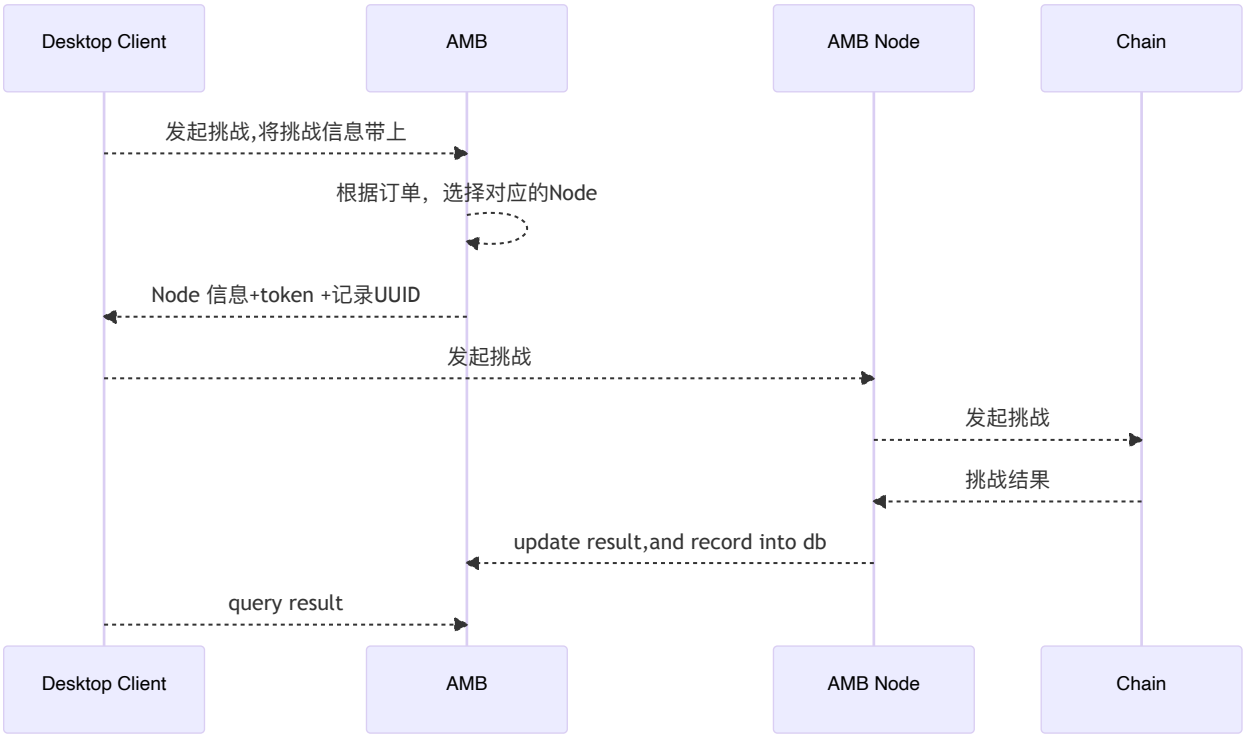
- 挑战
  - 移动用户挑战方案 A


mobile Client
AMB
AMB Node
Chain
发起挑战
根据订单，选择对应的Node
Node 信息+token+记录UUID
发起挑战
验证UUID合法，获取超时信息；
发起挑战，带上挑战信息。
挑战结果
update result,and record into db
query result
mobile Client
AMB
AMB Node
Chain

