白皮书

2017年8月10日

Aion - 第三代区块链网络

Matthew Spoke
matt@aion.network

Nuco 团队
aion@nuco.io

发布版本 v1.0.0, 8 月 10 日, 2017

摘要

主流商业采用区块链技术受到限制。在本文中，我们将提出一个新的设计：Aion 网络，第三代多层系统来应对这些挑战。我们的假设核心是，在独特行业内创造许多区块链来解决独特的业务挑战。因此，Aion 网络旨在支持自定义区块链体系结构，同时为跨链互操作性提供去信赖的机制。这个系统的根本是世界上第一个公认的公共企业级区块链，Aion1; 一种引入新的安全模式，公平，并具有代表性的加密经济激励机制。

路线图

本文旨在作为技术介绍，后续将继续研究及完善设计。因此，在接下来的几个月，Aion 团队将出版一系列研究论文，更全面地解释文中提出的共识算法，虚拟机和脚本语言，桥梁和跨链交易功能的概念，以及经济体系支撑网络。此外，技术介绍之后，Aion 将发布筹款策略和时间表供您参考。我们期待您的反馈，并与您分享我们的想法。

目录

1 介绍

由于可扩展性，隐私性和互操作性方面的挑战，主流商业采用区块链技术受到限制。Aion 是第一个旨在应对这些挑战的多层次区块链网络。

在我们预期的将来大量特定为各行业配置的区块链将会陆续诞生。为此 Aion 网络设计目的旨在支持各类自定义的区块链网络。Aion 网络的核心是第一个专有的，公共的，企业级区块链：Aion-1。

Aion-1 是一个最先进的第三代区块链，是一种引入新的安全模式，公平，并具有代表性的加密经济激励机制。

本文:

- 介绍和解释 Aion 网络 - 下一代区块链技术和第一个多层区块链网络及其必要的基础设施和协议。
- 详细介绍 Aion-1 的愿景和技术概念，Aion-1，一个专用的，公共的，第三代区块链和 Aion 网络中的组件。
- 为 Aion-1 和 Aion 网络的未来实施提供路线图。

本文提及概念，旨在构建探索性的意图，而不作为声明。点此加入Aion 网络邮件列表，以获取有关 Aion 更详细白皮书的更新。

2 历史

自从 Bitcoin 于 2008 年首次推出以来，数字货币和相关的区块链技术的发展形势发生了重大变化。

2.1 第一代区块链

Bitcoin[1] 作为第一代区块链技术，率先创建了许多货币替代平台。这些区块链通过实施加密-安全，对等式网络，以及一个由全球分布式网络验证的数字交易公共账目解决了传统交易受限的问题。产生了一个应用数字化优势的平台，同时严格保障了价值的稀缺性。

2.2 第二代区块链

随着第二代区块链，以太坊引入在区块链网络上执行应用逻辑的能力 [2]。这启用了超出交易的新功能，将状态、业务逻辑和多方合同在区块链中存储并执行，并写入不可变的账本。这些概念已被纳入其它分布式账本技术，并导致了构建区块链和构建区块链上的区别。

基于区块链的应用程序的出现对于行业来说是积极有用的。创新的区块链应用进一步证明并验证了区块链技术的发展并不仅仅局限于作为价值转移的工具。然而，这些分离的网络由于相互孤立，只能通过中心化交易平台传输数据或进行价值转移。从某种意义上说，经济与工业之间微小王国的壁垒正在被构建。随着网络数量的增长，行业将变得越来越不连贯和稀疏。

正如在互联网的早期发展过程中，不同区块链网络还没有真正意识到相互连接的好处。虽然专门的区块链网络将，并且应该被开发，但是能够在链上与其它网络进行互通具有显著优点，特别是在确保隐私和可扩展性的前提下。一个可加入不同网络的机制将为每个参与的网络带来巨大价值。

2.3 Aion: 第三代区块链

在未来，区块链将在一个类似于互联网的中心和 spoke 模型中整合数据和价值。主流区块链未来采用的方向将通过开发联合区块链来实现，以整合这些单独的 spoke。这个集成的区块链网络，即 Aion。

Aion 是第三代区块链网络，将使任何公共部门或私有组织能够:

- **整合**: 在任何与 Aion 兼容的区块链和以太坊之间发送数据和值。
- **扩展**: 为所有 Aion 区块链提供快速的事务处理能力和增加数据容量。
- **Spoke**: 允许创建定制的公共或私有区块链，以保持与其它区块链的互操作性，同时允许发布者选择治理，共识机制，发布以及参与方式。

AION 网络的核心是一个独特设计的，公开的，第三代的区块链，Aion-1。设计用于连接其它区块链并管理其自身的大量链上程序，Aion-1 还提供了激励互操作性的经济系统。

AION 令牌作为整个网络的燃料可用于创建新的区块链，货币化跨链桥梁和保护整个网络的安全。

3 AION 多层区块链网络

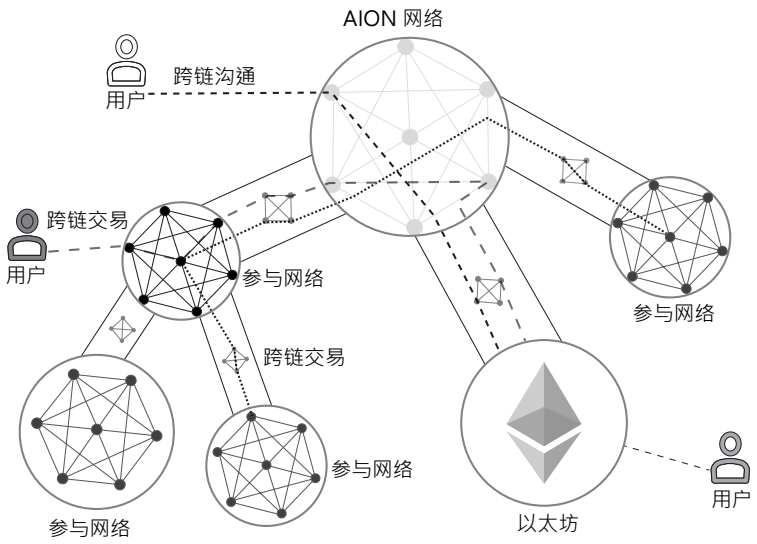

图 1: 简单的多层区块链网络，包涵所有主要参与者

Aion 多层区块链网络就像一个计算机网络，为不同的系统提供通信协议和标准来。然而，除了信息之外，Aion 网络将通过在参与的区块跨链传递逻辑和价值来创建一个连续的价值链，其中每个交易都发生在链上，逻辑和价

