centre

白皮书

文档版本2.0
2018年5月

内容

1

执行摘要

我们生活在一个开放，互联，全球，自由的沟通和信息共享的世界。

1.1 中心愿景

开放式互联网 – 一个全球性的分布式计算机网络，共享通用的开放式软件协议 – 使数十亿人能够即时，安全地连接和共享信息，并且消费成本为零。对世界的影响是深刻的，并且仍在展开。

密码资产和基于区块链的计算和数据共享的发明已经引入
在开放互联网的下一个主要时代。

正如HTTPS，SMTP和SIP允许免费信息共享和通信一样，加密资产和区块链技术将允许人们以相同的方式交换价值并相互交易：即时，全球，安全且低成本。
开放的价值交换互联网可以更深入地改变和整合世界，最终消除人为的经济边界，并建立一个连接地球上每个人的更有效和包容性的全球市场。全球经济的未来是开放的，共享的，包容的，分布更均匀，并且不仅对少数选定的看门人而且对所有将要联系的人都有力量。

CENTER诞生于实现这一愿景的愿望。

CENTER由价格稳定的加密资产，网络协议和业务规则组成，这些规则在过去几年中由Circle以早期形式实施，其中现有技术支持重要的每日活跃交易量。CENTER计划创建一个网络方案，以管理这些资产的创建，赎回和流动，这些资产独立于Circle并与Circle分开。

除了管理和审计网络成员资格外，CENTER还计划提供技术，以在现有公共区块链基础设施的基础上解决价格波动和交易可扩展性挑战。具体而言，CENTER计划提供：

- 发行会员以发行和赎回资产支持的法定代币或"稳定币"以解决价格波动的机制；
- 使用状态通道在公共区块链上实现全局稳定币交易互操作性的协议，以提高吞吐量和可扩展性；
- 网络成员规则和智能合约，用于管理，审计和管理注册，交易和赎回稳定币的许可网络参与者。

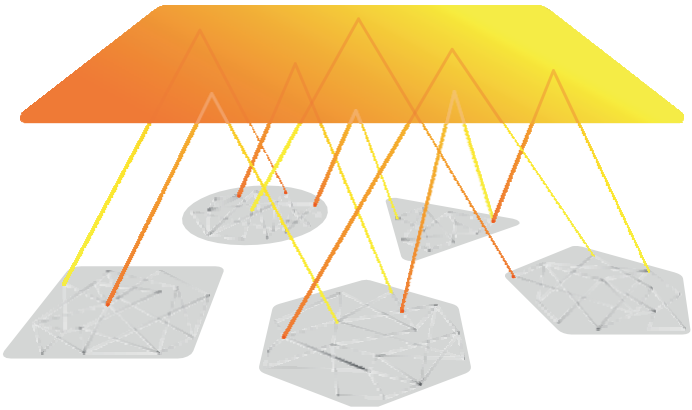
虽然Circle将成为CENTER网络的许可成员，但网络方案和加密资产技术将在一个新的独立实体下发展，该组织将独立于Circle管理和进一步开发CENTER协议。

本文档介绍了CENTER，它旨在解决的问题，设计如何操作，
以及如何管理它。为了澄清词汇，提供了关键术语的词汇表作为附录。

1.2 全球支付用例

在过去的五年中，基于移动的数字钱包已经在全世界范围内出现。这些应用程序允许人们使用他们的移动电话进行个人对个人和个人对商家的付款。这些移动钱包在每个国家都有扩散，

它们由银行，移动运营商和技术公司混合提供。每个人都声称
使消费者支付更加无缝。然而，几乎所有这些都是在传统银行和卡网络支付系统之上构建的薄软件垫片。每一个都是孤立的和专有的。他们住在有围墙的花园里，借用互联网1.0时代的在线服务。虽然我们可以自由地交换信息和内容，并以开放和全球的方式，金钱和自由交流付款仍然锁定在旧的封闭世界孤岛中。



CENTER旨在为连接世界上不同的数字钱包提供解决方案和新的激励措施：法定令牌稳定币的网络方案，允许钱在钱包之间流动，就像信息在网络浏览器和服务器之间移动一样，邮件服务之间的电子邮件，文本SMS提供商之间的消息。CENTER回答了这个问题："我可以立即给使用不同移动运营商的人发短信
我这样做，并且我不付钱给使用不同电子邮件服务的人发电子邮件给我，所以为什么我不能用支付宝付钱给使用Square的人付钱给在印度使用Paytm的人付钱给某人谁使用Facebook Messenger
– 即时，免费，世界上任何地方？"

全球消费者可以免费共享内容，并且可以互操作，而不是锁定在特定软件中

程序或设备;所以它将具有价值，因为金钱成为另一种形式的互联网内容。

企业和组织，无论是直接支持CENTER认可的稳定币还是通过与商业收单机构间接合作，都能够支持来自兼容数字钱包的直接支付。就像个人可以使用她的网络浏览器浏览商业网站的内容一样，她同样可以使用任何网站
她选择向那些使用其他合规钱包的人和企业立即安全地支付任何货币的钱包。

CENTER为钱包提供使用相同或不同货币进行价值交换的解决方案。持有令牌美元的一个钱包的付款可以发送给另一个持有韩元的货币，通过无缝和即时货币兑换。当然，也可以使用相同的货币在钱包之间进行付款 - 例如，使用Venmo的人可以使用Square向另一个人付款
现金或圈子。[1] CENTER协议旨在管理货币内外的不同稳定币代币的汇率规则和合约。

13 加密交换用例

除涉及全球支付的交易用例外，CENTER网络成员发布的稳定币还旨在解决涉及加密资产交换风险的关键用例。

加密资产交换是在线市场，买家和卖家聚集在一起交易比特币，以太币等加密资产。这些加密资产根据市场价格波动。标记化的法定货币，
例如象征化的美元，价值不会波动，而是与其底层支持资产的价值保持价格挂钩（在此示例中，一个代币化的美元的价值总是打算以一美元的美元价格计算。

