全球区块链生态技术大会

Global Blockchain Eco-Technology Conference

虫洞协议的设计与实现

姜家志

主办方 Geekbang 极客邦科技 InfoQ

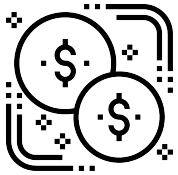
区块链前哨
BLOCKCHAIN OUTPOST

正本清源，打造链圈第一技术公众号

掌握前沿区块链资讯
深度分析区块链技术
致力于区块链技术普及

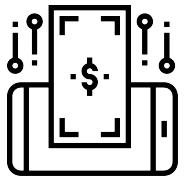
扫码关注区块链前哨

Wormhole



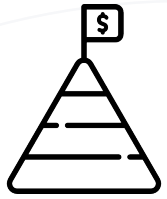
BCH

- 让更多的人有能力远离通货膨胀
- 全球无缝流通
- 低手续费
- 快速确认
- 数学保护的财富



ERC20

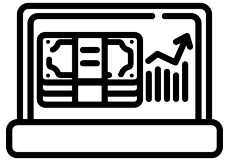
- ICO
- 一套标准接口
- 钱包自动支持代币
- 把ETH打到对应的合约地址上，自动获得代币



CryptoKitties

- ERC721 Token
- 每一只猫都是一种代币
- 每一只猫都是独一无二的
- 每一只猫都有自己的基因
- 最高的一只的价格高达13亿

更改共识



- 技术上的风险
- 对于这种风险而产生的顾虑
- 整个社区引起巨大的争议
- 快速活跃的创新，实现智能合约

虫洞协议?

Wormhole Protocol

- 基于BCH，在不改变基础协议的情况下，可做货币发行
- 所有工作都通过BCH交易
- 为BCH的一个超集，比特币网络解析不了它的协议
- 协议的实现在OP_RETURN上
- 基于OP_RETURN进行解析，完成Token的发行，转移和燃烧
- 它集成到了Bitcoin-ABC里面，不会对BCH协议和共识进行改变

原理

BCH提供去中心化时间戳服务

OP_RETURN数据的解析

运行节点形成共识

概念

- OP_RETURN

- Wormhole 协议

- Wormhole Cash

OP_RETURN

- BCH操作码之一，包含这一指令的交易输出是不可花费的（Unspendable），节点可安全将其移出UTXO集合，从而不会影响UTXO集合的总体积。
- 可用来存储220字节的元数据。

