Wormhole: 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（BCH）在区块高度478,558上产生，一直致力于为世界带来一种可靠的电子现金，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、无许可（Permissionless)创新等特点。在Bitcoin Cash如何实现发行通证（Token），众多的开发者已经有过不少的研究，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，提议增加OP_GROUP的操作码来实现发Token的方案。OP_GROUP方案需要修改Bitcoin Cash的共识规则才可以实现。更具体地说，类似于在Ethereum网络上广受欢迎的ERC20协议所具备的那些功能。

凡是需要更改共识才能实现的通证发行技术提议，都不可避免地会遇到问题。首先是技术上的风险，其次是对这种风险的顾虑常常引发技术开发社区甚至整个经济生态都陷入巨大的争议。争议中的反对方，其顾虑很可能也确实是真实的。不论这样的争议中谁对谁错，结果常常是有争议的提议无法被实现。这样的困难可以被视为一种保险机制，让具有的风险更改很难被添加到协议之中，保证协议的稳健与安全；但是，协议的创新就面临了着巨大的困难。导致了Bitcoin Cash社区独立的区块扩容大争论，旷日持久而没有共识的产生，就是一个更加令人不能回避的社会心理学证据。

快速活跃的创新，需要一种无需许可的环境。我们也一直在探索无许可创新的方法，在不需要改变共识的情况下，在Bitcoin Cash的区块链上实现智能合约。经过研究，我们关注到了OmniLayer协议，它是一种利用OP_RETURN操作码实现通证发行的方案。这个方案是广受欢迎的泰达币（USDT）日常发行和流通的技术基础。Omni Layer是运行在Bitcoin的区块链之上的。Omni Layer协议采用了MIT开源许可证。我们Fork了Omni Layer的协议，在Bitcoin Cash的区块链上实现了发行通证的技术方案。我们将这种技术方案命名为Wormhole协议，协议中的原生代币命名为Wormhole Cash。

术语

- `OP_RETURN` Bitcoin Cash中的操作码之一，包含这一指令的交易输出是不可花费（Unspendable)的，节点可以安全地将其移出UTXO集合，从而不会影响UTXO集合的总体积。在2018年5月最新的BCH协议升级之后，可以用来存储220字节的元数据。
- `Wormhole协议` 基于Omni Layer协议实现的，在Bitcoin Cash区块链上实现智能合约的协议规范
- `wormhole cash` Wormhole协议中使用的基础货币，简写"WHC"。

原理

Wormhole Cash是基于Bitcoin Cash区块链实现的，依附于Bitcoin Cash区块链，在不改变现有BCH共识规则的情况下，使得BCH区块链实现通证的发行、转移和燃烧等基本功能。

交易的元数据信息被写在OP_RETURN上。基于Wormhole协议的通证，其生成、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协议`复用了Bitcoin Cash的交易转账系统，它需要识别Bitcoin Cash区块链上的交易、地址以及OP_RETURN等数据。

`Wormhole协议`是Bitcoin Cash网络共识的一个超集，它识别的元数据在Bitcoin Cash区块链的共识协议中只是OP_RETURN数据，而Bitcoin Cash的共识规则不用理解OP_RETURN内的数据。

实现

`Wormhole协议`协议的实现，是通过集成到Bitcoind中实现的。但是Bitcoin Cash本身的共识规则却不需要做出改变，集成了Wormhole协议的Bitcoind客户端，被称之为Wormhole客户端。运行Wormhole客户端的节点就能够识别出OP_RETURN`Wormhole协议`。

安全和共识规则

`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的挖矿算法作为去中心化的时间戳服务器，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协议`复用了整个Bitcoin Cash中UTXO的安全模型，使用了Bitcoin Cash的去中心化时间戳服务器模型。

第二层保护是运行`Wormhole协议`的节点，不符合`Wormhole协议`的数据不会被`Wormhole协议`的节点解析，每个节点都有能力通过重新解析交易数据，计算出`Wormhole Cash`的最近的合法最终状态。

Wormhole Cash（WHC）

Wormhole Cash(WHC)是Wormhole协议中的基础货币，只所以引入WHC是因为：在`Wormhole协议`中实现智能合约的时候`Wormhole协议层`是不能控制Bitcoin Cash的，这样就无法在Wormhole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作为针对网络滥用的防护措施，也需要Wormhole协议存在一种原生基础货币。

WHC的生成

WHC通过燃烧生成(Proof-of-Burn)的机制生成出来的，持有BCH的用户可以在Wormhole协议正式上线之后，给bitcoincash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqu08dsyxz98whc 地址发送最低1个BCH来生成WHC。如果发送的BCH数量低于1BCH，那么将不会有任何的WHC被生成。这个燃烧生成的过程受制于BCH区块链发生回滚的风险，出于安全考虑，协议约定需要在1,000个确认之后，才可以动用生成的WHC。燃烧生成的兑换比例是，每1BCH的燃烧生成100WHC。