这使得价格稳定的令牌对于提供法定连接以及加密交换的对冲风险非常有用，特别是在那些不提供传统的法定上下坡道的交易所上
- 只要价格确实稳定，并且只要在这些代币的铸造和赎回方面有合规的保护措施。假设投资者可以选择通过在支持交易所交易其比特币兑换美元代币来保护自己免受比特币波动的影响，并确保这些美元代币的价值不会波动。

Stablecoins还允许加密交换中的投资产品（例如证券和股权代币）以法定价值而非加密货币价格定价。诸如那些令牌
旨在代表股权，资金利息，结构性债务，贷款，股息权和其他投资产品，受益于价格和投资回报的稳定价格挂钩。

最后也是最简单的说，很多交易所都没有为法定银行账户提供任何直接的入口和出口连接。在这些交流中，

[1]如果在本文档中包含的示例中使用了真实公司，则仅用于说明目的，并且绝不表示此类公司正在参与或将参与CENTER网络。

与法定储备挂钩的稳定币可以为多种令牌类型的基本交易活动提供所需的集成。由许可和合规网络成员创建和维护的Stablecoin网关成为第三方法定服务提供商，用于连接这些交换机。

CENTER提供智能合约和治理，使发布网络成员能够为客户提供这样的稳定币
然后可以使用它们来管理支持加密资产交换的风险敞口，并投资代表投资产品的代币。

14 应对加密资产和公共区块链的挑战

作为上述用例解决方案的基础推动者，区块链技术和加密资产有许多好处：一种透明的分布式机制，用于管理彼此之间具有不同程度信任的各方之间共享数据的可信更新;和可转让的有价值的商店
不依赖于发行主权的政策，而是基于支持它的处理能力，工作，股份和市场的价值。

然而，目前，现有的公共区块链实施和加密资产难以实现愿景，部分原因是由于三个重大挑战：价格稳定性，交易吞吐量以及由于缺乏对标准和网络参与者的独立治理而导致的风险（特别是那些成员提供贸易能力和平坦的上下坡。

首先，价格波动：为了使全球金融互操作性能够可靠和一致地运作，需要价格稳定的交换媒介和价值存储。以极端波动性波动的货币进行交易会产生复杂性和脆弱的结算合约，尤其是与在“标记化的法定货币”或法定挂钩加密资产中进行交易相比。

CENTER通过提供涉及“真实世界”资产储备的稳定币框架来应对这一挑战。每个stablecoin令牌对应于由发布的CENTER网络成员保留并由CENTER验证和审核的真实世界资产。

例如，像Circle这样的网络成员可能会选择提供标记化的美元和标记化的欧元，并使用保留的美元和欧元支持此类令牌，并使用CENTER审计Circle来确保合规性和偿付能力。从理论上讲，另一个网络成员可能会将另一个资产（例如黄金）标记为代币，并且类似地使用实物黄金备用该代币。关于限制，证明等的规则将由CENTER对每个发布网络成员强制执行。

当前技术的第二个挑战是区块链事务吞吐量。当前的公共区块链实现不支持高容量性能，因为每个事务都被写入底层分类账，并且向这些分类账打印新块目前涉及相对较高的延迟。

CENTER通过为钱包提供协议来解决这一挑战，使用状态通道以更高的速度进行交易。两个参与成员之间的交互的初始和最终结算状态（例如账户余额）被写入相关的底层区块链，但是干预交易不会写入底层链并因此以互联网的速度执行。这允许用于代币化法定货币的支付，但具有区块链的速度，安全性和可审计性。

现有实施的第三个挑战是缺乏对稳定币的独立治理
供应商。发证机构必须独立审计偿付能力和担保，否则
相关资产无法独立验证，价格稳定性变得脆弱。

以前尝试过生产资产支持的稳定金币时出现了这个问题。

CENTER通过将CENTER组织与其发布网络成员分离来解决此问题。CENTER本身不是发行会员或金融机构，而是网络
计划经理和技术提供者。CENTER强制遵守有关成员资格和行为的网络规则，以确保稳定性，问责制和消费者保护。

15 服务提供商：合规，身份，欺诈，风险

CENTER计划提供服务提供商机制，以支持信任和身份决策，支付结算和撤销规则，
以及KYC / AML相关信息的安全交换，以履行合规义务。

欺诈检测，风险评估，身份管理，AML服务提供商
监控和网络上的其他服务将能够实施CENTER服务提供商接口，以便参与网络并获得他们为交易网络成员提供的服务的费用。

例如，当使用CENTER将不同的钱包提供商相互连接时，这些参与的钱包必须符合适用的合规性和监管要求，其中包括相关的KYC和AML义务。
CENTER的服务提供商界面将允许提供商
提供支持KYC和AML信息交换的功能，同时利用加密技术保护PII并降低现有传统支付网络常见的PII泄漏风险。

16 治理和中心组织

CENTER软件实施预计将由为此目的而创建的新独立组织和实体进行管理。该组织旨在为CENTER开源软件项目提供支持，治理和持续研发。

该组织还希望提供可选认证，以提高对稳定币发行成员和钱包实施的信任，证明成员的合规性，审计资产支持，并提供支持和网络操作，以确保网络节点的连续运行。

该组织还致力于开展业务开发和支持计划，以便将新成员引入网络，并提交工程和支持资源，以便在构建CENTER的基础加密基础架构上工作。

预计网络治理将包括分布式共识和投票机制，这些机制利用即将出现的与特定令牌分开的CENTER特定令牌，旨在促进此类网络决策。

2

技术与网络

CENTER使世界各地的加密交换和钱包能够互操作。

通过跨区块链和平台轨道使用标准协议交换价格稳定的标记化值，并使这些钱包通过插入网络的服务提供商的良好定义接口，利用服务进行合规性，身份和风险管理。CENTER提供的技术通过资产支持的稳定币支持令牌化的法定货币，并通过采用可选的状态通道实现实现高交易吞吐量。