值像流动资产一样在跨链自由流动。

这些基础设施，协议和概念将一起工作，以确保跨链通信从始发到目的地的传输。这些技术的价值在于它们使一个区块链与另一个区块链交互，以及一个区块链与多个连接的区块链进行交互。

3.1 连接网络

连接网络是促进多个私有或公共区块链网络之间的跨链通信和跨链事务的网络。连接网络由在 Aion 上下文中指定的角色要求来定义连接网络和跨链事务提供了通用接口，使区块链开发者和用户能将消息从一个网络路由到另一个网络。具体来说，连接网络应提供以下核心功能：

- 通过通用桥接协议在不同的区块链网络之间路由消息，该最终协议涉及消息的转换和传播。
- 提供去中心化的问责制。
- 提供桥接协议。

Aion 网络协议规定了外部组件的标准。虽然每个连接网络的实际功能和内部组件可能因供应商和预期目的而异，但是这些核心功能应该被实现。

诸如跨链交易中继或 BTC 交易中继的点对点连接作为中心集线器存在。这样的协议虽然简单而有效，但往往导致复杂的状态可能引起争议，并且经常会依赖于运维中继网络的人员。

连接网络代替使用网桥和去信任的区块链网络来验证并确保流动交易的正确性。通过引入第三方将消息从 A 点路由传递到 B 点，而网络本身不存在管理困难或不清楚的情况。

3.2 跨链交易

跨链交易是区块链网络之间的去信任消息，这是一个关键的基础设施组件，用于链路间通信。跨链交易允许任何已连接的区块链网络交换信息，如互联网上的计算机。

跨链交易最初是在源块上创建的，然后在最终到达目标区块链之前通过桥梁和连接网络进行处理和转发。如前所述，跨链交易的创建者必须使用 AION 令牌为通信支付交易费用，从而激励每个交叉点的参与者。

跨链交易从源块到目标网络的设计类似于数据包，即可通过多个连接网络。

3.2.1 格式

理想情况下，跨链交易格式将包括三个部分：

- 创建者特有的有效，通常是 **常规事务数据**，但可能会由创建者和源网络自行决定扩展为任意数据。
- 关于包含路由信息和费用的链路间交易的 **元数据**。
- **Merkle 证明**仅在发件人绕过桥梁时使用。

桥梁和连接网络验证者可不解释载荷数据，而是检查整个交易的完整性。如果需要，隐私敏感信息应用程序可以选择加密数据。

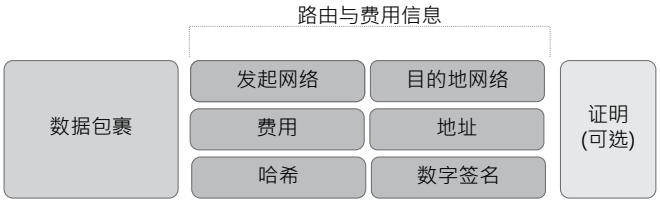

图 2: 跨链交易的视觉描述

3.2.2 路由

跨链交易的路由是一个多阶段的过程。在每个阶段，验证者验证交易，并就交易是转发还是被拒绝达成共识。如果一个交易在任何时候被拒绝，则任何由于跨链交易而导致的状态改变将被撤销，至少在连接网络中。路由路径可以分为两个子路径：前向路径和后向路径。在前向路径中，跨链交易从源链一直流向目标链。在后向路径中，跨链交易的确认被传回。

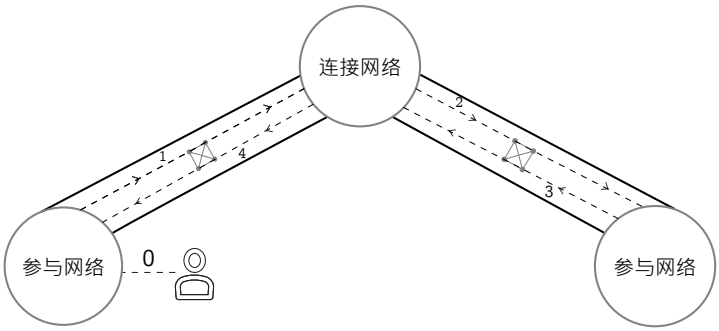

图 3: ICT 生命周期，由链 A 发起，得到确认后终止

如果桥梁由于任何原因拒绝广播跨链交易，则发送方可以选择将包括证据在内的跨链交易直接传递到连接网络。连接网络将基于参与网络的 merkle 哈希值来验证跨链交易，如果有效则将其广播。

跨链交易的设计仍在考察之中，随着项目进展，将出版关于跨链交易运作的详细文件。

3.2.3 条件

从连接网络的角度引入交互状态来表示跨链交易的不同阶段/状态。

- 当第一次参与网络中的桥梁验证者观察到跨链交易时，状态将更改为接收。

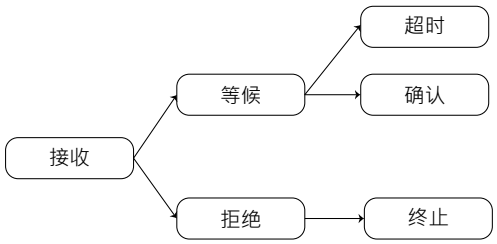

图 4: ICT 生命周期内状态转变

- 如果超过三分之二的桥梁验证者对于跨链交易投票为对，则连接网络将将跨链交易的状态更改为保持状态，这将触发事件，其中相应的连接网络令牌将被锁定，直到交易处理为止。
- 如果不到三分之二的桥梁验证者为跨链交易投票，状态将被拒绝。
- 保持状态的交易将由连接网络和路由上的下一个区块链的桥梁验证者转发。
- 从目标区块链接收到确认后，状态变为确认。
- 如果没有收到确认，状态将更改为超时。
- 对于确认的跨链交易，状态变更确定，所有锁定费用分配给连接网络和桥梁验证者。