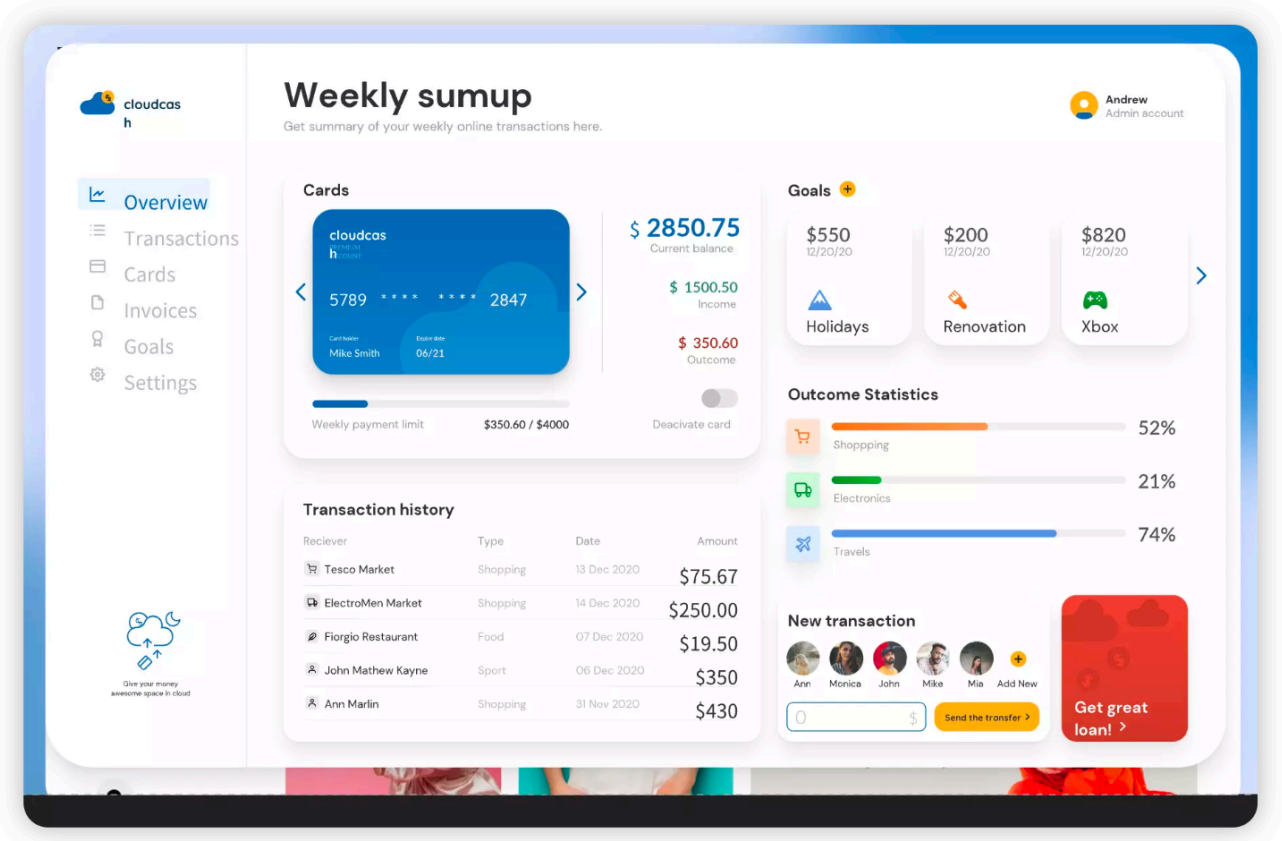
- 移动端发起挑战方案B


mobile Client
AMB
Foundation
Chain
AMB Node
发起挑战
申请基金会挑战
发起挑战
挑战结果查询
update result,and record into db
query result
mobile Client
AMB
Foundation
Chain
AMB Node

- 桌面版本发起挑战



3.3.5管理页面原型参考：



3.4 用户认证管理

- 用户统一认证。
- 设备管理中心和用户认证分开。
- FoggieV/Desktop/mobile 账户统一管理。
  - token分发记录登录设备信息（浏览器指纹）
  - redis 缓存存储信息。针对手机客户端/pc 浏览器设置不同的超时时间。

3.5 客户端

3.5.1 邀请码

- 注册支持邀请码注册；
- 绑定经理人需要dmc账户/邮箱。DMC账户可以修改。
- 已有用户购买云端矿池检测是否有邀请码，如果没有提示用户输入邀请码才能购买
- 客户端浏览器支持手机扫描注册，账户绑定操作。查看收益/订单信息（所有，分类，云端矿池第一优先）（含归档）（第一期）。
- 简化登录：钱包登录流程。

  用户可以通过dmc钱包进行登录和注册。当使用DMC钱包登录后，建议用户绑定邮箱和密码。
  - DMC 钱包验证流程：使用dmc钱包插件进行进行签名，将签名信息+钱包名称发给平台
  - 后台通过获取该钱包的公钥进行验签，成功后，用户可以登录。

    - 登录后，用户账户右上方提示黄色感叹号！建议邮箱绑定，便于找回账户和方便登录。
    - 使用邮箱注册的用户，可以使用绑定的钱包账户一键登录。
- 绑定钱包后的账户，显示红色感叹号！，你的DMC钱包不受安全保护，需要设置2FA！（即开启 google 验证码验证）

3.5.2 购买

- 新增云端矿池购买入口
- 购买订单优先筛选金牌矿池数据

3.5.3 收益

- 新增提现功能;
- 新增收益展示页面。含归档。具体收益信息参照经理人展示
- 订单信息展示。含归档。