脸书将如何&#039；天秤座区块链的工作？Libra协议允许一组来自不同权限的副本(称为验证器)共同维护可编程资源的数据库。

这里没有语言——系统会被一系列权威以自上而下的方式控制。但是请注意

，这意味着数据库是为&quot可编程资源&quot不仅仅是数字货币。

这些资源由通过公钥加密验证的不同用户帐户拥有。

，并遵循这些资源的开发人员指定的自定义规则。

常用词如&quot资源&quot让我怀疑这不仅仅是一种稳定的货币。

交易基于预定义，在未来版本中，用户定义的智能合约将采用名为Move的新编程语言。

。我们使用Move来定义区块链的核心机制，比如货币和验证者成员资格。

好了，现在变得有趣了。

。使用定制的智能合同语言会导致许多关于语言丰富功能的问题，从而导致系统&#039；反对合同的能力。还有一些关于开发者友好性的问题，以及Libra如何保护智能合约开发者不受影响。

这些核心机制可以创建一种独特的治理机制，这种机制基于早期存在的机构的稳定性和声誉。

但是随着时间的推移，向完全开放的系统过渡。听起来天秤座协会将会变成一个联盟。

可以借助投票系统和一些预存的口碑来开发。还有一些关于开发者友好性的问题，以及Libra如何保护智能合约开发者不受影响。

1.简介

这个生态系统将提供一种新的全球货币——Libracoins——它将完全支持一篮子银行存款和来自高质量央行的政府债券。

Libra是一个通用的加密资产协议，第一个资产将是一个stablecoin。

久而久之，会员资格将完全开放，只基于会员所持有的天秤。

听起来像是权益证书。显然，计划是在五年内开放会员资格。

而且我希望他们能找到当时的股份证书——虽然我预计他们会遇到和以太坊一样的问题。

该协会发布的报告概述了向无能为力的制度过渡的路线图。

我&#039；我敢肯定，这将是分布式网络第一次从允许变为不允许。也许全网都可以转换成权益凭证，但是为了维持币/篮稳定，

一些实体必须对传统金融体系保持开放。这将是通过天秤座协会集中控制的持久点。

验证人员轮流推动接受交易的过程。当验证者充当领导者时

，它建议将客户直接提交给他们的交易和通过其他授权码间接提交的交易移交给其他授权码。所有验证器执行交易并形成包含新分类帐历史的经过验证的数据结构。作为协商一致协议的一部分

验证者投票给数据结构的验证者。

这听起来像真正的拜占庭容错，一种20年前就很好理解的算法。

虽然他们可能做了一些调整。我们在白皮书的第5节中了解到，它被称为LibraBFT，是HotStuff共识协议的一个变体。

作为在版本I提交事务t1的一部分，

共识协议在版本I中输出数据库的完整状态的签名——包括其整个历史——以验证对来自客户端的查询的响应。

这是值得注意的，主要是因为这意味着新的验证者应该能够加入网络并快速同步，而不必重放区块链的整个历史。

假设他们信任现有的验证器。账户模式是有意义的，因为脸书不太可能关心隐私，而且它对智能合约非常感兴趣。

2.逻辑数据模型

Libra协议使用基于帐户的数据模型来编码分类帐状态。

从数据结构上来看，天秤座更像以太坊或者说涟漪，而不是以太坊。由于基于输出的历史的简单性

UTXO模型有优点也有缺点——更好的隐私和更强的交易历史——但是使用复杂的智能合约可能更困难。因此，账户模型是有意义的，因为脸书不太可能关注隐私，即使该平台听起来对智能合约感兴趣。

Libra协议不将帐户与真实身份相关联。用户可以通过生成多个密钥对来自由创建多个帐户。

。由同一个用户控制的帐户之间并没有内在的联系。该方案效仿了比特币和以太坊的例子，因为它为用户提供了假名。

听起来出乎意料的好，但我想知道资产天秤币是否也是如此。

。有趣的是，观察这个系统对那些想要构建更多隐私保护应用程序的开发人员有多开放。

每个资源都有一个由模块声明的类型。资源类型是一种名义类型，由类型的名称和资源的声明模块的名称和地址组成。

似乎可以生成一个可以分配任意数量资产的地址，只要每个资产都有唯一的名称。

执行交易Ti以生成新的分类帐状态Si和执行状态代码、气体使用和事件列表。

所以，现在我们知道了如何保护系统免受资源耗尽攻击，也许是通过使用类似以太坊的资源消耗系统。

分类帐历史记录中没有事务处理冻结的概念。

有意思。Libra协议中没有实际的区块链数据结构——块更像是一个虚拟的逻辑结构，验证者用它来协调系统状态的确认快照。

。备份，现在这部分的第一句话更有意义：

Libra区块链中的所有数据都存储在单一版本化的数据库中。

。版本号是一个无符号的64位整数，对应于系统执行的事务数量。

我所熟悉的每个加密资产网络都以相同的方式在非常高的级别上工作：有一个系统状态，然后执行一个事务，它实际上是一个状态转换函数。

，然后出现一个新的系统状态。

将批处理事务放入容器或块的目的是对它们进行排序和标记时间戳。这对于未经授权的网络非常重要。

其中数据通过动态多方签名进行认证，验证者可以自由地加入和离开网络。由于Libra运行的是允许的系统，所以可以使用更高效的一致性算法，不需要批量处理事务，因为事务历史更不可能被重写。