基础货币WHC

1个BCH=100个WHC

燃烧地址
qqqqqqqqqqqqqqqqqqqqq
qqqqqqqu08dsyxz98whc

当前有2300多个
BCH参与燃烧

携带燃烧信息

1000个块确认

WHC的使用范围

早期运行的Wormhole协议中，转账无需支付WHC作为手续费，需要支付WHC作为手续费的情况如下：

新创建Token

需收取1WHC的手续费，手续费被直接燃烧掉，WHC总供给减少。

原因——创建Token需消耗计算资源，为防止Wormhole节点被恶意攻击

大量地址转账

如给所有拥有某种Token的地址都发送Token，该操作需遍历所有的地址，故需支付WHC作为手续费

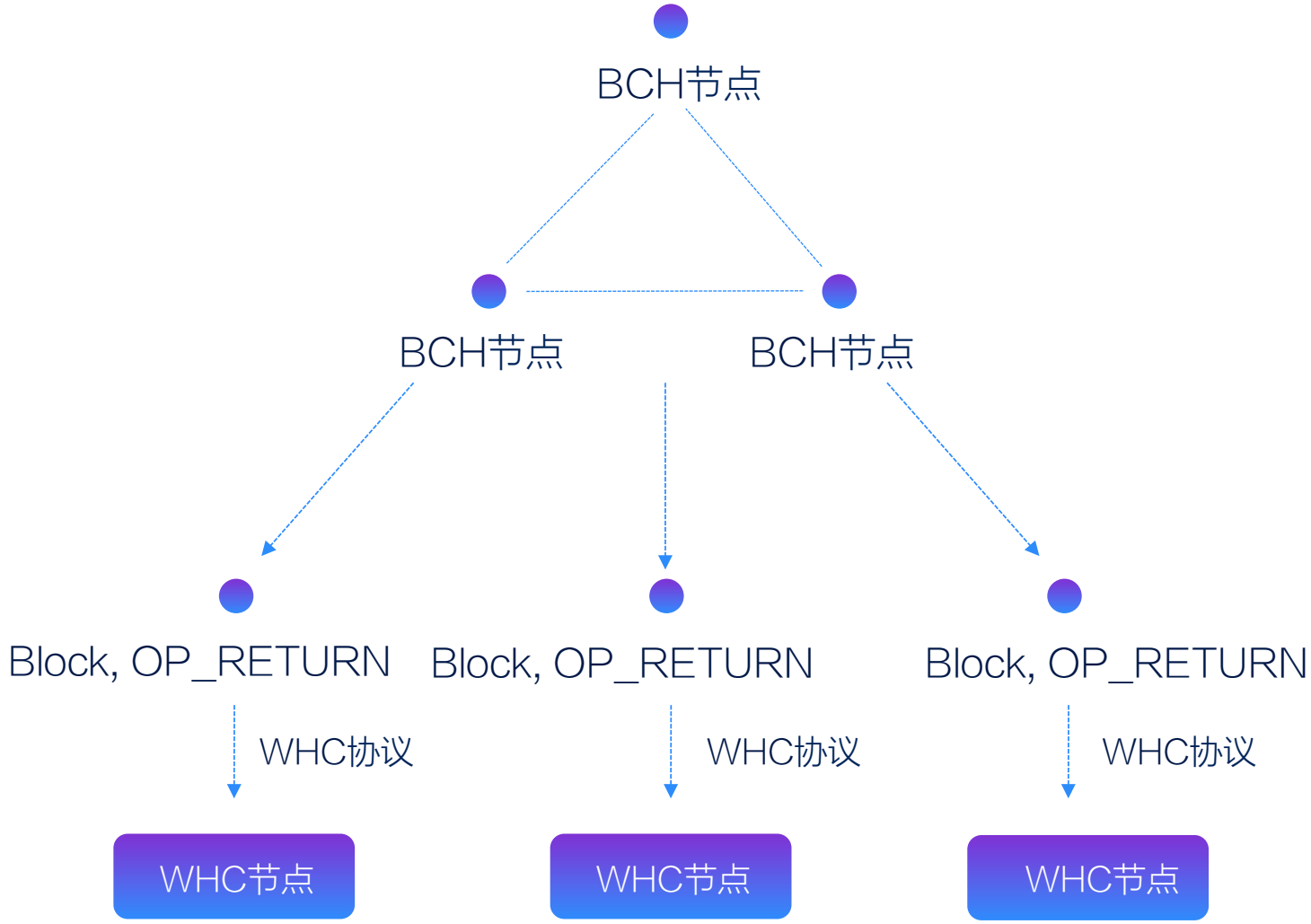
智能合约Gas

其他事物性操作，或者其他被认定为具有DoS风险的操作类型

安全

1. BCH的POW算法
2. WHC数据存储在BCH链中，数据可追溯性
3. 去中心化时间戳服务
4. WHC节点，不符合协议的数据不会被解析

WHC安全模式


BCH节点
BCH节点
BCH节点
Block, OP_RETURN
Block, OP_RETURN
Block, OP_RETURN
WHC协议
WHC协议
WHC协议
WHC节点
WHC节点
WHC节点

识别协议需安装客户端

更改Wormhole协议到ABC客户端

在block验证和交易验证之后预计好接口

以库的形式实现和ABC的代码合并

ABC的协议变 动直接合并

Token Issue

1

固定数量的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

可管理Token

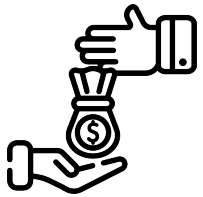
- 创建时，Token数量为0
- 不能众筹
- 可以增发，可以燃烧

3

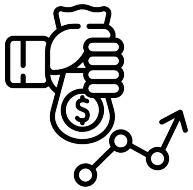
可众筹Token

- 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

Token Transfer



代币之间也可以做到原子交换



一个标准的BCH交易

输出对于BCH的Output

地址不在OP_Return, 其他信息在OP_Return

Token Burn

手动管理的Token

燃烧Token会减少总量

Wormhole

路线图

01 初始（Earth）

02 融合(Tropos)

03 电离(Lonize)

04 散逸(Exophere)

01 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。此阶段暂不支持Omni Layer协议中的去中心化交易功能。

Earth阶段已完成的工作:

