IOTA ($MIOTA)分析

文 Myles Snider, Kyle Samani, and Tushar Jain

2018年1月23日

披露：Multicoin Capital在IOTA中未持有任何多头或空头头寸。

介绍

IOTA是一个数字货币项目，旨在成为物联网(IoT)的支柱。外界吹捧它拥有“后区块链”架构。虽然IOTA与许多区块链项目有一些相似之处，但它的设计并不包括区块或单一的线性链。相反，它基于一个称为有向无环图(DAG)的概念。虽然IOTA不是区块链，但它的DAG仍然是一个公开的、无许可的分布式账本。由于其独特的结构，它提供了一些传统区块链的优势。

概述

背景

IOTA于2014年首次概念化，2015年由David Sønstebø、Sergey Ivancheglo、Dominik Schiener和Serguei Popov博士创建。几位创始人起初在一家专注于物联网的硬件初创公司工作，开始意识到当时的物联网在支付方式方面的局限性。于是他们创建了IOTA，希望解决这些问题。

最初的IOTA供应(2,779,530,283,277,761 IOTA)在2015年的代币销售中分配，为开发团队筹集了1,337个BTC（当时约合58.4万美元）。IOTA的供应为固定的，因为既没有挖矿回报，也没有通胀。该项目目前由总部设在柏林的非营利组织IOTA基金会开发和管理。

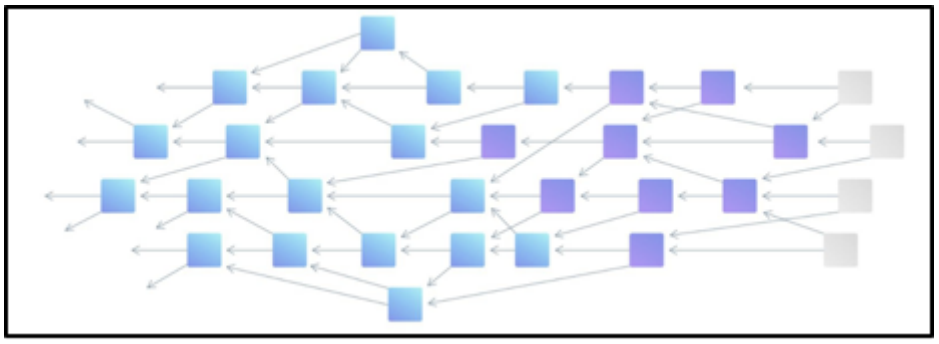
特点

缠结

IOTA实现了缠结，这是一个有向无环图。

- 图是相互连接的节点网络（在IOTA中，通过引用彼此的事务）。这些连接称为边。
- 非循环图是不循环的图；通过沿着边从一个节点移动到另一个节点，将永远不会回到以前遇到的节点。每条边都从前一个节点移动到后一个节点。
- 最后，定向意味着节点之间的连接只向一个方向移动。

这三个属性的组合意味着网络本身形成了一个节点和关系的结构，并最终收敛。这些特性可以通过数学证明，这使得网络能够创建松散结构的事务顺序，并防止在没有专用的矿工、区块或单一链的情况下出现双花。



A visualization of the Tangle

缠结的可视化

在IOTA中，节点和矿工不是彼此独立的实体；相反，每个生成事务的节点还必须通过执行一个小的工作证明(PoW)来确认之前的两个事务。用户和矿工是一回事。用户是图的节点，之前事务的确认构成了图的边缘。虽然IOTA中的事务不需要用户支付任何事务费用，但是这个小型的工作证明承担了与在其他系统中支付事务费用相同的反女巫攻击(Sybil attack)机制。

将一组矿工与网络用户分开可能是危险的。矿工有审查、抢先交易和欺骗用户的能力，他们甚至可能有这样做的经济动机。IOTA消除了这些问题，因为所有用户都充当验证者，并且他们随机选择要验证的事务子集。审查和抢先交易将不起作用，因为这些交易将很快得到其他用户的验证。