3.3 桥梁

桥梁是通信协议，有助于参与网络和连接网络之间的通信。桥梁由自己独特的验证者网络组成，提供交易的问责和确保协议被正确执行。

桥梁是定向的; 源块链是发送交易的链，目标块链是交易到达的链。

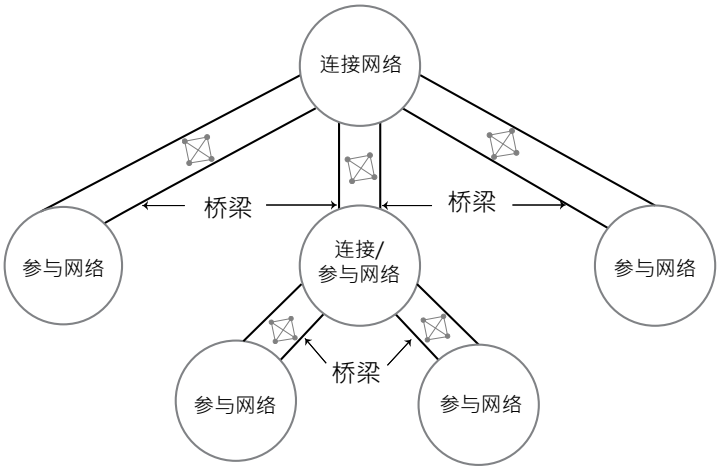

图 5: 桥梁与连接网络关系俯视图

桥梁有两个主要职责：* 签署并转发已被源区块链收录并支付了跨链通信费用的跨链交易 * 通知连接网络参与

网络的 merkle 哈希值更新。

桥梁验证者将使用基于轻量级 BFT 的算法来达成共识。交易仅在收到三分之二以上的总票数（加权）后才获得批准。

3.3.1 注册

连接网络负责注册其直连桥梁。对于每个桥梁，一个专用的验证者表将保留在区块链上，按照股权排序。任何人都可以参与公共桥梁。具体来说，合同或协议的目的是保持一个全局的桥梁注册，随着节点加入或离开桥梁网络动态更新。

达到了最低股权注入的桥梁才被认为是有效的。投入最多的验证者才能参与桥梁共识。

3.3.2 竞争

当多组验证者使用不同的标识符注册同一个区块链网络时，可能会产生多个桥梁。从连接网络的角度看，这些桥梁是不同的，尽管它们向同一个网络传播和接收消息。

因此，用户有责任通过指定目标网络标识来确定要使用的桥梁。这里的目标是通过激励不同的桥梁网络在稳定性，声誉和价格方面进行竞争来推动开放市场，以市场需求驱动最优费用为目标。

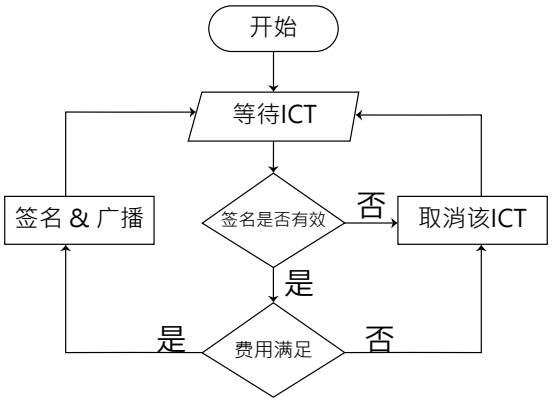

图 6: 桥梁验证算法流程图

3.3.3 桥梁共识

桥梁验证者通过遵循轻量级的基于 BFT 的协议达成共识，其中交易处理一轮而不是多轮。每个验证者根据它们对前一个区块的视图来评估一个交易。如果三分之二或三分之二以上的验证者投票为是，则跨链交易被视为有效，此时下一个区块链认为交易有效。

从开始状态开始，需要桥梁验证者等待，直到接收到跨链交易，然后验证签名和交易费用的有效性。根据交易的有效性，它将被验证者删除（未签名），或签名并传播到连接或目标网络。

3.3.4 费用分布

桥梁验证者可以从跨链交易费中得到奖励，并可能获得区块奖励的一部分。费用分配的目标是公平的分配政策。在内部，到桥梁的所有费用都分配给桥梁验证者。这可以按照每个验证者放在桥梁上的比例完成，也可以均分完成。

在外部，桥梁与路由路径上的其他桥接器和连接网络验证者共享跨链交易费用。外部费用有两种可能的分配模式：

- 跨链交易的发送方指定了网桥与连接网络之间的费用分配。这种方法的优点是用户可以选择根据桥梁负载和最低费率优化费用。缺点是在发送交易之前，用户需要基本了解每个桥的路由路径和费用要求。
- 发件人仅根据协议或硬编码协议规定总费用，网桥和连接网络共享此费用。该方法的优点是对用户更简单。这种方法的缺点是，如果不是很难，改变桥梁和连接网络之间的比例是缓慢的。

3.4 参与网络

Aion 网络设计的核心概念之一是它专用于兼容区块链或区块链相关网络的联合。这些可以是特定的区块链，私有网络或联盟区块链。无论上下文如何，以更有效、更安全和更透明的方式相互联系和相互操作以至逐渐增加了每个网络的价值，并为区块链生态系统提供稳定性。

参与网络是成功实现与连接网络集成的任何网络。参与网络应该是区块链，但不一定局限于此。参与者可能是 oracle，cryptlets [3] 或可验证信息的数据库集群。唯一的限制是参与网络与连接网络集成的灵活性。一旦与 Aion 网络集成，参与网络可以访问先前指定的通信协议（跨链交易），从而实现许多可能的用例。

参与网络具有完全灵活性，可以自定义其区块基础设施的不同模块，包括共识算法，散列算法，虚拟机（VM）和脚本语言。

3.4.1 符合 AION 标准的区块链

符合 Aion 协议的区块链是指通过 Aion-1 可以轻松地建立桥梁来转发跨链交易的参与区块链。

要符合 Aion 标准，区块链必须满足以下要求：

- 在一定程度上是去中心化的，并且支持常见的区块链规则，如原子广播（atomic brodcast）。确切的实现由桥接协议和网络本身决定。
- 能够识别与常规交易不同的跨链交易。
- 能识别桥梁所用的共识协议和储存共识的合法交易。
- 实施锁定时间或类似功能，允许令牌由网络持有一段时间。

区块链供应商将符合 Aion 标准的要求。Nuco Blockchain 基础设施将成为首个符合 Aion 要求的网络。

随着项目的进展，更多具体细节将被发布。

3.4.2 现有网络兼容性

与 Aion 兼容的区块链不同，现有的区块链并不具备互操作性。为了实现 Aion 网络和现有区块链之间的跨链交易路由，需要额外的假设和/或妥协。在本节中，我们将讨论以太坊区块链连接到 Aion 网络的可能性。

3.4.2.1 AION 至以太坊

作为桥梁协议的一部分，桥梁验证者使用基于轻量级 BFT 的共识算法。在连接网络中，这些 BFT 投票由区块链验证者聚合处理。以太坊区块链没有这个内置的功能，所以它需要一个支持此功能的智能合约。