- 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

02

融合

去中心化交易所

P C 端

Android客户端

IOS客户端

2018年11月


阶段3:电离
实现ERC721
多语言SDK
冷钱包解决方案

04

散逸

无需许可的智能合约

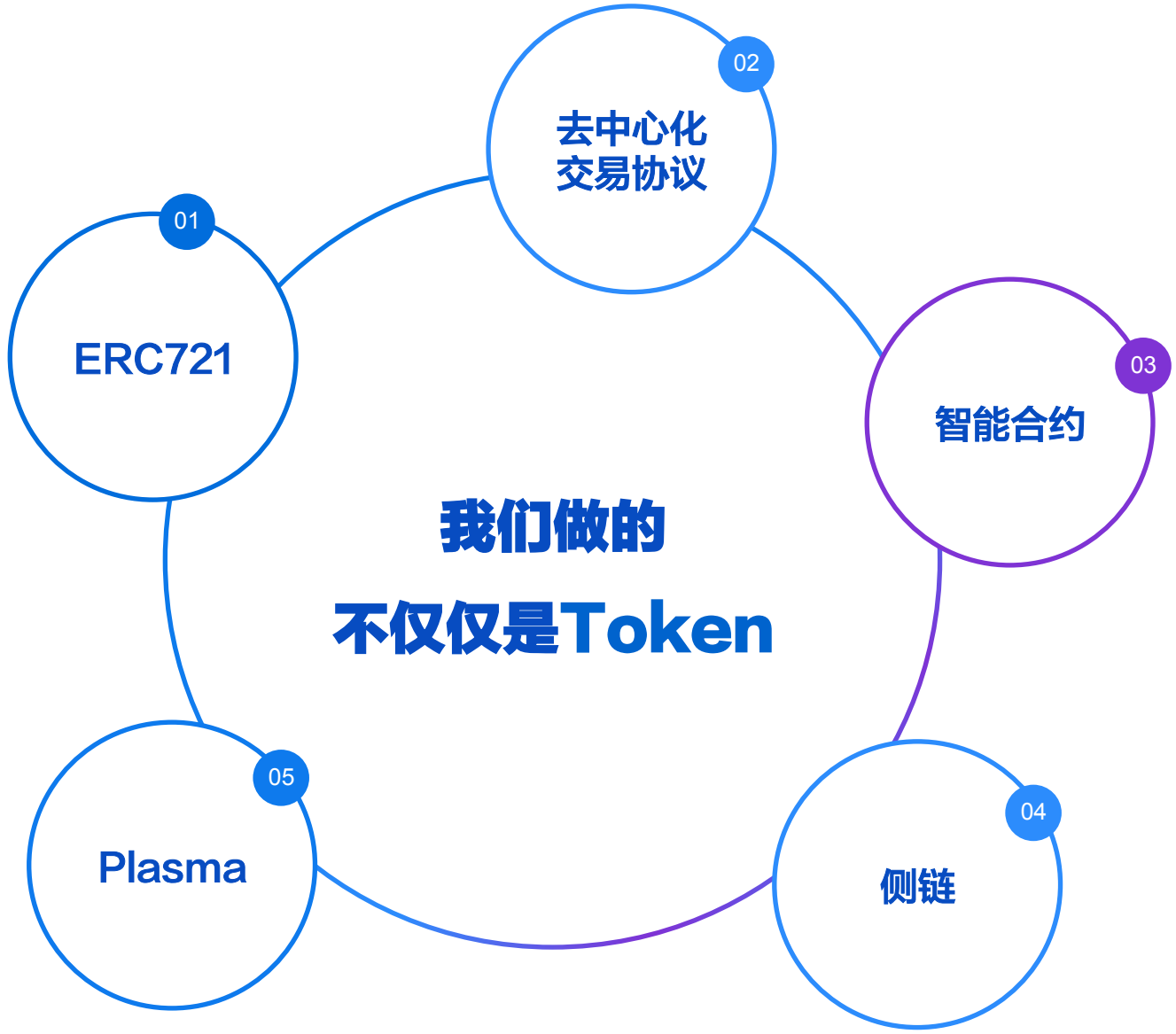
在遵守维护协议安全的必要规则后，任何开发者都可以发布智能合约到网络中运行

智能合约虚拟机

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

Plasma协议

实现Plasma协议，实现扩容


01
ERC721
02
去中心化
交易协议
03
智能合约
04
侧链
05
Plasma
我们做的
不仅仅是Token

主办方 Geekbang 极客邦科技 InfoQ

THANKS