本节将更详细地介绍此技术。

21 Stablecoin Minting和Redemption Sequences

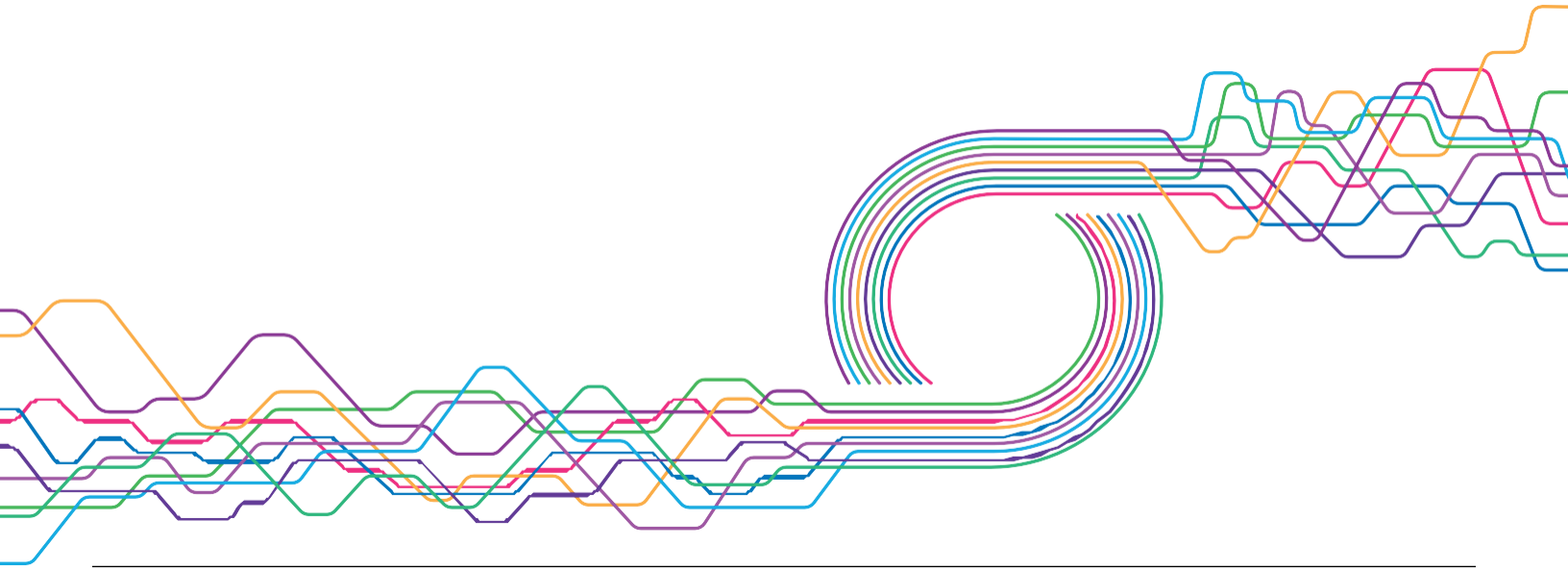
CENTER合同管理稳定币的铸造和赎回/燃烧，可用于交换和钱包互操作性用例。

通过stablecoin入口登机的客户，例如由持牌CENTER令牌发放会员创建和维护的Web应用程序，可以将法定资金转入该CENTER发行人的账户。然后，发行人与CENTER网络执行一系列命令，以验证，确认和验证与这些存入资金的价值挂钩的法定代币。然后客户可以将这些代币转移到其他地方以便使用它们。

赎回遵循相反的顺序：当客户访问诸如由许可的CENTER发布成员维护的Web应用程序之类的出口时，就会烧毁法定令牌。成功验证和确认后，基础法定储备的资金将转移到客户的外部银行。

考虑这个例子：

大卫是加密交易的交易员，他想在交易所购买加密资产，这些交易不能直接向他的美国银行提供法定连接



他还希望通过维持一些不会出现价值波动的美元代币形式的持股来对冲这些交易所加密资产的波动风险。

David访问由Circle创建和维护的Web应用程序（David也可以访问Web应用程序任何其他令牌发行成员的中心，但在这个例子中，他选择圆圈）。David注册了一个客户账户，这需要满足KYC的要求，然后开始存款流程，以便将他的法定货币变成代币化的美元。存款流程要求David将美元从其银行帐户转入Circle帐户。大卫对他在特定时期内可能转移的资金数量（以及他可能获得的美元代币数量）进行了限制。

一旦David的转移结算，Circle将与CENTER网络交互以执行所需的过程把美元代币传给大卫。这些代币可以从Circle的预先筹资的法定资产缓冲区中的现有储备中提取，以提高流程的速度;如果没有这样的储备，那么Circle使用CENTER协议来铸造新的代币。然后David收到令牌，这些令牌的价值直接对应于他存入系统的资金的价值。

大卫可以将美元代币转移到钱包或交易所的地址，以便他可以使用它们来支持他的交易活动。CENTER维护一个禁止地址的黑名单，以保护大卫和其他网络参与者免受已知不良行为者并支持监管合规。

当大卫 - 或大卫的一个交易对手可能已经获得一些美元代币 - 希望兑换代币并撤回底层的法定货币时，则该过程以相反的方式执行：大卫返回发行的网络应用程序（Circle）在此示例中），将令牌存入其可用于该Web应用程序上的帐户的钱包地址，和Circle执行基础美元储备转移到David的注册银行账户。

令牌从流通中撤出，或者被置于保留状态以便为将来的请求提供服务，或者如果这些令牌的价值超过Circle维持的预先补偿的法定缓冲区，则会被烧毁/销毁。此过程需要进行身份验证与存款顺序类似的授权，验证，确认和合规性。

请注意，访问stablecoins不需要在此示例中的专用Web应用程序中，但也可能发生在钱包，交换，银行门户或由CENTER网络的许可，合规，令牌发布成员创建的其他产品中。