在这个模型中，根据 Aion 网络规范，支持此功能的智能合约将定期同步桥梁验证者的公钥。当请求一个跨链交易时，桥梁验证者使用私钥对其进行签名，并将签名发送到支持此功能的智能合约。合约将收集所有投票（签名），并提供包含跨链交易数据和投票信息的可证明记录。如果已经收到至少三分之二的投票，桥梁验证者将在确认交易间交易时使用该记录作为证据。

由于多重签名验证的计算成本高（在以太坊中，单个 ECDSA 签名验证需要 3000 个 ether），因此预计可以获得较高的桥接费用。为了降低这个成本，在桥梁中可以使用具有完全 BFT 功能的区块链，只有投票结果将存储在以太坊区块链中。

3.4.2.2 以太坊至 AION

由于以太坊可编程的特性，从以太坊区块链块传送跨链交易到 Aion 网络更为简单。跨链交易可在数据字段中包含所需的路由信息。

根据接收地址，从以太坊跨链交易（从以太坊区块链到 Aion 网络的跨链交易）可发生两种可能的情况。如果交易发送到外部拥有的帐户，则可以使用数据字段而不进行修改。如果交易发送到合同帐户，因为数据由以太坊虚拟机解释，所以需要对数据进行封装。当合同逻辑不依赖于 `CALLDATASIZE` 操作码时，一种解决办法可在跨链交易的原始数据上附加标签和路由信息。

桥梁可能需要额外的区块确认来确保交易的最终确定; 主流交易中心通常需要 120 个区块确认（半小时左右）。

4 AION-1 区块链

Aion-1 区块链是连接网络的第一个实现。它被设计为一个公平的，分布式的，开放的区块链框架，能够满足多层区块链网络架构的规定。作为一个开放的区块链，Aion-1 的设计有以下目标：

- 通过去中心化网络的可靠通信以及连续网络，连接区块链和外部服务（例如，oracle 和数据库）
- 提供必要的基础设施来开发高性能，分散式的跨链应用。
- 通过强大和可持续的经济模式创建可维护的网络。

用户将能够部署适合自己的参与网络，并通过可靠的路由架构与其它网络进行通信。无论是大型企业托管的私有网络，还是面向社区的公共网络，都可以连接至 Aion-1。未来，去中心化应用程序可以处理和整合来自多个区块链网络的数据。

此外，Aion-1 区块链配备了一个全功能的经济系统，旨在推动网络的持续维护和完整性。

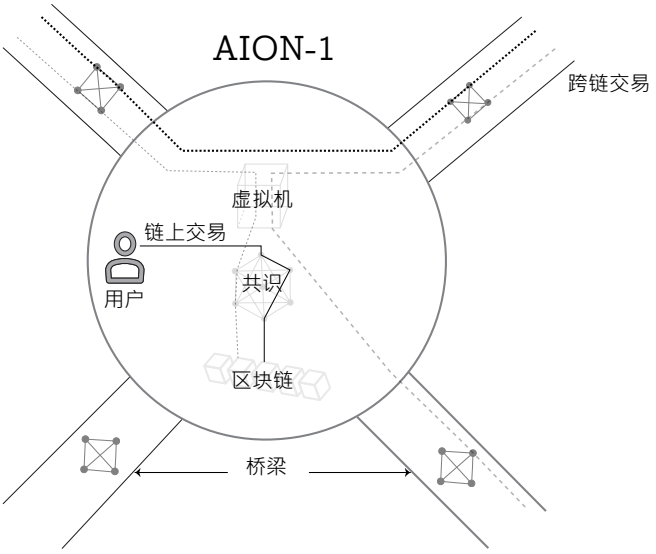

图 7: AION-1 架构鸟瞰图，网络组成：连接 [网络架构]，共识协议和虚拟机上的应用

4.1 高阶概览

在本文中，Aion-1 是指连接网络的首次实现。Aion-1 同时也是一个采用了当前区块链领域的最先进技术的功能齐全的区块链架构。我们设想 Aion-1 是一个标准化模板，为未来的网络实施提供了基础。Aion-1 区块链的关键组成部分包括：

- 将使用 **共识**来实现连接两个或多个区块链的架构。将设计 BFT 协议的两个变体，以便在桥梁和连接网络上达成共识：
  - **桥梁共识**是一个轻量级的变化，可以在桥梁上快速达成共识。
  - **连接网络共识**是一个共识协议，重点是提供规模稳定性。
- **Aion 虚拟机（AVM）** 是一种定制的，轻量级的，性能稳定的 VM。该虚拟机采纳了 Java 虚拟机（JVM）的关键特性，并为区块链环境提供了可并发性和坚固性。AVM 负责在 Aion-1 之上运行应用程序。AVM 也将自主拥有脚本语言（下面将进一步描述）。

4.2 共识

我们首先探讨 Aion-1 中的共识算法，旨在解决连接网络的要求。该共识算法需同时支持链上交易和跨链交易的共识。为了以有效和不变的方式满足这些要求，Aion-1 将使用基于拜占庭容错算法的共识算法，并结合混合协议，

其目的在于公平支持两方代表：部分通过令牌系统，部分通过基于现代神经网络中使用的新颖验证算法的智能证明。

为了满足运营规模并能够广泛参与网络验证过程，Aion-1 将采用类似于 BitShares 团队 [4] 和 Lisk[5] 的委托模式的代表性验证模型。这种验证模型将使 Aion 网络参与者能够支持积极参与共识的验证者，从而大大增加参与度，超出传统的 BFT 算法技术上允许的范围。基于 BFT 的协议的具体细节尚未确定，但保证活动性和安全性的标准属性。因为网络应该激励选择最优和正确的验证者，所以这些假设由代表性选择方法补充。我们正在研究当前的一些 BFT 提议，如 HoneyBadger[6]，Tangaroa[7] 和 Stellar[8]，尤其关注 HoneyBadger 中的提案行为和 Stellar/Tangaroa 协议中的选举协议。

代表性网络验证背后的概念设计源于代表民主制，候选人通过从选民获得的投票来让自己获选。不同的是，在这个系统中，验证者必须得到支持者的支持，同时每个支持者都会收到区块奖励的一部分。这种设计背后的理由是相信网络的自治，网络的集体行动直接通过适当的投票影响网络的安全。

总而言之，所提出的共识协议是，网络中的每一个节点都可以自己作为候选人并向候选人提供支持。在每个时期开始时，获得最高支持的候选人被选定为这个时期的验证者。这些验证者通过基于 BFT 的协议为区块链生成过程做出贡献，并通过这种方式获得区块链分配的奖励。这将持续到期限结束，下一个时期开始，重新启动此过程。

