本期项目：ZCASH

完成时间：

**Zcash基本情况及概述**

ZCASH于2016年10月公募，基于比特币核心软件及代码开发，承袭比特币优点，又在匿名性，加密算法有进一步突破。

Zcash是第一个使用零知识证明的加密货币，创始团队具有强大的技术研究团队，与高盛等金融机构合作，还有行业大咖老猫李笑来等为其站台。

不可否认，背后资金推动，大佬站台，但是Zcash本身体量很小，和BTC ETH完全不在一个量级上，即使一枚曾高达200万美金，也急跌99.999999%

Zcas源自一些极客修改了比特币0.11.2，加上了“零知识证明”技术，想让比特币更具匿名性。但比特币开发团队拒绝支持Zerocoin，于是极客团队另起炉灶，搭建了一条新链。Zcash核心代码来自BTC，它使用UTXO交易模型和Pow共识算法，Zcash具有2mb块大小和2.5分钟的块间隔。这使Zcash更快一点，吞吐量也更大。

Zcash用户可以选择两种交易方式，由具有两种地址类型的系统完成。t-ADDR透明地址是以t开头的36字符字符串，z-ADDR隐私地址是z开头96字符的字符串。

两种地址可以互发交易，无论地址是否一致。如果是z-ADDR发送给z-ADDR的交易，则交易是隐私的。交易的地址和交易的ZEC数量都会被隐藏。如果z-ADDR发送给t-ADDR的交易（或相反），则z-ADDR会被隐藏但是交易的ZEC数量不会被隐藏。

上述验证交易算力花费很大，且已经被提议在链上做存储证明，但是会极大增加区块链大小，最终被否决了。技术团队已经在考虑下一版本Sapping升级中采用链下存储以解决。