根据已知的密码学理论和工程实践经验，bitcoincash:qqqqqqqqqqqqqqqqqqqqqqqqqqqqqu08dsyxz98whc地址是没有人拥有私钥的。在我们开始有关Wormhole协议的开发工作之前，也没有人在Bitcoin Cash区块链的历史中使用过该地址。为了防范理论上存在的极端情况——未来有一种我们目前未知的方法和理论构建出了这个地址的私钥——BCH协

议可以考虑禁止这个地址的币被转出用于花费。当然，这并不属于本文和本文作者需要关注的事项范围。

WHC发行后，如果WHC形成了一个流通市场，那么有需要WHC的用户，也可以从市场上购买到WHC。

为什么没有考虑实现与BCH的双向锚定呢？这个问题自从侧链理论被提出后，无数的工程师醉心于双向锚定问题的研究。但令人遗憾的是，目前并没有可行的双向锚定方法， 可以做到即安全又去中心化，还能够有效应对区块链不可避免的回滚风险。伊隆·马斯克（Elon Musk）在讨论有关星际旅行时就说，他移民去往火星，就打算待在那里不回来了。Wormhole协议实现了智能合约，具有与Bitcoin Cash较为不同的编程语言，未来还有快速演进的开发计划。这种燃烧生成的发行方式，与星际旅行的单程票非常相似。每一聪（satoshi）被燃烧的BCH，都需要做好单程星际航行的准备，前往Wormhole定居，不再回来。

燃烧生成WHC的过程是不设截止时间点的。

WHC的使用范围

手续费常常是为了防止对网络的滥用，或者网络的使用超过了当前技术和区块链基础设施允许的性能瓶颈。Wormhole协议中，智能合约的运行，依靠Bitcoin Cash交易实现。Bitcoin Cash交易本身需要支付一定的手续费，已经可以阻遏DoS攻击，因此我们在早期运行的Wormhole协议中，转账不需要支付WHC做为手续费。

需要支付WHC作为手续费的情况：

1. 新创建Token需要收1WHC的手续费。手续费会被直接燃烧掉，WHC的总供给减少。创建Token需要消耗计算资源，为了防止Wormhole节点被恶意攻击，才收取WHC手续费
2. 大量地址转账。例如给所有拥有某种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，或者其他被认定为具有DoS风险的操作类型。

Token的发行

支付了正常的BCH交易手续费和WHC创建费用之后，任何人都可以自由的在系统上创建Token。

目前，WHC协议支持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Wormhole Cash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协议决定手续费多少。

1对多转账需除支付必要的BCH交易手续费外，还需要支付一定的WHC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Wormhole协议中会显示燃烧之后的总量

Wormhole路线图

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

Earth(初始)

Wormhole协议从Omni Layer协议分离，并在BCH上实现智能合约的解决方案，首先聚焦于去中心化通证发行管理功能的实现。

为了确保整个协议的安全，并且可以尽快上线，我们在这个阶段暂时不支持了Omni Layer协议中的去中心化交易功能。

Earth阶段需要完成的工作:

- 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
- 发布Wormhole协议白皮书

预计完成时间2018年8月

Tropos(融合)

需要完成的工作:

- 基于Wormhole协议实现的去中心化交易所协议在经过谨慎的测试之后重新上线
- Wormhole的Android钱包参考实现
- Wormhole的iOS钱包参考实现
- Wormhole的PC端钱包参考实现

预计完成时间2018年11月

Ionize(电离)

需要完成的工作:

- 在Wormhole协议中实现ERC721
- 开发Wormhole多语言实现SDK。为了方便开发者更加简单的在Wormhole进行开发，我们会提供解析`Wormhole`的多语言SDK。
- Wormhole Cash的冷钱包解决方案

预计完成时间2019年1月

Exophere(散逸)

需要完成的工作:

- 无需许可的智能合约。Omni Layer本身不是一种无许可创新的机制。任何新型的合约类型，都必须被合并到程序代码之中才能够被识别。我们会在Exophere阶段，实现无许可的智能合约平台。也就是说，在遵守维护协议安全的必要规则后，任何开发者都可以发布智能合约到网络中运行。
- 实现Plasma协议，实现扩容。我们在内部研究中，可能已经发现了一种有效的Plasma实现方法，我们在进一步研究之后将可能将其实施。与此同时，Vitalik也在Twitter上宣布他们发现了一种Plasma的实现方法，我们届时也可以考虑采用Vitalik即将发布的实现方法。
- 新一代的智能合约虚拟机。Solidity作为将智能合约这一古老概念变为实现的编程语言，受到了计算机专家的广泛审视。近些年也有更好的想法被提出来。我们将考虑开发一些新型编程语言的虚拟机，让最有效率、开发者基础最广泛的计算机语言被用于构建DApps。

预计完成时间2019年6月

总结

首先要感谢Omni Layer，他们在USDT上的广泛应用，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UTXO模型的特点，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。同时，Omni Layer也秉承了开源运动的精神，采用了MIT许可证，是我们可以实现无许可创新的重要基础。
智能合约的缺失一直是基于UTXO模型的公链的一大弱点，Wormhole协议可以在完全复用UTXO的安全可靠等特性的情况下，也可以实现智能合约，Wormhole协议将会给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/