4.2.1 定义

对于本文中所以用的代表共识的定义的理解，请参阅以下一组定义：

- **提名**是一个节点注册成为验证者，在 Aion-1 上参与代表共识的过程。提名必须在网络中的任何其他用户能够承诺支持之前完成。
- **排名**用于确定具有最高支持的验证者。这个排名列表是一个动态的集合，这意味着选举人节点可以对共识过程作出投票。
- **动态集合**是动态验证者的分层列表。动态集合中包涵验证者。
- **备份集合**构成动态的候选验证者，但不在动态集合中。备份集合是下一个获得最高支持的验证者。在发生恶意行为或不活动的情况下，网络会看到此替换验证者。
- **支持者**是指支持验证者的节点。网络上的验证者将会有更多的支持者，他们的参与直接影响到动态集合中验证者的排名。此外，支持者根据其验证者的奖励比例进行奖励。支持者由两个不同的小组组成：权益者和解算者。
- **权益者**是使用令牌作为承诺支持验证者，是支持者的子集。
- **权益者的令牌**由网络锁定一定时间，直到它们在预定义的时间被释放回权益者为止。
- **解算者**是使用智能证明来解决网络提供的算法问题的用户，然后将证明转为支持，是支持者的一个子集。
- **时期**是网络为了基于 BFT 的共识而使用静态集合定义的持续时间。在每个时期中，一组静态验证者验证新的区块。在每个时期结束时，动态集合被冻结并根据利益变化生成新的静态集合。

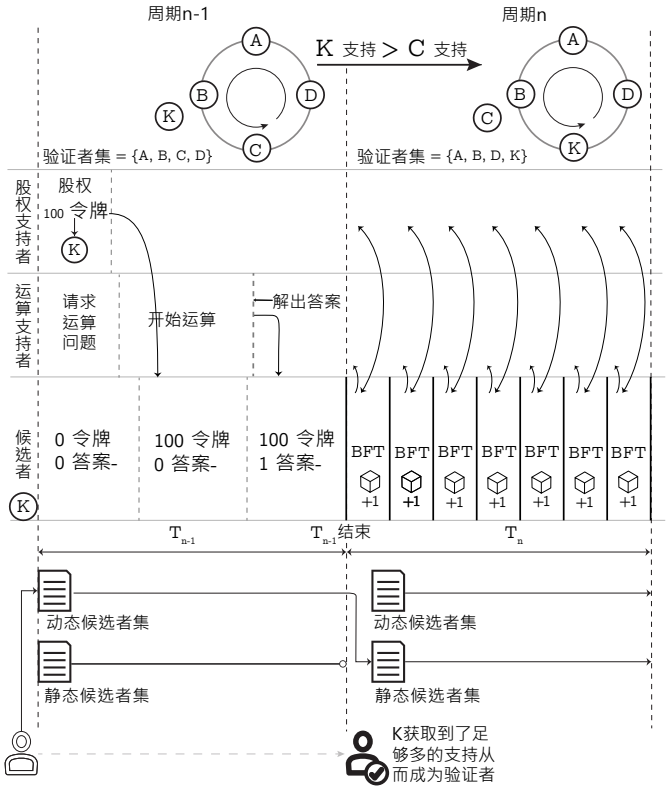

图 8: 动态 / 静态候选者集合 & 权益周期，以及候选人参与共识的过程

4.2.2 验证者提名程序

任何节点都可以自提名并注册成为验证者，但是它们需要足够的支持才能在 Aion-1 上激活。网络维护并及时刷新验证集合，使用提名合同。

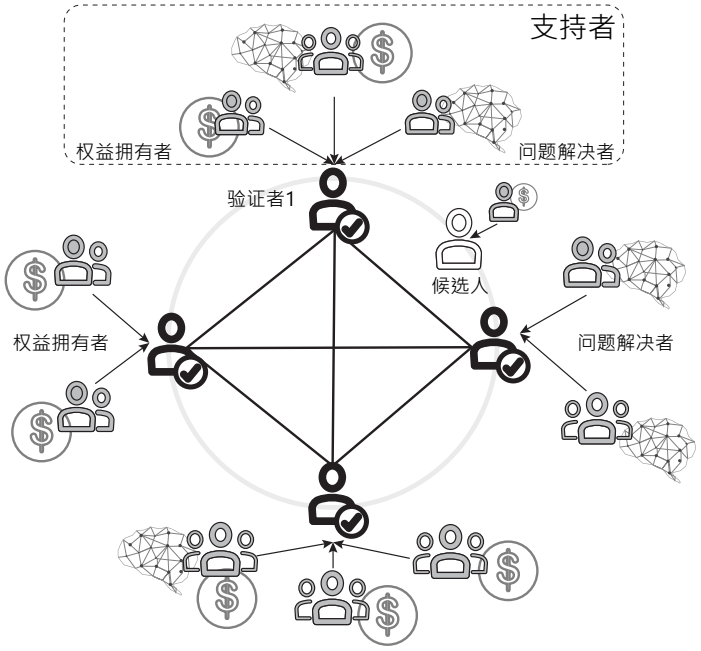

图 9: 代表投票结构: 该图描述一个进行时的投票集合，每一个验证者被支持者通过权益或问题解决支持。候选人则需在新的轮换时拥有具备足够多支持成为正式验证者。

验证者通过网络的持续支持变得活跃。动态集合的成员始终是最高支持的候选人。为了促进这种持续的支持进程，任何时间点都有两份提名合同。网络用户返回或撤回对候选人的支持，以及静态集合的存在仅在该时期内。共识协议从静态集合中派生其动态集合。在每个时期结束时，静态集合在下一个任务期间被动态集合替换。

验证者可自定义如何补偿他们的支持者。因此，验证者提出其支持条款，如果这些条款被同意，则支持者将向该验证者提供资源。这会产生一个平衡的影响，因为一个有效的验证者的排名（和随后的奖励）是基于它与其他验证者支持量的比对。

同时，Aion-1 也将提供一个验证者节点声誉机制。候选验证者可以将其声誉作为吸引初始支持者的一种方式。声誉的具体内容还在研究中。它们将是定量的，可衡量的和明确的。目的是鼓励所有参与者考虑成为候选验证者，以及使用 Aion-1 网络作为其固有效用。

4.2.3 验证者-支持者奖励分配

所有用户被视为有效候选验证者的条件是向网络提供一定数量的权益。然而，验证者的奖励不一定与他们的权益成比例。相反，验证者在向提名合同提出建议时，提出验证者和支持者奖励的比例。这个想法旨在让支持者和候选人验证者对市场价值达成一致。