IOTA的工作原理如下：当用户希望生成一个新事务时，她必须首先使用私钥签署事务输入。然后，她的钱包使用马尔可夫链蒙特卡洛(MCMC)选择算法来选取两个她必须确认的“提示”（缠结中的未确认交易）。因为不是每个节点在任何时候都有相同的缠结状态，所以两个不同的事务可能会确认相同的提示。MCMC实际上并没有在协议级强制执行，但是IOTA团队已经发表了关于缠结均衡的研究，这种均衡甚至在“自私的提示选择”存在的情况下也是如此。为了将新生成的事务添加到缠结中，用户必须执行一个小PoW来验证随机选择的两个提示。一旦

这些被验证，用户的新事务将作为提示添加到缠结中，而它又将等待另一个事务的确认。这个过程永远如此不断重复。

与比特币一样，随着时间的推移，IOTA交易更有可能被纳入规范的分类账。在比特币中，这需要等待一定数量的区块确认（通常是6次）。用户可以通过运行MCMC算法来确定其事务的确认级别。如果算法运行N次，并且事务被确认M次，M (N)是随机选择的提示有直接路径指向你的事务的概率，因此是整个网络确认该事务的概率。那些接受IOTA作为支付方式的人可以自由决定接受最终交易的概率。随着网络的增长，到达可接受的最终结果的时间应该会越来越短，因为将有更多的事务确认以前的事务。目前，交易往往在几分钟内得到确认。

无交易费用

如前所述，IOTA交易不包括明确的费用。为了生成交易而执行工作的需求可以看作是一种费用，但是区别很重要。由于IOTA的主要目标是成为小额支付的解决方案，因此消除交易费用至关重要。交易费用会使小额支付变得不可行。比特币在早期曾被许多人誉为互联网小额支付的解决方案，但高昂且不可预测的费用使其在今天几乎不可能实现。IOTA没有试图以一种始终保持较低或更可预测的方式来设定费用，而是完全取消了交易费用。有了IOTA，一组机器可以向另一组机器发送支付流，每台机器的支付流小于1美分，无需计算或支付任何交易费用。如果发送了1 IOTA的付款，则会正好收到1 IOTA。

可伸缩性

从理论上讲，IOTA独特的设计应该能使得它随着规模的增长而扩展。事务可以并行处理，而且由于每个事务确认前两个事务，因此随着更多用户加入网络，确认的时间会减少。因为IOTA没有区块，所以它不受区块大小的限制，在每个时间段只包含一定数量的事务。但是，只有当网络中有足够数量的完整节点时，这种体系结构才会扩展。

去中心化

在IOTA中，不存在像区块链中那样矿工或验证者与用户相分离的概念。相反，每个用户在每次发送事务时都充当验证者。这是为了解决几个问题。首先，用户和验证者具有完全相同的激励机制，因为这两组实际上是一回事。用户每次发送交易时都在验证其他人的交易，由于没有区块奖励或交易费用，所以验证者没有竞争的动机。

由于去中心化通常是由控制交易验证的多方数量来衡量的，因此从理论上讲，成规模的IOTA比几乎任何区块链都要去中心化得多，而区块链的区块生产往往随着规模经济而趋于中心化。IOTA的一个问题是，由于没有费用或区块奖励，用户没有动力运行完整的节点。目前，大多数钱包都是连接到运行IOTA IRI的完整节点的轻客户机，IOTA IRI为轻客户机用户执行MCMC。IOTA过去的一些网络问题被归咎于缺乏完整的节点，随着越来越多的物联网设备加入网络

，这些问题可能会变得更糟，这些设备太小，无法运行完整的节点（它们甚至小到无法执行PoW）。

恶意行动者也有动力执行一个女巫攻击，以获得对大多数验证能力的控制，并执行双花攻击。IOTA尤其容易受到这类攻击，直到网络规模达到无法实施此类攻击的程度。因此，该网络目前依赖于由IOTA基金会运行的中心化、闭源的“协调器”(Coo)。本分析稍后将探讨协调器的结构和所涉问题。