22 电子钱包到钱包的交易顺序

CENTER可以促进在共享和不同货币中使用不同钱包应用程序的个人之间的合规，可靠，安全，高速传输，而无需私人业务发展谈判或使用私人网络。

考虑这个跨越应用程序和货币的假设示例：

移动钱包印度的Paytm和北欧的Vipps可以参与CENTER网络，并允许他们的客户转移卢比和克朗，即使钱包本身不直接相互融合，即使他们不共享普通的法定货币。

在幕后，本例中的Paytm钱包可以使用CENTER发行价格稳定的INR代币，并在该代币化卢比和其他标记化的法定货币之间公布汇率。同样，Vipps可以发行价格稳定的克朗挪威克朗代币，并公布该稳定币与其他法定代币之间的汇率，例如克朗兑换卢比汇率。

爱丽丝是挪威Vipps的客户，并希望将她的Vipps钱包汇给印度的Bob，后者使用Paytm作为他的钱包。当Alice开始交易时，Vipps指的是克朗和卢比稳定币代币之间的汇率；
如果Alice接受此费率，则交易将继续。如果Vipps没有这些硬币之间的汇率，但Paytm确实如此，那么Vipps也可能已经反映了汇率，并将克朗送到Paytm，而Paytm反过来会使用该汇率将其转换为卢比。

接下来，Vipps和Paytm可以执行任何所需的身份检查，合规性请求或风险评估，作为交易批准过程的一部分。这些操作可以可选地呼叫向CENTER网络提供此类服务的服务提供商，以换取在令牌中支付的费用。

例如，要继续Vipps-Paytm叙述中的序列：Vipps可能已将其CENTER节点配置为执行其自己的内部身份检查，而Paytm可能已配置其
节点使用提供身份验证服务的第三方服务。
Paytm和公司同意这项服务的价格，Paytm可以通过利用州渠道和稳定币令牌余额在每个API调用的基础上支付该价格。其他服务提供商（例如涉及欺诈检测或其他风险评估的服务提供商）可以类似地插入序列中。

如果在此示例中任何检查失败，Paytm或Vipps可以在传输任何值之前中止事务。

如果检查全部通过，则可以通过使用链式状态通道以原子方式传输该值。

为了完成这个例子：Vipps会更新Alice的应用程序余额以扣除相应的克朗，而Bob会看到他的Paytm卢比余额相应增加。当状态通道关闭时，Vipps和Paytm异步解决一批客户的问题。

23 商家付款顺序

CENTER还有利于合规，可靠，安全，
使用消费者钱包应用程序的个人与使用该消费者的商家之间的高速传输
销售点应用程序。消费者钱包和商家销售点软件使用CENTER标准进行交互。这类似于使用HTTP协议访问远程网站的Web浏览器，而不需要使用封闭的专用网络。

请考虑以下交叉货币示例：

Carol有一个WeChat钱包，持有中国人民币稳定币余额。她正在美国旅行，并希望从Dave购买一个三明治，Dave是一个使用Square移动销售点应用程序接受美元付款的商家。

在此示例中，Dave’s Square销售点应用程序不接受人民币或微信支付，而微信与Square没有直接整合。但是，如果Square和WeChat支持CENTER标准协议，付款可以在WeChat和Square之间无缝地工作，而不需要在它们之间进行自定义私有集成。

在这个例子中，微信和广场可以通过商定人民币和美元代币之间的汇率来促进他们的卡罗尔和戴夫的应用程序之间的支付。
微信的CENTER节点可以显示从人民币代币到美元代币的汇率，并使用人民币代币为Carol购买美元代币。转移将涉及将美元代币发送到Square。就像在人与人之间一样

如上所述，作为交易批准逻辑的一部分，也可以调用相同的服务提供商（用于合规性，风险，身份等）。

当然，如果节点所有者（在这个假设的例子中的微信和广场）同意另一个用于结算的令牌，则不需要在稳定币令牌之间进行交换。例如，如果Square直接接受RMB stablecoin令牌，则可以使用该令牌
对于同一笔交易，转让的人民币金额将由Square的人民币兑美元汇率而不是微信的汇率决定。

更简单地说，考虑这个相同货币的钱包互操作性示例：

查理有一个手机钱包应用程序，以美元结算。他在Dave的三明治店跟Carol排在一起，当轮到他时，Charlie用他的手机钱包支付给Dave's Square销售点应用程序。

即使Charlie和Dave有竞争公司的应用程序，这些应用程序也可以互操作，因为它们都支持美元代币的转移。使用CENTER，应用程序实现了互操作性，并可以无缝地促进基于付款
支持共同的开放协议。

24 加密资产跨区块链序列

CENTER还计划在区块链和加密资产之间实现交易，并且可以将这种加密资产连接到基于法定的账户和钱包。

例如：

弗兰克在Ledger（一种基于硬件的钱包）中持有比特币余额。如果他的钱包支持CENTER，他可以打开与其他CENTER节点的状态通道，以便路由基于比特币的交易和转移。例如，如果Poloniex加密
交换支持CENTER，然后弗兰克可以与Poloniex保持一个国家频道。

如果弗兰克希望用他的比特币钱包寄钱给查理，就像上面的例子所说的那样
他的手机钱包中有美元余额，然后弗兰克可以使用他的比特币钱包这样做，因为弗兰克和查理的钱包都通过CENTER进行互操作，尽管弗兰克没有持有任何美元代币。

Frank的连接是Poloniex，在这个例子中维护着一个支持美元稳定币令牌和BTC的CENTER节点。查理的手机钱包支持美元稳定币代币，但不支持BTC。Poloniex节点公布BTC与美元代币之间的汇率（即比特币的当前美元价值）。该费率显示给Frank，如果他接受，则交易可以继续。