4.2.4 分层活动集

在动态集合中，验证者将被组织成分层结构。分层结构对验证者按支持量从高到低进行排序。每一层通过提供更高的奖励作为报酬进一步激励良性行为。这个想法是通过引入成本效益平衡点来鼓励权力下放以达到去中心化，从而激励多样化的支持者。

表 1: 每个验证者所在层的奖励金额（%）和投票权利（%）。假设 $|n_{set}| = 100$

层	验证者	奖励 / 验证者	投票 / 验证者
1	10	2.5%	1%
2	20	1.25%	1%
3	30	0.83%	1%
4	40	0.625%	1%

这种设计将通过参与者之间的互动激励优化和良性行为。验证者将会接受更高的支持，支持者将从支持验证者中受益，但只有通过多样化支持来获得报酬，包括支持无效验证者。一个潜在的奖励分配方案如下。参考表1所示的奖励计划，奖励在层级（25%）中平均分配，然后分配给这些级别的所有验证者。更高层级的验证者由于限制层次的大小而具有较高的比例奖励。预定义的奖励介绍了支持者的经济模型，以评估支持验证者的机会成本，从而激励支持者在多个验证者（去中心化）之间分配他们的股份，甚至提名自己作为验证者。确切的激励模式和结构将进行严格的模拟测试。

4.2.5 支持

支持是指向特定验证者标记令牌或智能证明。该网络被设计为一个混合网络，强调各方在网络上均匀分配解算能力和货币价值的双重性。在一组特定的个体中，纯粹的基于权益的网络（权益证明）创造了货币价值集中。因此，另一个机会被强调，即对没有货币价值但参与到网络贡献的用户的纳入。

支持的算法分为两个不同的类别：

- 通过资金权益支持
- 通过解决问题支持

这两个因素结合起来产生支持，这个中间概念用来确定验证者的排名，以及给予支持者的奖励比例。在以下部分中，讨论了每个算法，并调查了这三个变量之间的相关性

4.2.5.1 通过资金权益支持

通过将令牌标记给特定的验证者来完成令牌支持。在 Tn 期间，用户可以向某个验证者 K 发送令牌。直到 Tn+1 结束，令牌被网络托管，Tn+1 结束时令牌被返回给用户（没有发生恶意动作）。在此之前，用户可以发送另一个消息表明他们希望令牌保持标记在相同的验证者 K 上。

更新支持，指的是保持支持于同一验证者。令牌产生时间也可能是一个有用的机制，这里的权益有一半的生命。这将鼓励流动性并维持验证者之间的竞争。作为回报，支持者收到验证者奖励的一部分。奖励与被放置的金额和现有的验证者的分层成正比。

4.2.5.2 通过解决问题支持

另一种形式的支持是通过解决一个神经网络问题来完成的，其详细定义在智力证明中指出。每个请求产生一个独特的难题，必须通过智能验证 算法来解决问题，以产生智能证明。然后将证明提交给网络，作为对特定验证者的支持量的证明。解算者也按比例奖励金额。

4.2.5.3 作为资金权益和解决问题的功能

为了激励混合网络，需要确定权益和智能证明的分配比例。这个比例目前被任意设计为 60/40（权益 / 智能证明）。每个时期累积的权益和解决方案总额和支持比例持续调整直到与预期比率一致。因此，具有比预期比例更大的比例导致每权益/智能证明的加权值下降，而比预期的比例更小则导致加权值上升。

4.2.6 激励

本部分提出的系统旨在减少不良行为，但并没有绝对制止这些行为。在这些行为发生的情况下，验证者将被降级或从动态集合中移除，并被拒绝参与共识过程。其支持者也不能得到任何奖励。

通过支持方式，来阻止恶意的支持者。网络造成的结果是消除被奖励的机会，而不是通过删除或重新分配其它验证者来惩罚。总之，当其中一个人的损失是另一个的获益时，这种机制消除了零和收益。相反，它调和动机，鼓励积极的集体行动。在这个制度到位的情况下，人们理解他们行为的后果，与其他善良行为者保持一致，并被激励以良性态度行事。不良行为者将被网络识别，并通过验证者的声誉和支持的降低，立即收到反馈并采取纠正措施或从动态集合中被删除。

表 2: 惩罚体系流程。假定位于首位的成员因违规被移除共识机制，其他代表向前移位，候选人将补位成为代表。

动态集合成员	之前回合	当前回合
1	1	移除
3	2	1
3	3	2
4	4	3
动态集合结束		
5	候选人	4

- **重复行为**通过锁定验证者提交的所有权益一段时间，并立即将验证者从共识中删除来对其进行惩罚。验证者的支持者根据他们支持验证者的方法受到惩罚。通过锁定权益来惩罚权益者。通过从共识中移除结算者

使得智能证明实效来惩罚结算者。
- **不活动**验证者在一段时间内的不活动则受到层级体系中的降级惩罚。如果无效验证者处于最低级别，则立即从共识中删除。

替换验证者（排名最高的）并将其立即转入共识过程，直到期限结束。

4.2.7 声誉

代表性共识决定了选择最佳验证者节点的义务在于网络。如果网络没有具备观察候选人和主动验证者过去行为的机制，这个过程是很难实现的。一种替用方法是依靠外部统计来选择最佳候选人。但是，会造成操纵这些数据的动机。因此，需要在网络内建立信誉系统，其中节点的过去动作和统计是网络协议的一部分，提供去信任数据以允许用户选择其适当的候选人。可以包含在节点信誉中的功能包括：

- 正常运行**时间**是节点在网络上活动的时间量，并且在确定节点的年龄（可靠性）时很重要。
- **总支持**是在该时间点之前收到的支持的总计或总支付总额，并且在每个时期结束时（在该持续时间内被锁定）汇总，可以用来评估节点的过去绩效。
- **向心性**在与社交网络中相同的上下文中使用，可以用来评估哪些节点是网络中最佳连接的节点，并且是评估可靠性和性能的有效指标。
- **交易起始**是指出现在网络上的第一个（被区块链接受的）实例交易，可容易计算出节点签署交易时发出的要求。
- **网络信任**是特定对等体的全局网络值，指示对等体从网络的每个角度的令人满意的行为。这是最初设计用于 P2P 文件共享系统 [9]，并且具有可以适应于考虑与我们的用例相关的参数的算法。

