Wormhole Cash

一种在Bitcoin Cash实现的智能合约解决方案

摘要

Bitcoin Cash在Bitcoin区块高度478558上分裂产生，一直致力于为世界带来一种可靠的现金，履行最初的比特币作为「点对点数字现金」的承诺。其具有全球无缝流通、无需许可的创新的特点。如果在Bitcoin发Token在很早的时候就染色币的方案Colored-Coins,之后Andrew Stone 提出了Enable representative tokens via OP_GROUP on Bitcoin Cash,该方案需要通过修改共识才可以实现。我们一直在探索一种不改变共识的情况实现在BCH上实现智能合约的方案，我们关注到了OmniLayer方案，他是一种利用op_return操作码实现发token的方案。
Wormhole Cash 是基于OmniLayer协议在BCH上实现发Token功能的一种解决方案。

术语

- `op_return` BCH中的操作码，包含这一指令的交易是不可花费的，节点可以安全地将其移除UTXO集合，可以用来存储220字节的数据
- `Wormhole Cash协议` 基于Omni协议实现的在BCH实现智能合约的协议规范
- `Wormhole Cash` Wormhole Cash协议中使用的基础货币 ， 简写WHC

原理

基于Bitcoin Cash网络实现，依附于Bitcoin Cash网络，在不改变现有共识的情况下，实现Token的发行，元数据信息写在OP_RETURN上。它的发行，转移，以及燃烧都需要通过Bitcoin Cash交易完成。识别OP_RETURN里的数据，完成对于Token的发行，转移和燃烧。
`Wormhole Cash协议`是Bitcoin Cash网络共识的一个超集，它识别的元数据识别在Bitcoin Cash中只是op_return的数据而已,Bitcoin Cash网络解析不了他的数据。而`Wormhole Cash协议`复用了Bitcoin Cash的交易转账系统，需要识别Bitcoin Cash网络中的交易，地址以及op_return等。

实现

`Wormhole Cash 协议`协议需要集成到Bitcoind中去，但是不会现有共识和协议做改变，需要运行Wormhole Cash的主节点才能识别出`Wormhole Cash 协议`。除了修改Bitcoind的实现之外，为了降低用户的使用成本还需要实现：

- 浏览器
- Web钱包
- 移动端钱包
- PC端钱包
- 冷钱包

为了方便其他人更加简单的在Wormhole Cash开发，还会提供解析`Wormhole Cash`的SDK。

安全

`Wormhole Cash`的安全又两层保护组成，第一层是Bitcoin Cash的交易安全，Bitcoin Cash采用POW的挖矿算法，该算法已经稳定运行将近10年，UTXO模型有以下的一些好处:

- UTXO无需维护余额
- UTXO是独立的数据记录单位，可以提升验证交易的速度
- UTXO模型无需关心事务问题，只关系锁定脚本和解锁脚本
- UTXO在处理交易的时候具有很高的性能

`Wormhole Cash`复用了整个Bitcoin Cash中UTXO的安全模型，用强大的算力保护。
第二层保护是运行`Wormhole Cash协议`的节点，不符合`Wormhole Cash协议`的数据无法写入运行`Wormhole Cash协议`的节点，每个节点都有能力通过重放交易数据，计算出`Wormhole Cash`的最终结果。

WormholeCash

WormholeCash(WHC)是WormholeCash协议中的基础货币，只所以引入WHC是因为，在实现智能合约的时候WormholeCash协议层不能控制Bitcoin Cash ，这样就无法在WormholeCash协议层中实现事务，而且在实现智能合约的时候需要引入Gas，也需要使用WHC做为Gas。

WHC的发行

WHC通过燃烧生成(proof of burn)，持有BCH的用户可以在WormholeCash上线之后，给bitcoincash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu08dsyxz98whc地址发送最低1个BCH在进行1000个块的确认之后就可以生成100个WHC。
bitcoincash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu08dsyxz98whc是一个没有人用户私钥的地址。生成WHC的条件必须满足：

- 发给地址 bitcoincash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu08dsyxz98whc
- 发送金额不小于1BCH
- 经过1000个块的确认

WHC发行后，用户在交易所可以购买到WHC

WHC的使用范围

Token的转账需要使用BCH的交易，BCH的交易中需要支持一定的BCH手续费，因此Token在转账的时候不需要使用WHC做为手续费，WHC的作用范围：

1. 创建Token需要收1WHC的手续费，该手续费也是采用直接燃烧的方式，创建Token需要消耗大量的节点防止WHC节点被恶意攻击，因此需要收取手续费
2. 大量地址转账，例如给所有拥有该Token的地址，都发送一定的Token，这样的操作需要遍历所有的地址，因此需要支付WHC做为手续费
3. 作为智能合约的Gas
4. 其他事务性操作

Token的发行

任何人都可以不受限制的在系统上创建TOKEN，除了支付正常的BCH交易手续费外，还需要支付一定数量的WHC（1 WHC，相当于0.01BCH）作为TOKEN的创建费用，该费用将会直接燃烧。
目前支持3种类型的TOKEN创建：

1. 固定token
    - 创建后，创建者立即自动拥有所有token
    - 不能增发，不能燃烧

- 不能发起众筹

2. 可众筹token

    - 创建后，自动进入众筹
    - 创建后，创建者不拥有所有token
    - 众筹结束后，未众筹完的token自动转到创建者地址

    - 不能增发，不能燃烧

    i. 可管理token
    ii. 创建时，token数量为0
    iii. 不能众筹
    iv. 可以增发，可以燃烧

Token的转移

创建后的TOKEN和WHC都可以进行转账，1对1转账除支付必要的BCH交易手续费外（由BCH网络决定手续费多少），不需要再支付任何费用；1对多转账需除支付必要的BCH交易手续费外（由BCH网络决定手续费多少），需要支付一定手续费（以WHC计价和收取），1对多转账主要在token空投的场景下使用；收取的WHC手续费将会直接燃烧掉。

Token的燃烧

手动管理的Token支持直接燃烧，燃烧之后的Token在WormholeCash协议中会显示燃烧之后的总量。

WormholeCash路线图

WormholeCash的发展分为四个阶段：Earth(初始)、Tropos(融合)、Ionize(电离)、Exophere(散逸)。

Earth(初始)

需要完成的工作:

- Wormhole Core 将Token功能移植到BitcoinABC 0.17.2版本上

- WHC的Web钱包
- WHC浏览器
- 发布WHC白皮书

Tropos(融合)

需要完成的工作:

- 基于WHC实现的去中心化交易所协议
- WHC的Android钱包
- WHC的IOS钱包
- WHC的PC端钱包

Ionize(电离)

需要完成的工作:

- 实现ERC721
- 开放WormholeCash多语言实现SDK
- WHC的冷钱包解决方案

Exophere(散逸)

需要完成的工作:

- 智能合约
- 基于WebAssembly的新一代智能合约虚拟机

总结

首先要感谢Omni团队，他们在Omni协议上所做的努力，让我们看到了基于Bitcoin Cash可以做的事情。在我们开发的过程Omni团队也给予了很多的帮助。智能合约的缺少一直是基于UTXO模型的公链的一大缺失，WormholeCash可以完全复用UTXO的安全可靠等特性，也可以实现智能合约，WormholeCash将会给Bitcoin Cash带来更多的可能性。

文档历史

1. Version 0.1 WormholeCash第一期完成的内容 2018-05-23
2. Version 0.2 WormholeCash路线图 2018-06-20
3. Version 0.3 WormholeCash alpha版本 2018-07-15