Jed McCaleb 谈恒星新特性

恒星是一个完全去中心的支付网络，允许任何人发送和交换任意货币。它可以被视为比特币的一个去中心化交易所。

为什么会创建恒星？在金融科技领域工作多年以后，我意识到世界的金融基础架构支离破碎，数十亿穷人被摒诸门外。所以，我和 Joyce Kim 共同发起了恒星基金会，意图为金融科技创建一个开放的标准。任何人都可以参与进来，对全球 20 亿无银行账户的人群更为有用。

自恒星基金会运营以来，我们已经宣布了数个合作关系，在联合国进行了演讲，以及发布了恒星新共识算法和代码库。与其他为恒星核心(Stellar Core)的贡献者，David Mazieres 教授、Graydon Hoare 和 Nicolas Barry 一道，我重新设计了此新代码库。我很高兴能够分享设计决策背后的动机，以及讨论恒星的前景。

升级为简洁的、模块化的网络

促进互联网有机增长的一个关键因素是底层简单的基础设施。据此我们设计新网络时尽可能地将复杂性往上层移。利用这些可以不同方式组合的基础设施，我们的系统既健壮及具备良好的可维护性，同时依然功能强大，富有表现力。

新网络更安全，更具伸缩性以及更加模块化。我们将网络的功能的分解到多个组件，使得它们易于被理解，维护以及扩展。恒星核心代码量比上一版本要小一半以上。现在数据存储于 SQL 数据库中，这样人们可以更加轻易的从恒星网络中将信息提取出来，使用标准工具和库即可交互。Graydon 的演示提供了恒星系统中数据的所在和复杂性移动的详细细节。

安全第一

我们重构代码的一个主因是实现新恒星共识协议(SCP)，这包含一个独特的，能够保证正确的联邦共识算法。分布式系统很复杂，在分布式网络中达成共识更加复杂——这需要一个对其充分理解和可证明的共识算法如 SCP，来保证网络不会分叉。

为保证最大限度的安全性，我们在单元测试和集成测试中模拟了大量的失败情景。我们还使用连接恒星核心和 Kyle Kingsbury 的 Jepsen 工具的接口和模型来验证分布式系统的网络分叉情景。在上述所有情景中，网络中断，直至必需的节点共识模型重新建立，并在中断点恢复运行。网络在这些条件时必须中断。要么选择分叉，这意味着网络分裂成两部分，网络状态不再一致。不分叉是任何分布式，去中心化共识算法的关键特性，我们在此花费大量精力和时间，来保证这一点。

智能合约

按照我们的设计理念，我们专注于设计简易的组件，用户可以任意组合来达到他们的目的。我们实现智能合约的方法是将大部分逻辑从核心系统中剥离，来保证恒星核心能够适应全球应用的使用规模。

恒星网络的智能合约的两个关键组件是多重签名支持和批量操作。恒星账户现在可以拥有多个不同权重的签名人，你能简单地实现 m/n 的账户或者更复杂的权限方案。

事务现在是一系列的操作，这些操作影响世界的状态。例如，一个单一事务可以是，如果 B 发送给 C，则 A 发送给 B。这些抽象（事务），加上恒星网络的分布式交易，能为智能合约生成令人惊讶的丰富词汇。债券，托管，债务抵押以及闪电网络在恒星网络上皆成为可能。

社区驱动的网络

目前恒星网络完全是由恒星基金会以外的社区运行。我们希望保证网络不会由恒星基金会操作和管理。恒星基金会贡献开源核心代码，除此之外，社区将会让这个网络更加丰富多彩，富有价值。

畅想未来

我们正在开发给予恒星协议的工具和衍生协议。未来将会支持更多特性如消息以及私有事务（private transactions）。

我脑中存着好多可以在恒星网络上实现的有趣的创意。我随手记下来一些我最喜欢的点子：https://github.com/stellar/docs/blob/master/guides/things-to-build.md

老实说，我更希望看到人们自己的创意，并且一定会有很多。

Jed McCaleb 是恒星基金会的联合创始人和 CTO。2000 年他开发了电驴，当时最大的文件分享网络之一。之后创建了 Mt.GOX，第一个比特币交易所，随后售予现有者并被重新编写。可在 GitHub、 LinkedIn 和 Twitter 联系 Jed。

原文链接：
https://bitcoinmagazine.com/articles/stellar-s-jed-mccaleb-what-s-new-on-the-upgraded-stellar-network-1452109082
翻译：老翅、喻学才
校对：梁然