用户可以通过互联网自由地访问这些统计信息。拥有掌握 Aion 一切信息的用户群对于形成民主网络的基础是必要的。

最后，声誉系统作为一个机制，说明了节点对网络的投资。这种投资受到节点的良性或恶意行为的影响，并且在评估支持风险方面是有效的。

4.2.8 智能证明

智能证明是通过要求参与者在 Aion-1 中进行人工智能（AI）计算的方式来阻止服务攻击的经济措施。目的在于激发未来可用于机器学习和神经网络训练的 AI 特定或专用硬件的创建。

4.2.8.1 机制

智能证明通过要求参与者训练预定义的神经网络，使得它将输出与期望值相似的结果（例如，将前 N 个区块的哈希值作为输入，将当前区块哈希值作为期望值）。经过训练的神经网络的参数将作为计算证据，可以较容易的对输入参数和确认结果进行验证。

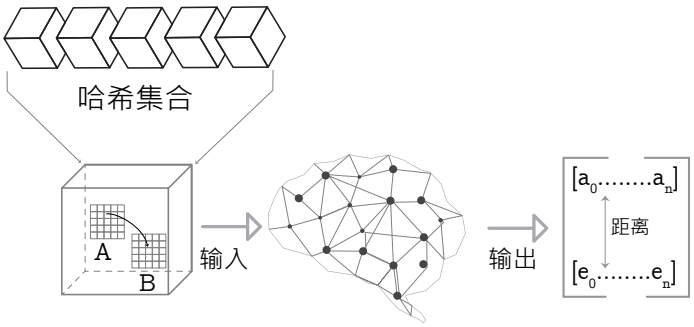

图 10: 智能证明算法

4.2.8.2 验证

与训练过程相比，证明的验证过程是快速的，主要包括以下步骤：

1. 按照提供的参数向量加载神经网络。
2. 把先前区块的哈希值作为输入，提供给改神经网络。
3. 运行并收集输出。

此验证过程正在研究和开发中。

4.2.8.3 汇集

通过将参数空间分为子空间来实现智能证明的汇集。类似于每个矿工在一个范围的随机空间上工作的工作证明的汇总概念，智能证明解算者在参数子空间上独立工作。他们分享证明和阻止奖励。

4.3 Aion 虚拟机 (AVM)

AVM 架构被设计为一个特定的区块链的解决方案，其重点在于性能，确定性和稳定性。AVM 是一种定制的轻量级 JVM 实现，适用于在分布式网络中执行链逻辑（应用逻辑），并对在这种环境中出现的场景进行强化。

AVM 是 Aion-1 连接网络的核心组件之一，它提供了对区块连逻辑的抽象，并支持跨链应用。此设计选择的理由和其它考虑因素将在下一节中进行扩展。

4.3.1 实现

在仔细考虑实际和技术目标之后，AVM 架构的核心是轻量级的，机器友好的，为区块链设计的字节码解释器。具体要求：

- **性能**通过使用一组机器友好的指令。

- **稳定性** AVM 的稳定性，通过使用隔离的 VM 沙箱环境实现，并仔细测量计算和重新使用。新的 VM 功能将通过一个正式的功能要求和规范程序，这意味着在迁移到生产环境之前，新功能已经被详细记录和测试。
- **确定性** AVM 的确定性，通过全功能区块链 SDK 开发进行保证，作为任何常规 SDK 的替代品。拟议的区块链运行时环境将以确定性作为主要目标构建。Aion VM，仅支持在本机和字节码上下文运行环境中的 Aion 区块链上构建的功能。
- **兼容性**旨在提供向后兼容，这意味着随着虚拟机基础设施的发展，链逻辑总是有效和可执行的。
- **工具**现有的字节码分析工具也可以适用于 AVM 字节码。利用这种互操作性允许适用于关键任务代码（如链逻辑）的工具。

AVM 利用现有的重要研究和开发工具。另外，使用对机器友好的字节码使链逻辑可以非常有效的执行。

定制意味着为计算资源使用计量和与主机（网络，文件 I / O，未过滤的系统数据）隔离的轻量级 VM 配置（在后续部分中说明）。孤立的环境将确保没有关于主机的有意义的信息，并且没有未过滤的（非 oracle）通信发生在链逻辑中。这对于确保主机的安全性和链逻辑的决定性至关重要。

希望实现程序的用户必须提交必要的交易数据（由一些二进制接口定义）。在收到消息后，链成员调用 start () 来启动序列，并通过 accept（data）接受数据。随后逻辑处理数据，修改其状态，返回对网络的响应，并调用 stop () 来关闭序列。

4.3.2 有限计算资源使用

运行在可公开访问的环境之上的 VM 中的关键问题之一是如何及时地制止恶意逻辑执行的可能性。当使用图灵完备的语言时，必须设置一个消耗性预算机制，使得执行逻辑不能无限期运行，或者阻止可能损坏主机或以故障定时行为扰乱共识机制的行为。具体来说，我们将预算机制定义为有限消费，其中分配的值由执行逻辑，空间和带宽消耗指定。

逻辑执行将有效的发生在隔离或沙箱环境中。在我们的上下文中，使用是指分配给特定链逻辑的 CPU 使用量。空间是指执行逻辑启动的内存分配。这样可以防止使用大量内存的代码执行。带宽是指 VM 的输入和输出消耗。通过这些机制，执行逻辑的用户将有效的租用 VM。

协议规定使用此机制需要用户精确地指定给予 VM 的资源量。从这里可能会发生两件事（两者都产生响应）：

- 成功的逻辑执行和后续响应
- 逻辑执行中的异常，通过超过提出资源边界或通过逻辑本身

在逻辑执行中出现异常的情况下，AVM 将通过 ERROR 响应通知网络事件。

4.3.3 面向区块链的并发模型

区块链网络在传统上被认为是串行的; 序列变化的状态和产生的交易为共识提供所必需的确定性。然而这也让特定时间内所要处理的交易量成为了性能瓶颈。解决这个问题在于交易并行的概念。特别当交易的实现需要上下文提供给他们所需的状态信息。如果这个定义被公式化，那么一个交易调度器的实现将允许并行交易执行。

从 AVM 的角度来看，需要支持程序级并发，并行处理多个链逻辑程序。为了实现这一目标，AVM 被设想为可扩展的，自动将多个 VM 和调度合同聚类并以确定性方式来处理。

4.4 脚本语言

Aion 脚本语言用于编写 Aion-1 和潜在的任何连接/参与网络上运行的链逻辑。Aion 语言编译成 AVM 字节码并由 AVM 执行。Aion 语言提供以下功能：