然后，如在先前的示例中那样，令牌消费服务提供商可以按照他们正在使用的产品的要求输入序列以向Frank或Charlie提供合规性，欺诈，身份，风险或其他服务。

此示例中的事务通过状态通道执行，因此Frank可以确定Charlie接收到转移，即使它跨越区块链从比特币到美元代币（在以太坊链上）。

25 现有技术

CENTER计划通过利用知识产权贡献以及Circle中的永久许可来启动其实施的开发，其中早期形式的这些协议正在生产中。

定义网络参与者之间的交互的协议，API和业务规则表示高于这些规则的任何特定实现的抽象级别。现有的Web内容协议说明了这种关系：HTTP定义了一个用于请求HTML页面的词汇表，但不需要任何特定的技术实现，操作系统或编程语言。

词汇。类似地，CENTER协议定义词汇表和业务规则，但不需要特定的分布式分类帐，语言，运行时或操作系统来实现这些规则。

最初实施的CENTER协议存在于Circle，它在过去几年中建立，并支持多种法定货币和加密货币的大量交易量。CENTER计划在以太坊之上实施协议，作为一系列智能合约
和ERC20代币。CENTER计划利用现有实施来加速协议的新实施的开发。

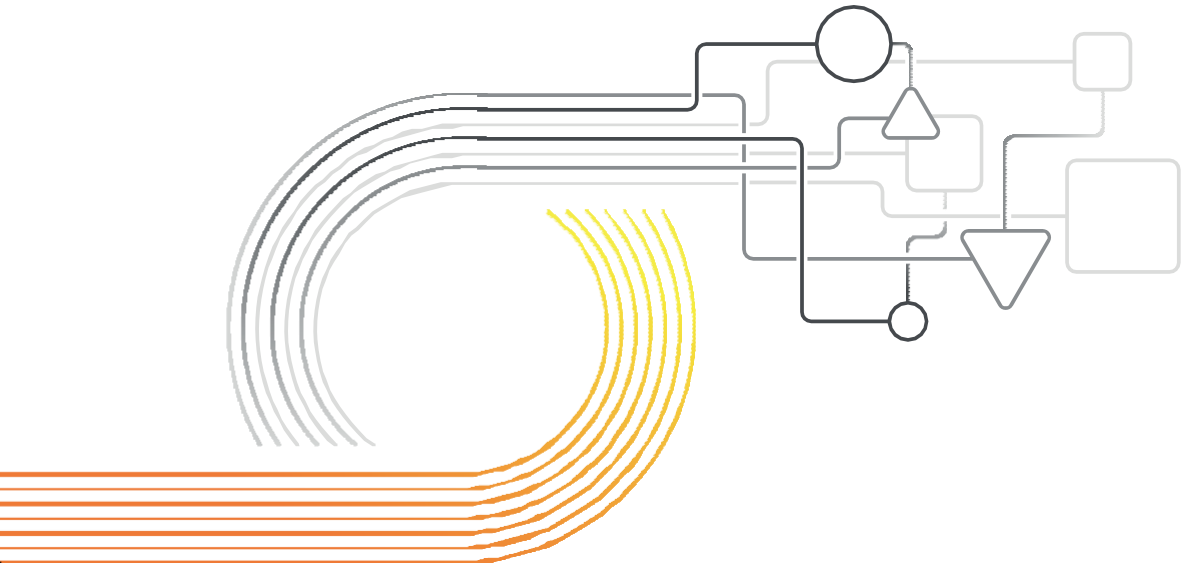
26 中心节点

CENTER打算将现有的协议实现从Circle发展为定义CENTER“节点”的新软件包。最初，节点预计包括（1）部署在以太坊上的智能合约集合，以及（2）代码知道如何与以太坊和那些智能合约互动。智能合约
包括法定代币合约（实施为ERC20令牌）和州渠道合同作为快速转移网络价值的选择。

电子钱包账户提供商，金融机构，软件公司和其他参与者将开始加入
通过托管一个或多个CENTER节点来建立网络。

节点旨在为网络参与者提供以下功能：

- 发行新的法定代币，例如代币，代表美元，欧元，人民币或节点所有者可以结算的其他货币；
- 配置哪些法定代币接受，或将决定委托给第三方；
- 发布交换法令令的费率；
- 将信任级别配置为规则，指示要信任哪些其他节点所有者和网络参与者，或将决策委派给a
  第三方，如支付网络；
- 在传输任何值之前交换有关事务的元数据，并根据元数据拒绝/批准事务；
- 确保通过使用状态通道以原子方式快速执行值传输。



初始CENTER节点实现（不同于协议的原始Circle实现）
旨在在以太坊上运行，使用状态通道允许网络在多个区块链上实现并跨区块链执行原子转移。因此，在将来，参与者不一定限于以太坊，并且可以将新的区块链添加到网络中。

27 技术实施说明

2.7.1 稳定币设计

存在价格稳定令牌策略的四种通
用方法：

- 菲亚特抵押：菲亚特储备中的资产抵押了代币，从而通过将代币值与保留的法定价值挂钩来提供价格稳定性；
- 加密抵押：储备中的加密资产抵押了令牌，并提供与这些保留的加密资产价值挂钩的价格稳定性；
- 算法无抵押：软件经济模型旨在提供价格稳定性，而不依赖于基础抵押资产；
- 混合：上述三种基本方法的混合。

CENTER旨在提供第一种：法定抵押方法。一个令牌化的法定货币单位由一个保留的法定单位支持。与其他稳定币开发方法相比，法定抵押方法需要满足公司传统监管要求，要求发行成员对传统支持资产具有强大的可审计储备能力（如作为法定银行关系），并提供较少的权力下放 - 而且就价格稳定而言，它目前也是最强有力的方法。

CENTER通过设想一个由多个令牌发放成员组成的网络来解决集中化权衡，从而提供多个储备和网络用户的流动性来源，而不是提出单一的抵押品网关故障点。这种方法是分布式的，尽管它并不意味着 - 或者目的是 - 完全分散。

此外，CENTER本身强制执行与审计/偿付能力，许可和合规性以及资本化阈值和限制相关的成员资格要求。这消除了对任何一个发布成员的依赖以提供这些控制。CENTER作为技术提供商和网络计划提供此类服务
治理并受到激励，以保持其所有持牌发行成员的合规性和偿付能力。

