Finchain(金融链)——技术简书（草案）

摘要

比特币作为第一个区块链的应用已经运行了 8 年，也创造了巨大的市值，但真正基于 btc 的商业落地应用少之又少；区块链要真正的商用，还需要解决以下问题，1.用户管理私钥的烦恼，2.交易确认和费用，3.用户隐私问题。金链将提出一些全新的理念来试图解决这些问题；下面将从技术的角度说明金链如何解决这些问题。

第一部分：主要解决的问题

1.用户管理私钥的烦恼

在区块链的世界里，极客拥有私钥就意味着控制自己的一切；但极客毕竟是少数，要想让区块链普惠大众，那么不得不面对的问题是：大量的普通用户是不会管理私钥的；丢失私钥就意味者丢失全部资产对于普通用户来说是不可接受的。

1.1 主控交易和自控交易

主控和传统账户一样，普通用户使用账户和密码登录，将自己的权益委托給商用实体，商用实体有权力更新区块链上用户地址的份额；用户也可以随时将权益转到自己控制的私钥的地址上来。为了保持去中心化属性，将引入多层签名机制。下面将简单介绍多层签名机制。

1.2 多层签名机制

用户使用用户名和密码生成种子 seed=Sha256(username||password),使用 PBKDF2 算法生成对称加密私钥 AES_P= PBKDF2(seed)k1。

服务器生成为每个用户生成一个随机数 R,并且保存密文 S=En（R）AES_P ，用户获得 R=De(S) AES_P，用户私钥 p= PBKDF2(PBKDF2(seed)k2||R)k3。

用户发送 v 数量 Token 到 to 地址，那么先计算出 H=sha256(v||to), 计算用户签名 Sig_u=Sign(H)p 并且构造数据 D = [to||value|| Sigu],将 D 发送到服务器。