- 防御性编程
- 区块链运行时环境
- 区块链上下文注入
- 安全性

4.4.1 产品规格

Aion 语言符合 Java 语言规范的一个子集，并针对区块链逻辑。为了实现这一点，现有的字节码将被检查并且可能被重构以适应给定的上下文。

另外，Aion 语言规范包括一个区块链运行时/开发的工具包（BRE / BDK）。其目的是为开发者提供高度优化的开发库来实施区块链上特定的功能。这些包括但不限于发送交易，触发事件，检索区块链相关数据以及链逻辑应用之间的通信。此运行时环境被用来在通用计算目的的环境中替代常规开发工具。一般来说，这种语言的用户可期望相同的句法结构，但完全独特的开发工具包。

4.4.2 防御型编程

防御性编程将由 Aion 语言支持。根据过去的研究 [10]，链逻辑开发人员的错误是由于输入意外的数据，以及重入时运行时异常而导致的。Aion 语言将提供减少这些常见错误可能性的机制。机制包括：

- 在将其传递给链逻辑之前，Aion 验证输入数据，并在执行后验证输出数据。
- 脚本语言提供前提条件，后置条件和断言，以帮助程序员将其思想清晰地组织成一种防御模式。
- 链逻辑支持完全支持 try/catch 异常，并强调应用程序应该主动处理异常而不是让状态更改撤消
- 在运行时检查数组访问的边界。

这些工具提供了指导开发者思维方式的手段，在发现不受保护的代码的领域添加警告和最佳实践。其他功能也将在未来考虑。

4.4.3 区块链运行环境

区块链运行环境通过提供确定性来促进链逻辑的执行力。该运行环境是精心设计的，以满足连锁逻辑确定性的要求。系统时间访问将被限制，取而代之的是区块时间。对象分配将以确定性方式实现，这使得基于存储器地

址的功能将继续工作（例如，默认的 hashCode() 函数）。此外，通用实用程序和算法将被仔细检查并包含在区块链运行时环境中。

4.4.4 区块链上下文注入

依赖注入是对一种常见的解决对象依赖的技术。它允许一个客户灵活可配置并隐藏依赖关系细节，例如在区块链上下文中的链逻辑。

在 Aion 脚本语言中，区块链接上下文和运行信息被视为依赖。任何链逻辑可以通过使用注释来访问这些依赖。随着 Aion 的发展，更多的资源将被添加到对象里。

4.4.5 安全

Aion 语言的安全性源于防御性编程的设计，以及 AVM 对时间，空间和资源使用上的严格限制。此外，安全性的着重也将通过提供脚本语言编写工具。例如，Aion 链码的逻辑正确性可以通过现有字节码的分析，验证和模型检查工具来提供。其他例子包括 Java Pathfinder [12]，FindBugs [13] 和 PMD [14]。

5 路线图

该白皮书制定的目标既充满壮志，也是拥有可试验性的。为了以务实的态度来处理这个问题，从现有技术出发，逐步实现目标，Aion-1 将以迭代的方式推出。

Aion-1 将分三个阶段执行，每个阶段都着重于技术的不同方面，构建区块，同时逐步完成网络（第 3 阶段）。因为每个阶段的选择都将进行更彻底的调查，则每个阶段的计划和截至日可能会发生变化。

5.0.1 阶段 1

Aion 发行时间表的第一阶段的重点是分组间通信和桥接基础设施。考虑到这一点，第一阶段的功能将包括：

- 优化的高性能 EVM
- 可运作的桥梁和跨链通信
- 改进的工作量证明的共识算法

5.0.2 阶段 2

Aion 发行计划的第二阶段针对从我们修改的 EVM 体系结构向拟议的 AVM 架构迁移。这一阶段的发展重点包括：

- Aion 虚拟机
- Aion 脚本语言

- EVM 遗留代码库支持

5.0.3 阶段 3

第三阶段完成预想的网络基础设施，为快速，有效的跨链通信和跨链应用提供基础架构。除了第一阶段的分组间功能和第二阶段的 VM 实施之外，本阶段将介绍我们的代表性共识，包括代表性共识算法。

6 结论

本文提出的解决方案是多年来在区块链行业中的实施和实验结果。Aion 背后的团队已经与多个大型企业进行合作，所面临的挑战显着。Aion 网络旨在克服这些挑战，并提出一个解决方案，使区块链应用程序能够实现其全部预期的潜力。在我们迄今为止的研究和开发中，我们很幸运地从研究互补概念的领先思想家和研究人员那里得到了重要的发现和实验结果。我们将在接下来的文献参考中予以列示。

我们将继续努力使 Aion 成为现实，连接不断增长的碎片化区块链系统，我们期待您的参与。

7 联系

本技术文档介绍了 Aion 第三代区块链网络的概念。本文背后的团队致力于实现区块链网络互联的梦想，这将在未来的企业，政府和公共数字基础设施中发挥关键作用。在接下来的几个月中，我们将对本文中介绍的每个内容进行深入研究，完成本项目的第一阶段内容。

加入 Aion 网络邮件列表，获取有关 Aion-1 具体方面更详细的白皮书更新信息。您也可以随时了解我们的进展情况：

- Twitter
- GitHub
- LinkedIn

参考

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] V. Buterin, “Ethereum whitepaper,” 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[3] M. Gray, “Introducing project ‘bletchley’,” 2016. [Online]. Available: https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md.

[4] Bitshares, “Delegated proof of stake,” 2015. [Online]. Available: http://docs.bitshares.org/bitshares/dpos.html.

[5] O. Beddows and M. Kordek, “Lisk whitepaper,” 2016. [Online]. Available: https://github.com/slasheks/lisk-whitepaper/blob/development/LiskWhitepaper.md.

[6] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, “The honey badger of bFT protocols,” 2016.

[7] C. Copeland and H. Zhong, “Tangaroa: A byzantine fault tolerant raft,” 2014.

[8] D. Mazières, “The stellar consensus protocol: A federated model for internet-level consensus,” 2015.

[9] S. Kamvar, M. Schlosser, and H. Garcia-Molina, “The eigenTrust algorithm for reputation management in p2P networks,” 2003.

[10] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter,” 2016.

[11] N. Atzei, M. Batoletti, and C. Tiziana, “A survey of attacks on ethereum smart contracts,” 2016.

[12] NASA, “What is jPF?” 2009. [Online]. Available: https://babelfish.arc.nasa.gov/trac/jpf/wiki/intro/what_is_jpf.

[13] U. of Maryland, “FindBugs™ - find bugs in java programs,” 2015. [Online]. Available: http://findbugs.sourceforge.net/.

[14] PMD, “Welcome to pMD,” 2017. [Online]. Available: https://pmd.github.io/pmd-5.8.1/.