令牌发放成员与CENTER网络之间的交互在一系列由其创建和维护的智能合约中编纂
CENTER，以及促进此类交互的协议和网络策略。CENTER本身不保留法定资产储备，而CENTER不是金融机构;同样，发布网络成员不控制法定代币合同，
而是在与CENTER网络交互时利用它们。新的发布成员必须登上CENTER网络，新的法定代币将通过该流程加入该计划。

由CENTER创建和维护的合同旨在成为开源软件，受到持续的全球同行评审以及正式的安全审查，并通过内部CENTER工程开发得以发展
以及与世界各地的开源开发人员合作。

2.7.2 国家渠道交易管理

要以更高的吞吐率转移令牌，作为除直接使用以太坊之外的选项，
CENTER事务可以利用状态信道模式。使用此选项，节点以转移的令牌形式交换余额信息

在国家渠道。本节描述了状态通道如何在概念级别运行。

状态通道是两个或多个参与者安全地更新它们之间的共享状态而不在分布式分类帐上执行事务的方式，除了创建和完成状态通道
在分类帐上。状态渠道类似于支付渠道，但除了支付数据之外，州渠道还可以管理多种类型的共享状态。

为了创建状态通道，参与者同意初始状态并在底层分布式分类帐上执行事务
锁定在那个状态。可以在不执行分类帐上的任何事务的情况下执行后续更新。每次更新都只是一个新状态，如果新状态有效，则每个参与者都会以加密方式签署新状态。当参与者希望关闭频道时，他们每个人都可以执行交易，表示他们同意最终状态。

例如，想象Alice和Bob希望为付款创建一个州渠道。他们各自将100美元代币锁定为国家渠道合同
在分类账上，初始状态如下：

```
{
   alice_balance: 100,
   bob_balance: 100,
   sequence: 0
}
```

此后，Alice和Bob可以通过自己之间的通信来执行更新：当Alice向Bob发送50欧元令牌时，她通过生成新状态，加密签名并将其发送给Bob来实现。如果Bob同意新状态，他会签名并将其发送给Alice。它们之间的新状态如下：

```
{
   alice_balance: 50,
   bob_balance: 150,
   sequence: 1
}
```

如果Bob随后将25个令牌发送回Alice，他会生成一个新状态，对其进行签名，然后将其发送回给签名的Alice，生成另一个新状态：

```
{
   alice_balance: 75,
   bob_balance: 125,
   sequence: 2
}
```

当Alice和Bob希望结算这些付款时，他们会通过关闭渠道来实现这些付款。爱丽丝执行报告她同意最终状态的交易;鲍勃同意，所以他也执行同意最终状态的交易。由于他们同意，国家渠道合同然后根据最终状态将资金发送给每个参与者。在此示例中，Alice收到75欧元令牌，Bob收到125.从Alice到Bob的25个令牌的净更改将提交给分类帐。任何中间状态更改都不会提交到分类帐。

当一方希望关闭一个频道时，国家频道合同不会立即关闭。相反，挑战期开始，其他参与者有一段时间:

- 同意，在这种情况下，渠道已关闭，并立即进行更改;
- 通过提交由序列号较高的所有各方签署的州来纠纷最终状态;要么
- 什么都不做，一旦挑战期到期，这将构成协议。

想象一下Bob希望通过播放早期状态来“欺骗”的场景
这给了他150个令牌而不是125个令牌。该状态也由鲍勃和爱丽丝签署，所以它在某种意义上是有效的。

在这个例子中，如果Alice不同意Bob提交的最终状态，那么她将有机会
提交后来的州（序列2），该州也由双方签署;在这个例子中，这将取代鲍勃的最终状态。然后鲍勃可以同意或什么都不做。由于他没有双方签署的后来的国家，他将无法提出异议。这意味着没有参与者
可以防止其他参与者关闭该频道，除了合法的最终状态之外，任何人都不应该关闭该频道。

此外，任何试图欺骗网络的一方的声誉影响被记录下来并随后对其他参与者可见。

2.7.3 链接国家渠道

可以链接州渠道以支付其他方的付款。如果Alice希望支付Carol，并且Alice和Carol都有一个与Bob直接相关的频道，那么从Alice到Carol的转移可以通过Bob然后转到Carol而不需要Alice和Carol打开直接频道。为了以这种方式链接国家频道，系统必须强制确保当Alice支付Bob时，Bob将反过来支付Carol并且Bob不能自己保留资金。

这是通过使用散列时间锁定合同（HTLC）来实现的，这使得链式支付的执行与通过正常的直接状态通道执行链接支付一样安全。一条链子建立国家，如果收件人可以产生秘密，资金将被释放。然后，最终的接收者被给予秘密，他们将链条传递给链，并且链中的每个人都可以使用该秘密来获得资金。

在这个例子中，Alice向Bob提供了一个新的状态，该状态基本上表明：“如果你能够产生将产生这个哈希的原像，那么你就可以获得资金了。”Bob然后与Carol产生类似的状态。
爱丽丝然后给了卡罗尔原像。Carol使用该原像从Bob获取资金，然后Bob使用它从Alice获取资金。由于HTLC是由国家频道强制执行的，如果一方试图窃取资金，那么另一方
派对可以与HTLC和preimage一起广播交易，这将把资金引导给他们。

2.7.4 节点模块

内部节点子系统之间的交互通过明确定义的模块和API接口发生

使CENTER节点的部件更换或扩展尽可能简单。不同的网络参与者可能希望采用不同的内部技术（例如关系数据库，密钥管理，PII存储等），因此CENTER具有支持这些要求的可插拔方式至关重要。

计划模块的初步非包容性清单如下：

分布式分类帐和智能合约模块

管理和使用分布式分类帐的模块和界面以及必要的相关智能合约。最初，CENTER提供了一个实现以太坊模块和接口的模块。
此智能合约模块包括：了解如何与以太坊节点通信的代码，根据需要部署的令牌和状态通道的智能合约，以及与所包含的智能合约进行交互以实现价值转移的代码。