抗量子

IOTA的另一个特性是它是一种面向未来的集成，使用基于哈希的抗量子签名，而不是椭圆曲线加密。具体来说，它使用温特尼茨签名(Winternitz signatures)。

注意，这并不是IOTA所独有的。以太坊和卡尔达诺(Cardano)社区正朝着在协议中加入量子安全加密的方向迈进。

用例

IOTA的目标是成为物联网金融体系的支柱。此外，它还集成了其他功能，如安全消息传递和数据市场。这些特性都是IOTA所设想的未来机器经济的一部分，其中数百万台机器实时交换数据和支付。这可能包括各种创新，从向充电站付费的电动汽车到全球范围内向致力于预测天气模式的科学家出售数据的气象传感器，不一而足。

IOTA适合物联网的主要特点是它没有支付费用。虽然对于这样一个系统有许多理论用例，但是**IOTA还没有找到一个真正契合的产品市场**。IOTA文档的“用例”部分很稀疏，也不具体，称“主要关注的领域显然是物联网，特别是在智能城市、基础设施和智能电网、供应链、交通和移动等领域。”目前还不清楚这些例子中的任何一个是否需要稳定的支付流，而不是一次性预付或可以定期结算的“账单”。

在某些情况下，双方互不信任，不愿在交易前或交易结束时交换付款；发送一个支付流可以让任何一方在任何时候退出交易，而不会损失大笔资金。低价值交易的整个可寻址市场目前相当小，而且可能没有足够的障碍来证明用户的切换成本是合理的。

随着联网传感器开始销售数据，或微支付网状网络等新的商业模式获得吸引力，这个市场未来有可能扩大。即使在这些情况下，IOTA也将不得不与第二层区块链解决方案竞争，如闪电网络(Lightning Network)、Raiden和概率微支付，以及其他收费较低的区块链，如EOS。

挑战

虽然像IOTA这样的DAG分类账背后的核心数学思想令人信服，但是IOTA的前景完全依赖于未来提出的具有重大技术挑战的特性。这是许多实验性加密项目的情况，但是IOTA当前的实现和它提议的功能之间的差异特别明显。

协调器高度中心化

IOTA目前依赖于由IOTA基金会运行并由其成员的多签名帐户管理的中心化协调器(Coo)。协调器的代码不是开源的。协调器被描述为其网络的"训练轮"的一种形式，一旦网络足够大，攻击在计算上不再可行的时候，协调器就会被删除。

Coo是每分钟进行一次交易的节点。这些事务称为里程碑，它们作为使用网络的其他人的有效参考点。它们本质上是可以信任为有效的网络状态快照。只要一个人的交易被Coo交易直接或间接引用，那么它就可以被认为是有效的。虽然Coo所能做的有限（例如，它不能凭空创建IOTA），但它是网络失败的一个中心点。**此外，由于交易必须得到Coo的确认才能被认为是有效的，IOTA目前的形式既不抵制审查，也不去中心化。**

需要Coo的原因是网络目前还不足以阻止攻击，因为恶意行为者仍然可以相对容易地控制34%的网络，使得他们能创建仍可被其他人引用的无效交易。攻击者只需在每个时间段内创建一定数量的事务（并执行适当数量的验证），确实事务量占该时间段内总网络事务的1/3以上。由于IOTA中没有事务费，攻击网络的唯一成本就是计算能力的成本。

Coo的另一个主要问题是IOTA团队没有就何时关闭Coo提供明确的指引。他们也没有表明该网络在实现自我可持续发展之前需要增长到多大的规模。IOTA团队最初给出的暂定日期是2017年夏季，但Coo仍在运行。

在官方的IOTA文档中很难找到Coo的具体功能。开发团队在Reddit、Slack和Twitter上的各种帖子中声称，即使是在当前的状态下，对网络的攻击也是不可行的，并假定垃圾事务邮件攻击或试图淹没网络实际上会增加确认的数量，从而使网络受益。他们还声称34%攻击需要的不仅仅是足够的计算能力。这就引出了一个问题：为什么一开始就需要Coo呢？此外，如果垃圾事务实际上有助于网络，那么似乎没有任何理由需要在事务上使用小型工作证明。该团队声称，即使有Coo，IOTA也是100%去中心化的。因此，目前还不清楚为什么Coo是必要的，以及为什么将来又需要删除Coo。