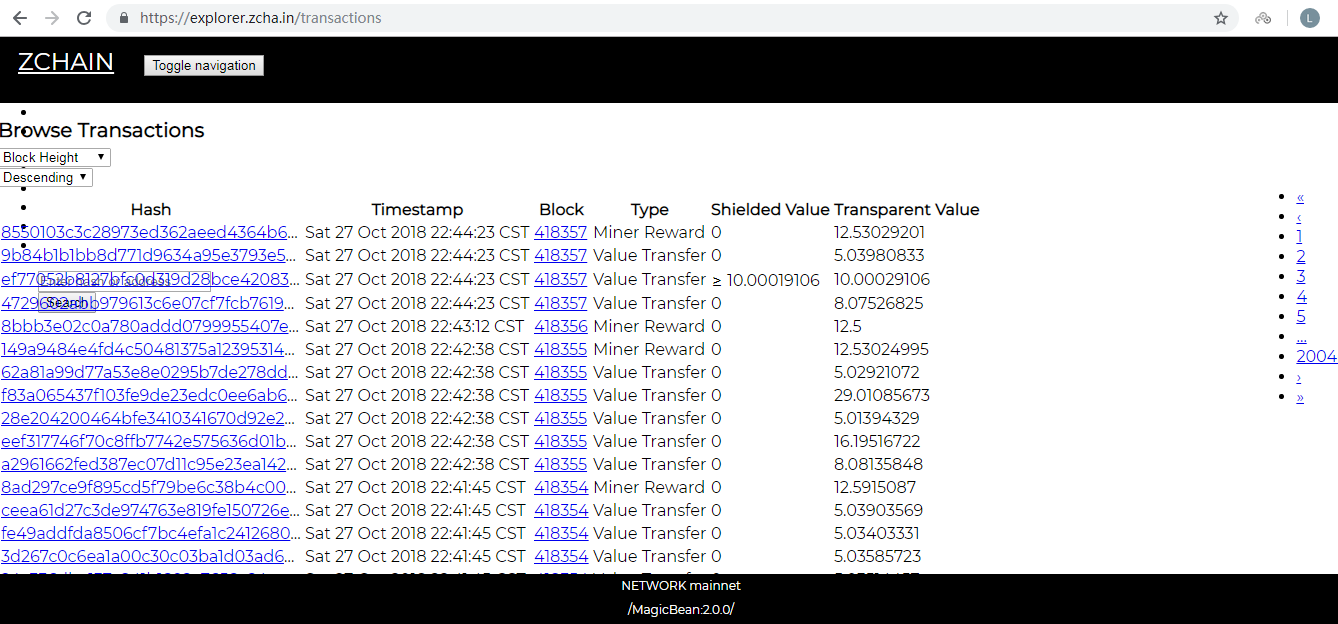
一、功能评测：

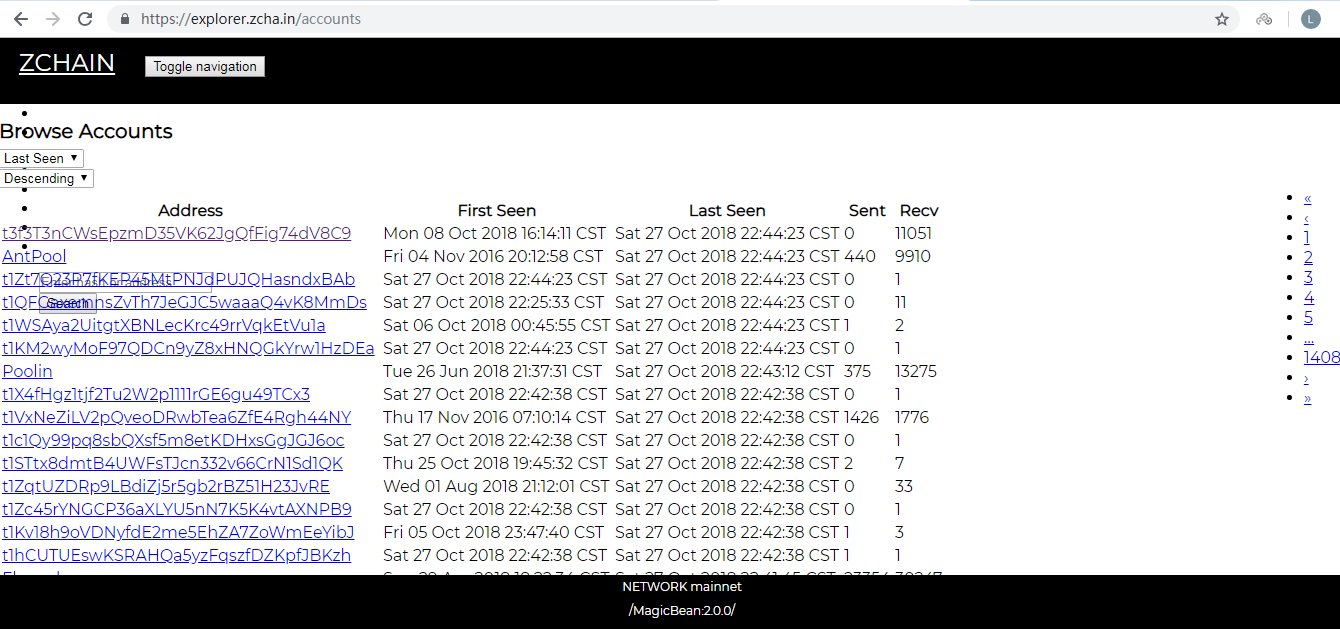
**（一）区块浏览器**

基本功能实现：区块查询、交易查询、哈希查询、地址查询、节点分布查询可实现

功能性能：界面不太友好，查询不太方便（非翻墙原因）







1. **钱包**

目前 ZCash 仅支持 linux 系统，不支持 Windows、MAC，且只支持命令行， 没有图形界面（zcash 团队没人擅长 GUI）。据说有win版本出来，下载了不能使用。

**二、技术及社区评测**

比较成熟的项目，代码方面其实没什么分析的了，核心代码来自BTC 0.11.2，加上零知识技术；挖矿算法创新自行设计：Equihash挖矿算法（理论依据是广义生日悖论）。BasicSolve用于测试挖矿，OptimisedSolve用于主网挖矿。

首个采用zk-snarks实现隐私保护交易的加密数字货币，交易数据通过匿名处理，无法再公开地址上查到，除非授予查看秘钥。

（一）Github代码提交量



（二）用户社群活跃度

|  |  |  |  |
| --- | --- | --- | --- |
| **分类** | **表现** | **分类** | **表现** |
| Twitter | 关注者：71.3k | Facebook | 关注者：9364 |
| Telegram | 成员数：2437 | Reddit | 关注者：14.5k |
| Medium | 关注者：3.3k | Youtube | 订阅者：2001 |
| Vimeo |  |  |  |

1. 全网算力对比

上述验证交易采用的零知识证明方法需要占用大量的CPU算力。而全网算力对比，和BTC等远不在一个量级上。技术团队计划Sapping升级采用链下存储，以解决交易验证工作量增加的问题。

|  |  |
| --- | --- |
| 分类 | 全网算力 |
| BTC | 48.732EH/S |
| ETH | 246.60 TH/S |
| DASH | 2497.72 GH/S |
| ZCASH | 1.99 GH/S |

**三、产品推进计划：**

没有发现Zcash有非常清晰的项目发展路线图，重要技术突破和项目合作，主要官网和博客发布。

2017年12月，官方blog发布技术路线图，

包括Saping，Overinter（https://z.cash/blog/roadmap-update-2017-12/）。

|  |  |  |  |
| --- | --- | --- | --- |
| **技术落地计划** | **技术规划** | **计划完成时间** | **实际完成时间** |
| Overwinter | Overwinter计划主要聚焦网络升级和用户交易的安全性。 | 2018.06 | 2018.03 |
| Saping | Saping将激活协议，提高隐私保护交易的时间和存储性能，并且支持移动钱包。 | 2018.09 | 2018.08 |
| Saping升级 | 升级主要针对隐私交易，将极大地提高交易速度，同时减少交易本身的的实际规模 | - | 2018.10 |