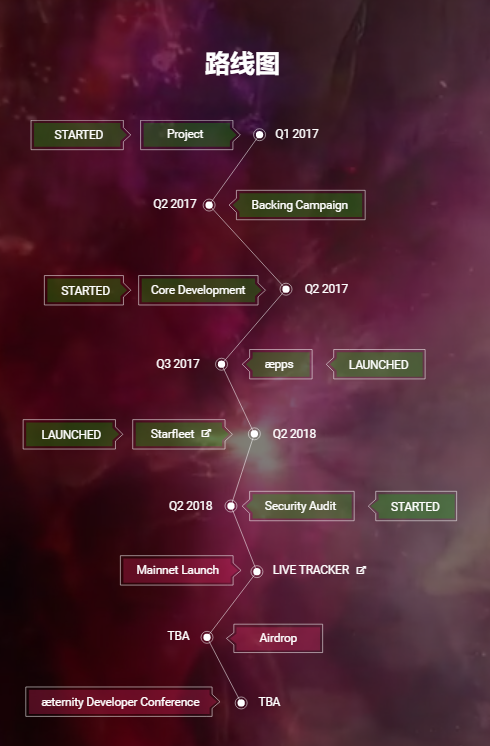
# Aeternity技术评测更新

## Aeternity功能评测更新：首先需要指出的是，目前，Aeternity主网依然没有上线，且测试网也没有相应可视化的版本发布，和上次评测相似，目前Aeternity项目整体参与度不高，还处于测试算法以及网络运行稳定性的阶段，本次更新主要介绍目前来看从功能角度有哪些新的特点和问题。

首先是目前Aeternity真正的进度的问题，上次评测时，Aeternity官方曾在官网中指出2018年第二季度会完成主网上线的相关工作，而目前并没有完成，主网还在迭代开发中，且新的roadmap也更新了新的计划，但此次并没有明确指出什么时候可以完成主网的开发，而是公开了一个pivotaltraker的链接，通过该链接Aeternity官方直接公布了官方开发人员的开发实时进度跟踪表，在该链接中可以更直观的看到代码的上传、测试、功能进度等等的开发流程，但是该链接只能帮助用户了解Aeternity官方还处于不停的代码迭代开发中，并没有对主网没有上线这一事实以及何时具备安全、初步功能的主网能够上线产生影响。