尽管该小组有上述说法，但一些潜在的攻击向量已经被确定：

- 双花攻击，攻击者将网络分成两个子缠结，然后使用多数哈希算力给无效子缠结增加权重。
- 协调器自身的双花攻击。
- 基于控制多数哈希算力的另一种双花攻击。
- 有关自私的网络使用和网络收敛的讨论。
- 有些人怀疑，即使有一个大型网络，许多小型物联网设备的哈希算力也不足以抵御拥有大型计算资源的攻击。

最后，IOTA网络在过去遭受过因攻击或bug导致Coo暂时关闭的情况。这发生在10月份，官方钱包（其只接受Coo确认的交易）有几天无法确认交易。考虑到比特币和以太坊多年来几乎100%的正常运行时间，这非常令人担忧。通过去中心化，加密网络被设计成永不崩溃。

IOTA还要求交易所在问题解决期间暂停存取款。该团队声称，网络本身并没有停止运行，没有使用官方钱包的用户仍然可以进行交易。这很难验证，因为几乎每个用户都在使用官方钱包。此外，由于这次攻击使一些IOTA用户的资金面临风险，IOTA团队决定接管这些风险资金，之后又要求用户收回他们的余额——这使其连表面上的免信任性也受到了损害。

虽然bug是不可避免的，但是IOTA团队还不清楚这个问题是由攻击还是bug引起的，以及Coo在控制用户资金方面扮演了什么角色。这是一个重大的危险信号，并进一步强调了IOTA不是一个去中心化的网络。

硬件需求

为了充分发挥IOTA的潜力，参与IOTA网络的物联网设备将需要进行某些硬件更改。正如IOTA团队所描述的那样，Curl hasher（本质上这是个微型ASIC，译注）将是硬件设备的必需组件，以便允许它们执行生成IOTA事务所需的PoW。该团队称这是一件“小事”，并表示这将成为标准硬件堆栈的一部分，因为物联网设备需要更加去中心化的账本连接。然而，他们可能是本末倒置。这很容易变成鸡生蛋还是蛋生鸡的问题；除非进行硬件更改，否则IOTA无法充分发挥其潜力，另一方面，除非IOTA成为物联网支付和数据共享的标准，否则硬件公司不会有动力添加这种新的硬件。IOTA的上市战略取决于其自身的成功，没有后备计划。

主要的担忧

网络可用性

IOTA的一个问题是出现过几次持续的网络停机。事实上，当我们第一次购买IOTA来自行测试功能时，由于网络问题，我们无法从交易所中提取IOTA。尽管交易所有时会暂停比特币和以太币的提现，但对IOTA来说，这个问题在反复出现。事实上，Github上有关IOTA的故障讨论，揭示出未确认交易、丢失资金以及无法收回基金会持有的资金等一系列持续的问题。

如前所述，在协调器临时关闭之后，网络变得不可用。据Reddit和Github上的用户称，几次“垃圾交易攻击”已经导致网络瘫痪。一次攻击被归咎于缺乏完整的节点；IOTA团队成员声称，网络在这段时间内运行良好（请参阅这篇文章的评论部分），而Reddit上的用户则持相反观点。

12月初发生的另一起攻击导致用户无法确认交易，甚至可能停止所有网络活动：

- Reddit关于垃圾事务攻击的讨论
- 社区成员要求垃圾事务发送者停止
- IOTA开发人员证实正在发生垃圾事务攻击
- Github在此期间有关未确认事务的问题讨论