服务器构造 Tx:{ ....., Data:D },使用主控私钥签名后广播到链上。

其中：

k_1：$2^{n1}+x_1$；

k_2：$2^{n2}+x_2$；

k_3：$2^{n3}+x_3$；

PBKDF2：[1]；

En（R）AES_P：用私钥 AES_P 对称加密原文 R；

De（S）AES_P：用私钥 AES_P 解密密文 S；

2.交易确认和费用以及隐私问题。

2.1 状态通道与闪电网络

经常发生交易的双方各自将一定量代币锁定到双方约定的合约里，而他们之间经常发生的交易都是链下签名确认，只有需要清算或者有争议的时候才把链

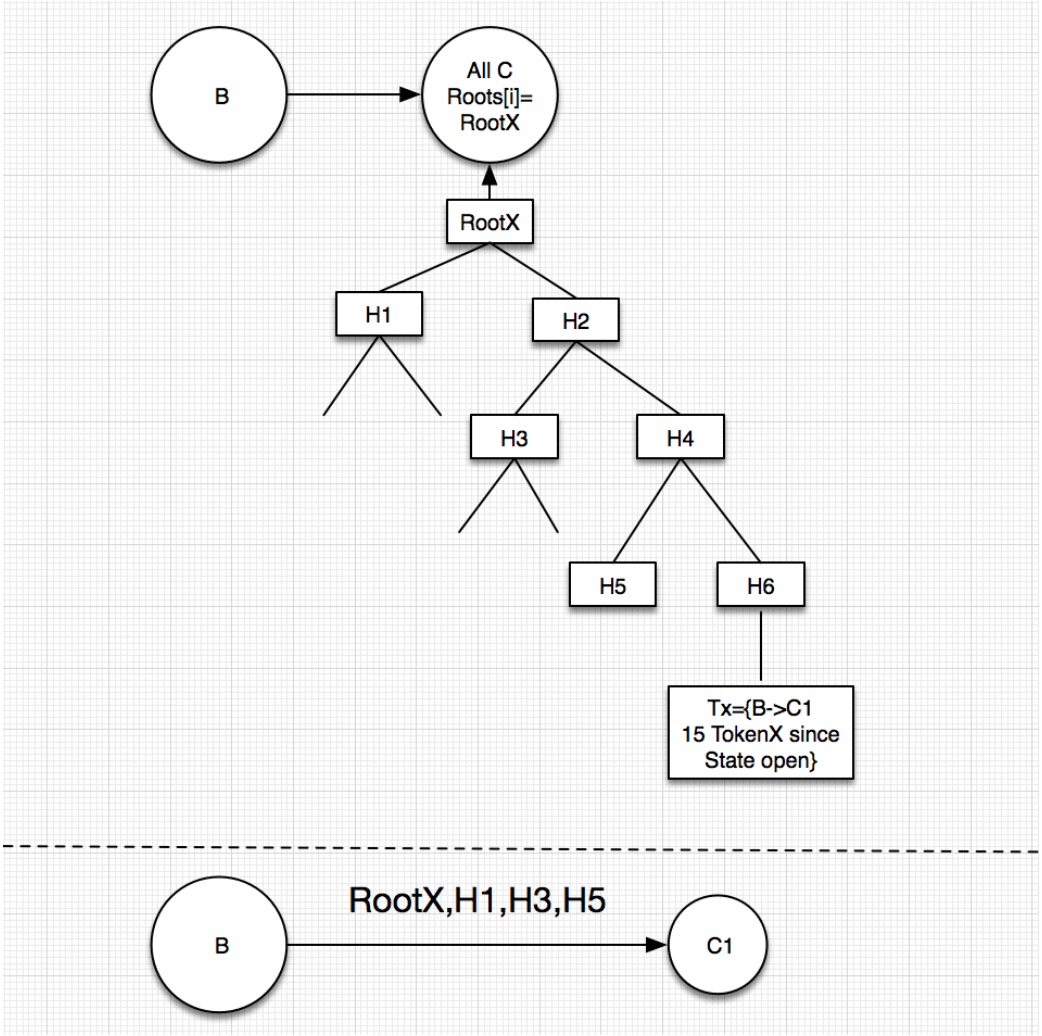
下签名广播的链上合约中关闭和清算；而由多个通道组成的网络就是闪电网络，一笔交易可以由多个通道串连完成。闪电网络让区块链交易变的低成本和高容量，但状态通道更适合于两个经常发生交易的机构间建立，而大量的商用应用，都是商户对大量普通用户，使用闪电网络就变的不那么有效；下面将介绍一种非常适合商业实体和用户之间的发生大量交易的网络协议。

2.2 状态证明

在状态通道中，商用实体必须和他的所有用户一一建立通道，商用实体需要锁定远远大于他所需支付的代币，否则频繁的清算和更新通道的开销往往会大于直接的链上交易；而在状态证明中商业实体和他的所有用户建立一个证明合约；这样只需要锁定所需支付的代币。商业实体向用户发送代币的时候，和状态通道一样只需链下签名交易即可。

2.2.1 延时证明

由于每个交易并没有放在链上，每个用户之间形成了信息孤岛，为了打破这个孤岛，商用实体需要提供状态证明。将所有交易最终状态的 Merkle Root 定时的更新到合约中。用户核对证明根 hash 和证明路径打破信息孤岛，证明自己的权益。