在Libra协议的初始版本中，用户只能使用Move的一小部分功能。尽管Move用于定义核心系统概念

，比如Libracurrency，但是用户不能发布声明自己资源类型的自定义模块。这种

方法允许Move语言和工具链通过实现核心系统组件的经验变得成熟——在它对用户公开之前。。该方法还延迟了通用智能合同平台的数据存储中固有的事务执行和可扩展性挑战。

这听起来非常类似于&quot开放验证者成员资格&quot前面提到的程序。

。看来脸书还没有&#039；它没有解决以太网多年来试图解决的任何大问题。为了管理对计算能力的需求

Libra协议收取以Libra币计价的交易费用。

天秤币其实是协议的原单位。

很像ETH是以太坊的原始单位。这就引出了另一个关于天秤座本质的问题&#039；化名：没有AML/KYC你能得到硬币吗？如果没有，看来你可以&#039；不要匿名使用任何系统函数。来自阅读Calibra钱包

，这将需要反洗钱/KYC。所以想知道最终会不会进入控制松散的系统。

该系统设计用于正常运行期间。

产能足够的情况下，成本更低。

这个真的很模糊，提出了很多问题：什么是低成本？什么是正常操作？什么是足够的容量？

？

3.执行交易

区块链的许多核心逻辑都是由Move定义的，包括扣除汽油费。为了避免循环，VM在执行这些核心组件期间禁用气体计量。

。

这听起来很危险，但本文作者指出，核心组件必须以防御方式编写，以防止DoS攻击。

Move的关键特性是能够定义用户定义的资源类型.移动式系统为资源提供了特殊的安全保障。资源是永远无法复制的。

，只能移动资源。这些保证由移动虚拟机静态实施。这允许我们在Move语言中将Libra币表示为资源类型。

这澄清了早先的问题，天秤座硬币是否是本地资产，如瑞士联邦理工学院或BTC。

。希望这些币只是系统启动时默认或者唯一允许的资源类型，以后还会出现其他资源。

动&#039；的基于堆栈的字节码比高级源语言的指令少。此外，每个指令都有简单的语义。

可以用更少的原子步骤来表示。这减少了Libra协议的规范空间，更容易发现实现错误。

这听起来很有想法；我希望这意味着他们的脚本语言会比以太坊更安全。

我们看到&quot天秤座区块链&quot实际上不是区块链。

4.经过身份验证的数据结构和存储

Libra协议使用单个Merkle树来为分类帐历史提供经过验证的数据结构.具体来说。

，分类帐历史使用Merkle树累加器方法形成Merkle树，也提供了有效的附加操作。

我们再次看到&quot天秤座区块链&quot实际上不是区块链。这个协议似乎设计得很好。

但是当分类帐历史的数据结构是一组有符号的分类帐状态时，他们仍然称之为区块链，这真的很奇怪。验证器对每个分类帐状态进行提交，所有历史分类帐状态也在Merkle树中提交。但我没有&#039；我真的没有见过任何形成一个链的反向链接数据列表——更不用说一系列块了。

帐户的身份验证者是此序列化表示的哈希值。

请注意，这种表示要求在对帐户进行任何修改后，重新计算整个帐户的验证器。这个操作的代价是O(n)

其中n是完整帐户的字节长度。

嗯，如果给定帐户中存储的数据量没有限制，这听起来像是DoS攻击的开端。

我们预计，随着系统的使用，与帐户相关的存储增长最终可能会成为一个问题。正如天然气鼓励负责任地使用计算资源一样。

我们预计存储可能需要一个类似的基于租金的机制。我们正在评估最适合生态系统的各种基于租金的机制方法。

另一个未解决的问题。能&#039；不要等&quot房租太高了！"迷因

在电子逆向拍卖期间以及电子逆向拍卖之后的一段时间内，投票权必须保持不变，以便允许客户与新配置保持同步。

。离线超过这段时间的客户端需要与一些外部事实源重新同步，以获得它们信任的检查点。

哎哟

。不清楚这要持续多久时间段&quot是，但如果一个时代不到一天，那么我猜想指定&quot时间段&quot也是一样的。似乎这个共识协议还不够强大，参与者可以随心所欲地离开和重新加入网络。