几乎每个去中心化账本都经历过网络可用性有限的时期。在以太坊上，部分首次代币发行(ICO)期间，以及“谜恋猫”(Cryptokitties)处在峰值、网络满负荷运行时也有发生。然而，这一问题在IOTA中发生的频率似乎要高得多，而且与钱包余额的差异也要大得多。事实证明，很难确定哪些网络不可用期是由攻击引起的，哪些是由bug引起的。对于IOTA来说，这种区别很重要。IOTA团队过去曾声称，垃圾事务攻击实际上增强了网络，因为它们提高了吞吐量，但在其他地方（包括上面的链接），他们则否认了这一点。考虑到垃圾事务攻击已经造成的问题，目前还不清楚未来网络将如何处理这些攻击（甚至也不清楚网络如何处理吞吐量极高的情况）。

IOTA在用户体验方面存在严重问题，导致用户资金流失。例如，最近在使用恶意在线种子生成器的用户那里，有价值数百万美元的IOTA代币被盗。由于随机生成是基于种子的钱包的一个关键特性，IOTA将此过程委托给用户而不是将其内置到官方钱包软件中，这似乎是一个糟糕的决定。事实上，官方的IOTA钱包一度曾经有一个种子生成器，但是开发人员在没有官方解释的情况下就删除了它。

加密和软件漏洞

麻省理工学院媒体实验室(MIT Media Lab)数字货币计划(Digital Currency Initiative)主任Neha Narula在其发表的一份报告中，详细描述了在IOTA使用的哈希函数中发现的关键缺陷。Narula很好地解释了这个概念：

> *加密哈希函数接受任意数量的输入，并产生固定大小的不可预测的输出。它的想法是，给定一个输出，很难找到一个映射到该输出的输入；给定一个输入和输出，很难找到另一个映射到相同输出的输入。当两个输入映射到相同的输出时，就称为冲突。能够轻松地找到冲突意味着加密哈希函数被破坏。*
>
> *加密哈希函数对于加密货币非常重要，因为通常事务在签名之前就被散列。因此，如果你可以破坏哈希函数，那么你也可能破坏签名，这意味着用于确定事务是否有效和授权花费的机制被破坏。加密货币提供的数学完整性取决于这种关系的安全性。*

Narula和她的团队能够轻而易举地在IOTA的Curl哈希函数中找到冲突，这个函数是由IOTA团队定制的，因为他们使用的是三元而不是二元表示法。这违反了所谓的构建加密货币的黄金法则，即“不要创建自己的密码”。各个项目应该只使用经过同行评审且经过良好测试的加密库。虽然我们当然承认，在某些情况下需要研究人员探索新的加密技术的前沿，但在IOTA函数中发现的漏洞清楚地表明，他们本应遵循这条黄金法则。当该漏洞被披露时，团队从Curl切换到Keccak-384 (SHA-3)进行加密签名。

糟糕的决定是一回事。团队如何面对逆境则是另一回事。IOTA团队对这种情况的反应简直令人目瞪口呆。

该团队在Reddit、Medium和个人博客上发表了几篇解释（内容有时相互矛盾），最后发表了一篇文章，貌似是他们的最终回应（该文是关于该主题的系列文章的第4部分，在事件发生近6个月后发表）。在这篇文章中，该团队声称，发生冲突的可能性经过了深思熟虑的设计选择，目的是防止IOTA软件被坏人使用。使用（中心化、闭源的）协调器可以防止IOTA事务受到这个漏洞的影响，但是IOTA团队知道它的存在。他们声称，任何试图使用IOTA源代码的善意开源项目都会发现这个漏洞并更改哈希函数，但是恶意项目不会（很可能是由于疏忽）。

IOTA团队声称，他们的目的是防止用户蒙受损失、被糟糕的项目欺骗。这是一个荒谬的声明，它不仅完全违背了开源社区的精神，而且回避了IOTA团队在不知道漏洞的情况下，如何使用他们的源代码对另一个项目作出反应的问题。允许已知的漏洞持续存在，让用户承受损失，这是完全不可接受的。

