# ZCASH技术评测

本期项目：ZCASH

完成时间：10月31日

功能评测：

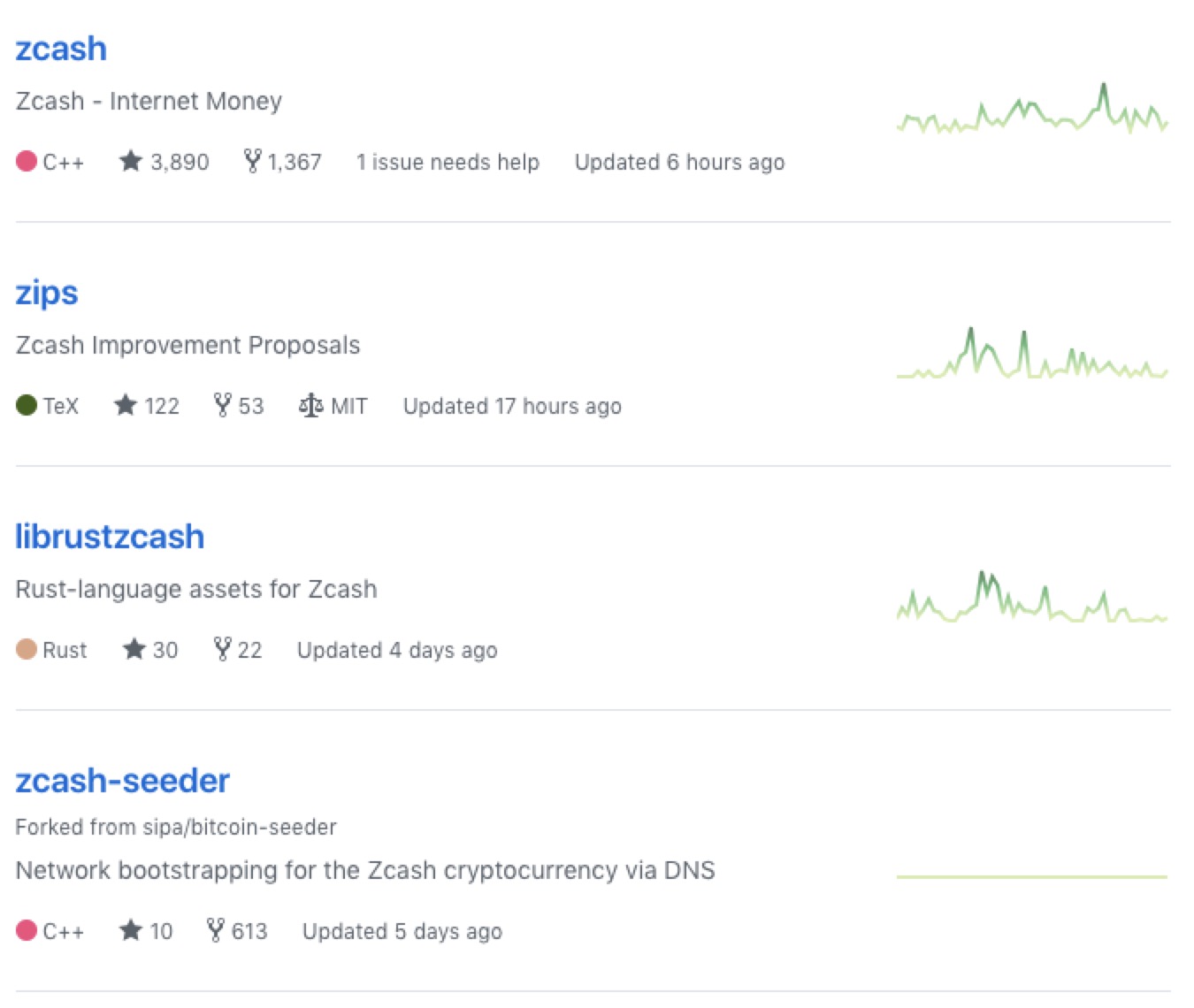
从功能角度出发，ZCASH主要增加了用户的隐私性，在比特币源码的基础上添加匿名转账支持。Zcash的支付交易在区块链上可见，但有个可选的隐藏打款人，收款人和具体支付金额的选项。

ZCash的地址氛围私有（以z开头）和公开地址（以t开头）。Z地址到Z地址的交易虽然在区块链上可见，但是具体的地址、交易金额和memo字段都是隐藏的，通过零知识证明技术来实现，在ZCash中被称为zk-SNARK协议。其他类型的交易，如 Z -> T，T -> Z 和 T -> T交易都是支持的，对应的包含Z地址的部分的信息都是匿名的。在ZCash中，包含Z地址的交易允许被审计，但是交易细节需要Z地址的拥有人同意才能公开。

ZCash的主打功能是支持匿名交易，由于其实际上是在比特币源码的基础上开发的，其他的如多签交易等比特币现有的功能其都支持。

代码质量：

目前Loom项目在github上已经有13个开源项目，项目更新都很活跃，基本上保持每周的频繁更新。ZCash本身的完整代码也是开源的，而且官网上也有明确的面对开发者的开发指导，以及如何加入项目开发的具体指导。总体上说项目的运作和进展还是很健康的。



ZCash白皮书中的想法据官网所说已经基本实现，而且在2016年9月9日发布了第一个beta版本，后续的改进采用类似比特币的BIP改进系统，--ZIP系统经过详细讨论再逐步实现。

技术能力：

ZCash作为美国约翰霍普金斯大学计算机科学教授的创业项目，团队技术能力较强。然后业界对其的风险以及质疑有几点：

1. 支持匿名交易的特性对计算机要求较高，不仅要求数GB的内存，而且在一个性能良好的笔记本上也要一分多钟才能完成匿名交易，注定其要在当前主流手机上实现匿名交易基本不可行。而且使用匿名交易对于最终用户来说要求较高，使得实际上很少有人使用zcash的匿名交易，也难以验证其技术实现的真实性。
2. 在一些Z -> T的交易场景中，也有可能通过非匿名部分泄漏匿名部分的交易信息。
3. ZCASH的零知识证明依赖一些公开的参数，而这些公开的参数又依赖于一些高等数学方面的假设。实际上除了一小部分学术圈的人能看懂Zk-SNARKS协议，大部分人都不大理解Zk-SNARKS的实现细节 – 包括笔者自己。一般加密学都是基于公开的广泛理解的加密算法实现，这样才能保证加密算法尽量公正，而只有一小部分人才能理解的数学算法，不排除真正发现算法漏洞的人出于某些目的隐藏这个事实的情况。

产品推进计划：

截止2018年10月31日，ZCASH团队已经进行了几次硬分叉升级，从产品实施角度来说，还是在稳步进行软件的升级。