5.拜占庭容错共识

LibraBFT假设一组3f1的选票分布在一群可能是诚实的验证者或拜占庭人的人群中。LibraBFT保持安全。

为防止双重花费和分叉等攻击，最多F投票由拜占庭验证者控制。

很像PBFT。

这种一致性算法可以容忍33%的验证者&#039；不诚实。HotStuff的修改听起来很合理：

通过让验证者签署块的状态而不仅仅是事务序列来抵抗非确定性错误。发出明确超时信号的起搏器验证者依靠法定人数进入下一轮——这应该会提高活力。不可预测的领导者选举机制，以限制对领导者的DoS攻击。聚合签名保留了对仲裁证书进行签名的验证者，以便对块接受进行投票。

6.网络

Libra协议中的每个验证者维护系统的完整成员视图，并且直接连接到任何需要与之通信的验证者。

。假设不能直接连接的验证器落在系统可容忍的拜占庭故障的配额范围内。

这将需要大量的工作来将系统扩展到数百个验证器。

7.Libra核心实施

Libra区块链的安全性取决于验证器、移动程序和移动VM的正确实现。

。解决天秤座核心的这些问题正在进行中。

几乎总结了这一部分，虽然他们用Rust写了实现。

这似乎是性能和安全性的良好开端。

8.表现

我们预计Libra协议的首次推出将支持每秒1000笔支付交易，提交和提交之间将有10秒的最终时间。

因为只有大约100个验证器，并且它们都直接相互连接，所以10秒的阻塞时间听起来是可行的。

最低节点要求：

40Mbps互联网连接1商用CPU16TBSSD。

一些先前的参考文献要求维持验证程序从头执行初始同步的能力，而不是信任来自其他验证程序的签名状态。

。我希望如果Libra被充分利用的话，执行这样的同步很快就会变得非常不切实际，那么节点安全模型将高度依赖于信任验证者。

9.用移动实施Libra生态系统政策

[天秤币]储备是实现价值保护的关键机制。通过储备，每枚硬币都有一套稳定的、流动的资产。

。天秤座硬币合约允许协会在需求增加时铸造新硬币，在需求收缩时销毁新硬币。该协会没有货币政策。它只能按照授权经销商的要求铸币和烧币。

。用户不必担心给系统带来通货膨胀或货币贬值：要铸造新的硬币，必须在储备中有相应的法定存款。

好

但现在我们说的是网络之外的事件。如白皮书前面所述，网络无法执行使用外部网络状态数据输入的脚本。因此，修饰语&quot可能&quot和&quot必须&quot在上述段落中，明确提及Libra协会的政策或合同义务，但网络并不知晓。

一致性算法依靠验证者集管理移动模块来维护当前的验证者集，并管理验证者之间的投票分配。最初的

，Libra区块链只授予创始成员投票权。

假设验证器对验证器集的更改进行投票。

听起来这将导致一个问题，类似于我们在股权系统的证据中看到的问题——远程攻击。如果创建成员的足够门槛&#039；私钥被泄露，攻击者能从Genesis写一个新的分类帐历史吗？如果是，其他节点会接受吗？

？尚不清楚共识协议是允许覆盖旧状态还是仅仅附加状态。

我们计划逐步过渡到股权证书。

如果他们能解决未解决的问题。

杰出的问题

治理是如何工作的？

这里可以看到，天秤协会是会员委员会，需要2/3的绝对多数才能做出改变。

。他们是唯一被允许铸造或破坏天秤币的人，但如果有足够的协议，他们可能会做出任何他们想要的改变。

您需要反洗钱/KYC吗？

显然，在协议层面上是不需要的，但Calibrawallet声明所有用户都将通过政府颁发的ID进行身份验证。

。听起来Calibrawallet至少在一段时间内是唯一可用的钱包，因此尚不清楚开发者和用户是否可以在Libranetwork上运行不遵循与Calibra相同标准的应用程序。

什么是低成本？什么是正常操作？什么是足够的容量？

CALIBRAwalletFAQ承诺低费用，但似乎这可能与高负载下底层协议的操作相冲突。

交易成本将是低成本和透明的，尤其是如果你在国际上汇款。Calibra将削减成本，帮助人们保留更多的钱。

天秤座真的会对开发者开放吗？

根据计划实现共识无动力：

Libra区块链将对所有人开放——任何消费者、开发者或企业都可以使用Libranetwork在其上构建产品。

，并通过他们的服务增加价值。开放获取确保了进入和创新的低门槛，并鼓励有利于消费者的健康竞争。

我怀疑开发者能在这个平台上运行他们梦想的任何技术上有效的应用。

。我读到的一切都让我相信这个系统会抵制审查，但只有时间会证明一切！