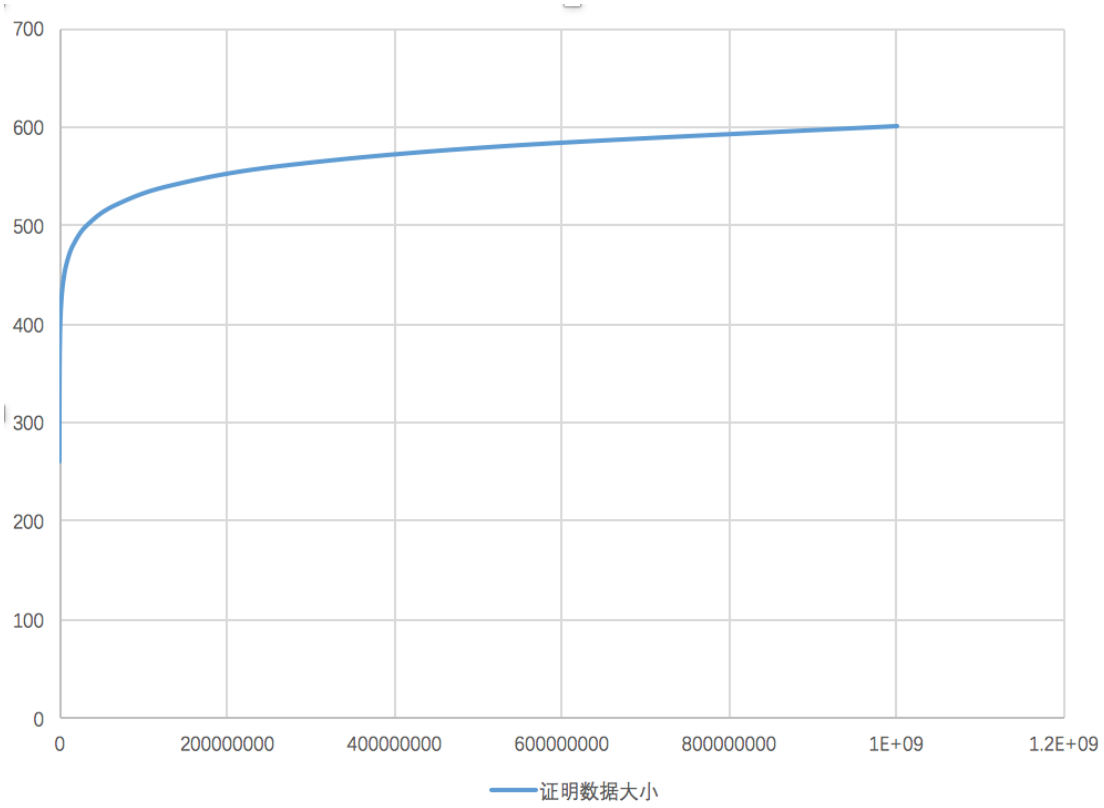
2.2.2 交易优先级

和状态通道一样，接受方只接受发送方权益递减的交易签名，任何发送方权益更少的交易又更高的优先级，哪怕低的交易 nonce。

2.2.3 树平衡和 Hash 压缩

一个大商用实体，会拥有千万甚至上亿用户，这样完全平衡的二叉树深度只会有 20 多级，考虑传输数据压力，使用 H160 代替 SHA256 来压缩 Hash 长度。下图为商业实体和用户间每笔链下交易的证明数据大小；可以看出在 10 亿

级别的用户的时候，链下证明数据的额外在 600B 左右；基本不增加链下网络压力。



第二部分：我们附带解决的问题

1.改进 DPOS 共识

Bitshares 是第一个引入 DPOS 共识的公链，后来的 steem 也采用来相同的共识算法，两个公链项目检验 DPOS 的高效，稳定和低延时。但在 DPOS 中出块代表不需要持有任何币，这无异增加了代表作恶的风险，再改进的 DPOS 共识每个代表的激活票数的最大值是他当前持有币数的 x 倍，

$$x = \frac{\sum_{i=1}^{n} vi}{\sum_{i=1}^{n} hi}$$

其中：

n:为预期活跃代表总数；

vi:获得投票前 i 个代表的票数；

hi:获得投票前 i 个代表持有的币总量；

2.改进的石墨烯引擎

石墨烯引擎采用 boost_mulit_index 将索引后的数据全部载入内存，这样保证了高效的撮合，但内存开销太大，现在完整的历史索引的节点需要几十 G 内存，普通的用户很难运行全节点验证节点，金链项目将重构石墨烯索引引擎，将时效性低的索引放入硬盘；大大减少内存开销。

3.签名抽象

基本上所有的虚拟货币都是使用 256 位 ECDSA 签名来保障安全，但如果两次 ECDSA 签名使用相同的随机数，私钥就会被泄漏；虽然客户端程序会避免这种情况出现，但无疑说明没有任何一种签名算法是绝对安全的；所以抽象的签名层无疑让金融链的安全性可以随时升级，将来量子计算机出现后也可以随时升级为抗量子的算法。

1、将支持的签名和加密算法。

secp256k1 曲线是 ECDSA 中经典和安全的曲线，也是绝大多数加密货币选用的曲线，所以金融链的加密和签名默认选择 secp256k1 曲线。

sm2是国家签名法指定的加密方式，所以金融链也支持sm2签名，曲线选用Fp256，而sm2使用的哈希算法将使用国密sm3。

2、金融链上的签名格式如下：

signature:{

```
        uint8 signType;
        uint8 v;
        uint256    r;
        uint256    s;
}
```

通过signType的不同值来标示签名算法类型。signType空间将可以支持最多256种算法。

［引用］

［1］: https://tools.ietf.org/html/rfc2898#section-5.2