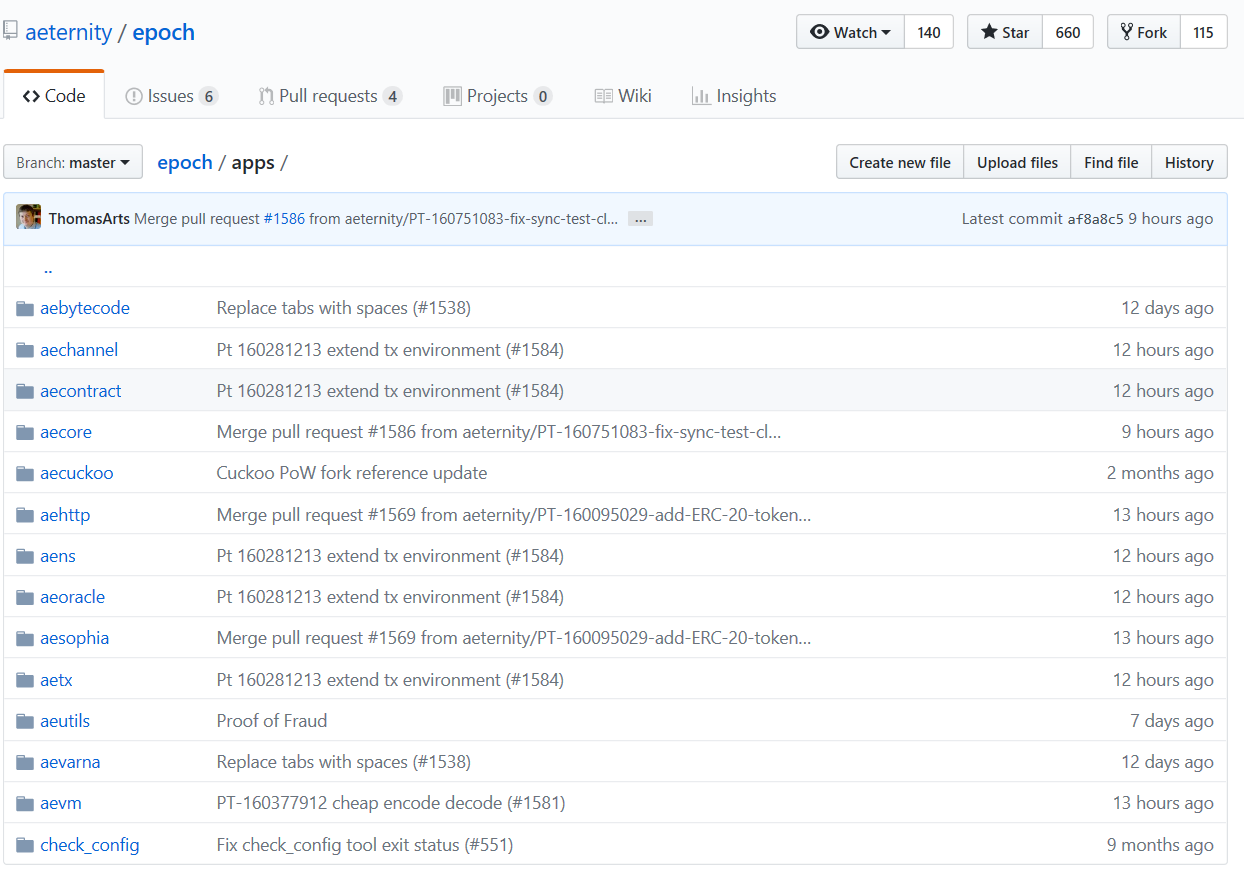


其次是关于Aeternity功能的直接表现，也就是dapp、区块浏览器等等应用并没有真正可用的版本，我们查了Aeternity开源代码库中几乎所有的代码，可以明确找到有关区块浏览器、dapp等的开发工作在进行中，如果有开发者想要接入目前的测试网，也有相关的api调用方式以及文档说明，但是所有的应用都只可能被极少数开发者调用，没有可视化可应用的版本发布，虽现阶段主网并未上线，但是测试网却上线时间不短，但是目前的测试网只具备某些功能的调用测试的能力，不具备性能展示的能力。

最后是关于目前测试网的功能以及相应的性能以及安全性的问题，在这里我们必须提到Aeternity官方的设计目标为一条具备极高拓展性且兼顾去中心化与安全性的一条具备预言机功能与相应智能合约能力的区块链主链，然而目前我们并没有看到任何一个功能目标的真正实现，更没有看到任何一个性能目标的测试参数，也就是说目前我们只知道Aeternity的设计算法与实现有可能可以提高拓展性以及有可能可以具备某些功能，但是真正的性能参数以及功能的可应用程度在目前的测试网中没有任何体现，至于压力测试等等环节以及Aeternity的理论最大性能等等参数，也没有相应的展示，所以基于目前的数据以及实现度，我们对Aeternity真正的性能以及安全性有一定的怀疑。

综合来说，Aeternity并没有履行自己的开发计划，在释放出正在开发以及在不断的迭代更新等信号后就没有真正的可用的应用落地了，我们承认Aeternity的开发人员的工作量以及迭代频率，但是在目前区块链行业结果导向的大环境中，没有经过大量数据以及用户检验的项目我们始终不能称之为成功的项目，所以所有的一切都要等到主网上线后，有了一定的数据量级的积累以及统计数据的展现后，才能有所好转，我们也会持续关注。

