Wormhole Cash

一种基于Bitcoin Cash的智能合约实现方案

作者:姜家志，姜和平，温隆

摘要

Bitcoin Cash在区块高度478558上产生，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、无需许可创新等特点。在Bitcoin如何发Token在很早的时候就有过不少的研究，比如染色币的方案Colored-Coins，之后Andrew Stone 提出了Enable representative tokens via OP_GROUP on Bitcoin Cash，增加OP_GROUP的操作码来实现发Token的方案，该方案需要修改共识协议才可以实现。
我们也一直在探索一种在不改变共识的情况，基于Bitcoin Cash上实现智能合约的方案，经过研究各种Token实现的方案，我们关注到了OmniLayer协议，他是一种利用op_return操作码实现发Token的方案。
Wormhole Cash 就是基于OmniLayer协议，在BCH上实现智能合约的解决方案，当前会先实现Token的管理。

术语

- `op_return` Bitcoin Cash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Bitcoin Cash上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

Wormhole Cash是基于Bitcoin Cash网络实现的，依附于Bitcoin Cash网络的，在不改变现有共识的情况下，实现Token的发行，转移和燃烧等功能。
交易的元数据信息写在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里的数据才能够完成对于Token的发行，转移和燃烧。
`Wormhole Cash协议` 复用了Bitcoin Cash的交易转账系统，它需要识别Bitcoin Cash网络中的交易，地址以及op_return等数据。
`Wormhole Cash协议` 是Bitcoin Cash网络共识的一个超集，它识别的元数据在Bitcoin Cash协议中只是op_return数据，Bitcoin Cash网络解析不了他的数据。

实现

`Wormhole Cash 协议` 协议需要集成到Bitcoind中，但是不会对现有共识和协议做改变，只需要运行Wormhole Cash的节点就能够识别出 `Wormhole Cash 协议` 即可。
除了修改Bitcoin ABC的客户端实现之外，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

为了方便开发者更加简单的在Wormhole Cash进行开发，未来还会提供解析 `Wormhole Cash` 的多语言SDK。

安全

`Wormhole Cash` 的安全有两层保护。
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，使用了Bitcoin Cash的交易安全模型。

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`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`的最近的最终状态。

WormholeCash

WormholeCash(WHC)是WormholeCash协议中的基础货币，只所以引入WHC是因为：在`WormholeCash协议`中实现智能合约的时候`WormholeCash协议层`是不能控制Bitcoin Cash的，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，也需要使用基础货币做为gas。

WHC的发行

WHC通过燃烧生成(proof of burn)生成，持有BCH的用户可以在WormholeCash协议上线之后，给bitcoincash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu08dsyxz98whc 地址发送最低1个BCH，在1000个块确认之后就可以生成100个WHC。汇率是1bch=100whc，
bitcoincash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu08dsyxz98whc该地址是没有人拥有私钥的。
生成WHC的条件必须满足：

- 发给地址bitcoincash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu08dsyxz98whc
- 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的转账使用的是Bitcoin Cash交易，Bitcoin Cash交易中需要支付一定的手续费，因此Token在转账的时候不需要使用WHC做为手续费。
WHC的使用范围：

1. 创建Token需要收1WHC的手续费，手续费会被直接燃烧掉，创建Token需要消耗计算资源，为了防止Wormhole Cash节点被恶意攻击，才收取WHC手续费的

2. 大量地址转账，例如给所有拥有该Token的地址都发送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. 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Bitcoin Cash交易手续费外，还需要支付一定数量的WHC（1WHC，相当于0.01BCH）作为Token的创建费用，该费用将会直接燃烧掉。
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WromholeCash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,不需要再支付任何费用,由BCH网络决定手续费多少
1对多转账需除支付必要的BCH交易手续费外，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实现：将Token功能移植到Bitcoin ABC 0.17.2版本上,后续会随着Bitcoin ABC的更新而更新
- Wormhole Cash的Web钱包
- Wormhole Cash浏览器
- 发布Wormhole Cash白皮书

Tropos(融合)

需要完成的工作:

- 基于Wormhole Cash协议实现的去中心化交易所协议
- Wormhole Cash的Android钱包
- Wormhole Cash的ios钱包
- Wormhole Cash的PC端钱包

Ionize(电离)

需要完成的工作:

- 在Wormhole Cash协议中实现ERC721
- 开发Wormhole Cash多语言实现SDK
- Wormhole Cash的冷钱包解决方案

Exophere(散逸)

需要完成的工作:

- 智能合约
- 新一代的智能合约虚拟机

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可以做到更多的事情，Omni协议是一套非常完整的协议实现，它完全利用了现有Bitcoin协议的特点，在不更改共识和协议的情况实现Token的管理。在我们开发的过程Omni团队也给予了很多的帮助。
智能合约的缺失一直是基于UTXO模型的公链的一大缺点，WormholeCash可以完全复用UTXO的安全可靠等特性的情况下，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

参考文献

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf,Oct 2008.
[2] OP_RETURN https://en.bitcoin.it/wiki/OP_RETURN
[3] OmniLayer https://github.com/OmniLayer/spec
[4] ERC20 Token Standard https://theethereum.wiki/w/index.php/ERC20_Token_Standard
[5] The Colored Coins Protocol https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki
[6] Andrew Stone : Enable representative tokens via OP_GROUP on Bitcoin Cash https://github.com/BitcoinUnlimited/BUIP/blob/master/077.mediawiki
[7] ERC-721 http://erc721.org/