路由模块

用于确定协商传输的路由的模块。

CENTER协议模块

用于实现CENTER节点用于彼此通信的API的模块。

中心管理模块

实现API的模块，节点所有者用它来控制和管理CENTER节点。这包括支持启动值传输，部署新令牌以及更新节点和令牌的信任参数以及其他功能。

汇率模块

用于管理节点在资产之间进行交易时提供的费率的模块。

密钥管理模块

用于处理安全存储和检索加密密钥以便签名事务和执行状态更新的模块。

身份，风险，PII，合规性，授权和服务模块

可扩展模块，用于身份和帐户管理，KYC / AML合规性，安全存储，身份验证和授权，风险评分和其他服务。

3

中心
团队和组织

虽然最初是Circle的全资子公司，但建议将CENTER运营和团队成员转移到CENTER组织，这是一个将在未来几个月内创建的新实体。CENTER组织希望独立运营，拥有完全独立的专用营运资金，员工和技术开发。Circle希望仅仅作为原始技术和IP的创始成员和来源，以及作为CENTER的生产用户，如下面进一步详述的。

3.1 中心组织

CENTER组织旨在满足四个关键目标：

- 提供CENTER开源软件项目的研发能力，支持和维护。这个包括管理开源代码存储库，促进和支持第三方开发人员参与，传福音和代码贡献。
- 为CENTER Network提供业务开发，治理和合规功能，包括为消费者钱包，商家，支付收单机构等将新节点引入网络所需的业务开发。
- 提供可选的认证测试，信任授权服务，合规性审查和尽职调查计划，以允许节点所有者选择证明，维护和广播高度信任以满足法律义务并提高其他网络参与者的声誉和存在。
- 为CENTER运行的基础分布式分类帐基础架构（如以太坊）提供工程和支持服务。

这一愿景使CENTER成长为一个重要的全球组织，在全球所有主要市场都拥有业务和运营专业人员，全球合规职能部门与各地区的数字钱包紧密合作，以及重要的研发功能，继续构建和改进CENTER软件协议。
软件贡献者预计将包括来自CENTER网络成员以及全球独立开发者的不断增长的第三方开发者社区。

3.2 圈子公司背景

作为核心CENTER技术和IP的创造者，以及作为网络的创始成员，Circle的更广泛背景和领导力至关重要
到CENTER的发布和初步开发。

3.2.1 领导，投资者和董事

Circle的高级管理团队带来了经验丰富的领导者，他们在互联网技术，在线服务和银行业的领先公司中取得了数十年的成功。联合创始人Jeremy Allaire和Sean Neville已经建立了多家全球上市公司，其产品和平台有助于改造软件开发，网络内容，在线媒体和核心互联网基础设施。

Sean和Jeremy加入了经验丰富的高管和来自高盛，亚马逊，广场，谷歌，AirBnB，Expedia，eBay和Adobe等公司的广泛领导团队。
管理团队是顶级互联网技术专家和熟悉全球金融复杂性和风险的运营商的独特组合
代表全球互联网金融行业最具经验和才能的公司之一。

Circle由领先的风险投资和战略投资者提供支持，包括IDG Capital，中国最大的风险投资公司之一，以及腾讯，百度和CreditEase的早期投资者;Breyer Capital由Jim Breyer创立，Jim Breyer是世界领先的风险投资公司之一，也是Facebook的第一个投资者;General Catalyst Partners，Snap，Airbnb，Stripe和Kayak的主要投资者。战略投资者

包括高盛，CICC Alpha，百度，万象，CreditEase和EverBright Bank。

除了Jeremy和Sean之外，Circle的董事会还包括资深风险投资人Jim Breyer，Quan Zhou和David Orfao，他们帮助在美国和中国建立了一些最重要的消费者，互联网和技术公司。独立董事Raj Date带来了数十年的消费金融经验
作为Capital One和德意志银行的高级管理人员，他被美国财政部长蒂莫西盖特纳和参议员伊丽莎白沃伦招募为一个新的消费者金融保护监管机构。
独立董事
M. Michele Burns是全球领先的财务主管，曾任Delta Airlines，Mercer和Marsh McClennan的首席财务官，曾在Walmart，Cisco，Goldman Sachs（她担任风险委员会主席）和Inbev的董事会任职。独立董事Alex Norstrom是Spotify高管，负责监督Spotify订阅业务部门并带来强大的背景
消费者互联网领域的增长和营销。

3.2.2 围绕产品作为中心采用的催化剂

凭借数十亿美元的交易量，数百万客户以及不断增长的全球业务，Circle的产品可成为更广泛的CENTER网络采用的主要催化剂。

Circle目前运营着四大产品线：Circle Pay，Circle Trade，Circle Invest和Poloniex。

Circle Pay是一款全球社交支付应用程序，可让客户即时付款，无需支付任何费用，包括跨越货币和边境的即时付款。Circle Pay将开放的交叉货币交易与令人愉快的社交消息行为 – 对话，媒体和支付相结合。

Circle Pay是从区块链技术开始构建的，特别是CENTER背后的技术。该公司设想超越围墙花园的资金和价值将变得更具包容性和全球化，几乎即时，安全，并为企业和个人带来新的增长和创新形式。收取付款的费用将消失，为全球价值交换开辟了巨大的机会，包括将数十亿人带入全球数字经济。

Circle Trade经营公司的加密资产交易业务，今天是最大的做市商和OTC流动性提供商之一。世界。Circle Trade在市场上每月直接交易超过$ 2B，为大型自然买家和加密卖家提供每日流动性，以高价值交易（最低50万美元），并作为所有成熟加密的流动性提供商和做市商资产交换。

Circle Invest于2018年春季首次在美国上市，是一款面向Circle Trade的移动应用程序零售消费者的能力。Circle Invest简化了加密资产投资，特别是对那些新的投资到太空。Circle Invest拥有零佣金，即时资金访问，最低1美元。Circle Invest将在2018年期间发展其功能并扩大全球市场可用性。