## GitHub代码质量评测更新：Aeternity项目早已在GitHub中开源，开源代码也在不断的迭代更新中，该项目的代码结构以及相关创新点在上次评测中已做过解析，本次评测主要侧重于代码更新以及之前没有提到的点，首先需要指出的是，虽然上面说了Aeternity的可应用功能方面的实现度不尽如人意，但是在核心创新点以及算法方面在GitHub中几乎都有相应的代码体现以及很快的更新迭代频率，真正可应用的版本并不是遥遥无期的事情。



首先是去中心化预言机，首先预言机机制并不算是Aeternity项目的创新点，在Aeternity项目中相对有所创新的叫做去中心化的预言机机制，在该机制的代码体系中Aeternity制定了相对严格的预言机生命周期，限制了每一个操作的参数、传值、返回值、方法等等，严格规定了如果要成为去中心化网络节点中的具备预言机功能的节点需要提供的参数，通过这部分的代码研究，我们发现Aeternity的设计的确可以实现使预言机去中心化这一操作，每一个在网络中的节点都可以进行预言机注册，而后根据协议规定发布相应的现实世界的数据转码为可以被系统识别的字节码，在该部分中我们认可Aeternity使预言机机制去中心化这一操作，可以进一步提高系统的去中心化程度，降低所谓的官方这一概念，但是在这样的体系中系统不仅仅是维护一个预言机数据的真实可信，而是要维护每一个预言机所提供数据的真实可靠没有恶意操作，在这样去中心化的网络中权衡去中心化以及安全性的问题始终是一个难题，然后在Aeternity去中心化预言机的代码机制中，我们并没有找到很好的明确的确保预言机体系安全可靠的算法保证，在该部分的性能与安全性的权衡中，我们认为Aeternity项目还有一定的改进空间。

其次是智能合约的部分，Aeternity在该部分的代码实现中原创了Sophia这一适配于Aeternity智能合约体系的合约语言以及相应的虚拟机，在该部分的实现类似于对ETH智能合约平台的改进，虚拟机也与EVM的机制有很多相似的地方，我们判断在该部分的实现原理以及运行机制上与ETH会有一些相似的地方，虽然ETH的智能合约以及虚拟机相对成熟，但是Aeternity的机制中，某些轻量级的智能合约会在两个用户之间的状态通道（侧链）直接运行，不会经过网络中其他节点的认证与共识，虽然几乎所有的操作只与用户两方本身相关，但是我们不得不设想一下关于智能合约攻击主链本身的问题，由于智能合约的自由度大大增加，所以智能合约的不可控因素大大增加，当然Aeternity可以在合约权限以及运行权限以及设置不同的代码层次隔离智能合约，但是这些设定必须要等到真正的智能合约功能上线后才有可能体现，目前我们只是猜测有可能增加智能合约作恶的风险。

最后就是Aeternity最最核心的状态通道的问题，这样提高扩容性的解决方案在ETH的新的项目规划中也有所体现，我们在之前的评测中也有所分析，但是在更新评测中我们再次研究了实现方案、算法论证以及代码体现，我们发现在主网中只更新最新的状态这一设定是对传统保障透明性的UTXO模型的颠覆（我们并不表示谁好谁不好，因为Aeternity并没有真正的实现，不可在现阶段进行比较），在该网络中用户不能追踪到每一笔交易的前世今生，只可根据账户的参数状态直接判断下一笔交易是否可以进行，这样的代码实现的确可以加快程序运行的效率，但是这也有可能降低主链本身的安全性，况且可追溯与交易透明是区块链的初衷，这样的设定能否有很好的权衡我们也会持续关注。

## 综合评测：总得来说，Aeternity有一定的创新点，在代码层面也有一定的实现度以及相对较高的更新频率与热度，但是目前所有的功能与性能并没有稳定安全的可应用的版本发布，再加上这样的设定在算法论证阶段具备一定的理论基础，但是真正的性能与安全性的展示并没有数据的支撑，所以所有的一切都要等到项目有一定的安全与性能后的发布版本，才能有真正的检验，我们也会持续关注。