我们不相信IOTA团队对这种情况所做的辩解。个人投资者可以自行对IOTA团队行为的道德影响做出自己的评估。我们认为他们的行为是有着致命的弊端，因此认为IOTA是不可投资的。此外，Sergey Ivancheglo在Reddit上对该漏洞进行解释时，拒绝承认IOTA软件中是否存在其他已知的缺陷。相反，他反对使用“缺陷”这个词，进而表示公开披露其他任何缺陷将使他们无

法抵抗“欺诈者”。“对于一个数十亿美元的网络来说，这是一个可怕的现实：IOTA团队可能可以利用这些漏洞控制IOTA网络，同时无需承担任何责任。

结论

有向无环图体系结构是一种有趣的、新颖的分布式分类账组织机制。虽然我们认为DAGs并不会令区块链过时，但它们提供的某些特性和权衡可能使其更适合某些去中心化应用程序。与分布式账本领域的许多技术一样，DAGs也处于起步阶段，基本上还没有经过测试。我们期待着在未来继续对这一领域进行研究。

虽然IOTA是首批构建DAG而非区块链的主要项目之一，但是我们发现IOTA团队采用的方法暴露出了很多令人高度关切的问题。虽然基于DAG的系统可能成为加密生态系统未来的重要组成部分，但是如上所述，我们对IOTA的DAG实现持保留意见。尤其在于：

- 明确的中心化（通过引入Coo），没有确定的去中心化时间表
- 多次网络停机
- 团队要管理用户资金时没有问责制或治理
- 故意在代码中包含一个（或多个）漏洞的决定
- IOTA核心团队对这些漏洞的解释自相矛盾
- 缺乏清晰的用例。到目前为止，我们还没有看到太多的用例需要机器对机器的微支付，而这些微支付无法通过概率微支付或状态通道来满足。

我们祝愿IOTA团队一切顺利，并希望他们能够实现自己的愿景，因为这是物联网经济向前迈出的引人注目的一步。然而，考虑到IOTA网络的现状、巨大的技术风险以及协议中存在严重缺陷的压倒性证据，我们认为，按照当前的价格，IOTA被严重高估了。截至发稿时，IOTA的市值为6,807,664,212美元，总市值排名第11位。

披露：

截至本报告出版之日，Multicoin资本管理有限公司及其附属公司（统称“Multicoin”）、对本报告做出贡献的其他人以及我们与之分享研究成果的其余人士（统称为“投资者”）可能持有本报告所涉及项目的多头或空头头寸，或拥有相关代币期权，在代币价格上涨或下跌的情况下实现收益。本报告发布后，投资者可就本报告所述项目的代币进行交易。本报告所有内容均代表Multicoin的意见。Multicoin获取的所有信息均来自其认为准确可靠的来源。但是，此类信息“按原样”呈现，不作任何形式的保证，无论是明示还是暗示。

本文件仅供参考之用，不作为任何交易的正式确认。所有市场价格、数据和其他信息均不保证其完整性或准确性，它们都基于选定的公开市场数据，并反映截至发表之日的普遍情况和Multicoin的观点，上述所有信息都可能发生变化，恕不另行通知。Multicoin没有义务继续提供有关该项目的报告。报告是按所标明的日期编制的，可能因随后的市场或经济情况而不再精准可靠。

任何投资都存在相当的风险，包括但不限于价格波动、流动性不足和潜在的本金完全损失。本报告的基本价值估计值仅代表对特定代币潜在基本价值的最佳努力估计值，并不明示或暗示为对代币质量的评估、对过往业绩的总结或对投资者提供的可操作投资策略。

本文件不以任何方式构成买卖本文件所述任何投资或代币的要约或邀请。

本文件所含信息可包括或引用前瞻性陈述，其中包括任何非历史事实陈述。这些前瞻性陈述可能被证明是错误的，可能受到不准确的假设、已知或未知风险、不确定性和其他因素的影响，其中大多数超出了Multicoin的可控范围。投资者应在专业财务、法律和税务专家的协助下，对本文件中讨论的所有代币进行独立的尽职调查，并在作出任何投资决策前对相关市场做出独立判断。