Poloniex是全球最大的加密资产交易所之一。圈子设想Poloniex发展成为一个强大的多边分布式市场，可以托管代表价值所有东西的代币：实物商品，筹款和股权，房地产，创意产品，如艺术品，

音乐和文学，服务租赁和基于时间的租赁，信贷，期货等。Circle认为围绕交换任何事物和所有事物的合同规则将越来越多地体现在分布式全球软件中，依赖于分布式账本形式的不可转换的分布式共享存储器，并受益于全球多维市场的服务。

3.2.3 监管和许可证组合

加密货币和区块链技术的出现代表了自商业互联网出现以来最重要的技术突破，Circle认为与寻求了解技术并确保市场可采用的政府建立牢固的关系至关重要。
同时也解决了社会，经济和消费者面临的主要风险。正因为如此，Circle自成立以来一直专注于与监管机构的深入和高质量的合作，并拥有世界上任何加密公司最广泛的许可。

Circle是一家注册的货币服务公司（MSB），拥有美国财政部的金融犯罪执法网络（FinCEN），并持有货币传输（或同等）许可证。
美国48个州和地区。Circle是第一家获得纽约BitLicense的公司，也是目前仅有的四家公司之一。Circle还持有英国金融行为监管局颁发的电子货币发行人执照。这些许可证使公司能够在美国，英国和欧盟提供法定和加密资产存储，货币兑换和支付服务。

3.2.4 技术和知识产权贡献

Circle正在为CENTER组织贡献核心技术和知识产权。此IP是Circle多年技术开发的结果
支持消费者社会支付和加密资产交易业务。
Circle的开创性工作
建立无缝的消费者支付体验，并在底层区块链结算和集成层之上使用法定货币是CENTER的核心。其他技术创新包括用于将KYC和AML风险决策分层到支付网络中的系统和服务
交易，以及提供即时流动性和法定资产与加密资产之间转换的系统。

33 组织结构和顾问

CENTER组织将与几位关键的Circle员工一起播种，他们期望从Circle进入CENTER。这些人才包括工程，运营，业务开发，财务和合规方面的人员。

CENTER组织将得到一个强大的顾问委员会的支持，他们在互联网平台，协议和消费产品，企业发展，开放方面拥有丰富的经验
源软件，以及加密货币和区块链技术方面的深厚专业知识。

4.0 CENTER组织

CENTER工作组希望在技术同行评审，法律和合规审查，财务和税务顾问以及正在进行的工程进展期间定期更新本文。

预计将在CENTER网站上报告重大更新：
http://centre.io.

5.0词汇表

反洗钱规则（AML）：旨在阻止通过非法行为产生收入的一系列程序，法律或法规。

应用程序编程接口（API）：用于构建软件应用程序的一组例程，协议和工具。API指定软件组件应如何交互。一般而言，它是各种软件组件之间明确定义的一组通信方法。

比特币：一种网络，其中使用加密技术来规范单位的生成
货币和验证资金转移（当小写时，该术语也指货币单位而不是网络）。

CENTER：跨货币和边界，跨多种软件实施，跨多个区块链，分类账和结算轨道的数字钱包互操作性协议。

CENTER网络：由钱包提供商，服务提供商和金融机构等参与者运营的CENTER节点的连接网络。

链式状态通道：允许两个未直接相互连接的状态通道使用与其他状态通道的中间连接间接安全连接的机制。

Circle：Circle Internet Financial是创建协议初始实施的公司，它将通过IP贡献和许可帮助引导CENTER开发。

加密资产：数据和软件代码的加密单元，具有可交易资产的价值。

以太坊：一种基于开源，公共，区块链的分布式计算平台，具有智能合约脚本功能。

哈希时间锁合同（HTLC）：一类智能合约，要求付款接收方通过生成确认在截止日期之前收到付款
加密证明付款或丧失索赔的能力，将其退还给付款人。

借条：承认债务的加密签名数据。

实现：以特定软件代码的特定形式形式的协议或其他软件抽象的特定实现。
简而言之，蓝图是一个房子，因为协议规范是一个实现。

了解您的客户（KYC）：业务识别和验证其客户身份的规则和流程。该术语也用于
指管理这些活动的银行和反洗钱条例。

节点：一种软件包，用于代表网络参与者操作和管理网络参与，包括提供协议和API实现。

支付渠道：特定于比特币，小额支付渠道或支付渠道是一类
旨在允许多个事务而不提交所有这些事务的技术区块链。在典型的支付渠道中，只有两个交易被添加到区块链中
但参与者之间可以进行无限制或几乎无限制的付款。支付渠道是一类国家渠道。

协议：一套通信规则和准则。在两个或多个节点之间的通信期间为每个步骤和过程定义规则，并且节点必须遵循这些规则以成功地传输数据。可以在不同的实现中以不同的编程语言和跨不同的区块链或其他基础设施的运行时间来实现单个协议。

服务提供商：CENTER网络参与者，为网络提供服务以支持金融交易。作为代币支付的费用的交换，服务提供商可以提供合规性，KYC，身份，数据存储，欺诈检测或其他网络参与者感兴趣的其他服务。

结算：履行可能已在网络成员之间进行交易的IOU的义务。

智能合约：旨在促进，验证或执行协议谈判或执行的计算机协议。

Stablecoin：用于描述加密资产的术语，该加密资产与基础保留资产挂钩和/或由软件算法管理以实施价格稳定性。

状态通道：网络参与者之间的讨论通道，能够更新内部数据（状态），而不需要将每个这样的数据更改打印到底层区块链。超级付款渠道。

令牌：用于访问和使用网络的智能合约，它将持有者标识为网络参与者，并且隐含地按照其解锁的网络的有用性来累积价值。

交易：在CENTER中，交易是将IOU从一个网络参与者转移到另一个网络参与者。

信任级别：网络参与者的信任和认证级别的数字指示符，由该参与者的许可配置文件及其随时间的行为确定。