NEM 投石车白皮书

作者：LON WONG 黄伦

Dragonfly Fintech Pte Ltd.

蜻金融科技有限公司

NEM核心团队成员

E-mail: lwong@dfintech.com

2016年11月

摘要：金融机构的各自独立运营，使得其延续繁多账簿共存的现状，多账簿在诸多系统中的无效性构成了金融管理的重大挑战。一个具有多个账本用于多种资产的区块链解决方案提供了转型以解决这个问题的方法。我们介绍基于新经（NEM）技术与概念的全新的区块链解决方案平台---“投石车”。作为一个开放平台，该解决方案被设计去减少实施与部署的开销，它可以作为媒介强化当前与未来区块链驱动的解决方案。投石车架构方案允许简便地集成大多数应用，对于已存在的银行标准是透明的。它允许在不同区块链实例上相互操作，因此其允许可共享或不可共享数据存在于同一个环境中。本文意在向广大的读者阐述该方案。

关键词：投石车 猕迅 新经 NEM 科技局 蜻金融科技 区块链 智能合约 允许链 开放系统区块链 银行标准 多链账本

目录

1. 介绍

NEM区块链技术已经问世两年多。完全按照主流应用设计，其目标是创建具有最广泛的适用性的区块链科技解决方案。NEM项目聚焦于发挥区块链技术的巨大力量，允许各类项目在该平台上灵捷地、快速地建立应用，实现区块链技术的价值。

我们认为区块链技术正在努力寻找商业领域的用武之地，但是在方法和标准上缺少统一。围绕市场上已有的解决方案，不难发现，大多数区块链方案创造者都围绕着区块链账本完成改善，均对区块链应该如何运行具备自己独到的思路。

我们的方式则是调整一下着眼点。一个强大区块链的功能和特点不是我们唯一的重点。我们汇总了哪些被忽视却同等重要因素。包括：

- 允许任何方案在其上独立存在;
- 有着全套API的抽象层，易于集成，并因此具备可驾驭区块链分布式账本强大力量
- 可扩展性.

本文的宗旨是描述NEM如何达成这一目标，以及作为最佳的解决方案，NEM如何在区块链行业扮演重要角色，并为区块链行业设立全新的标准。

2. 相关

区块链技术是一种总账方案。自然地，作为总账，它的一个明显特点是与金融领域的特有相关性。在所有核心银行的核心解决方案中，总账系统是唯一至关重要的环节。

很不幸，一个众所周知的事实是许多应用建立在那些提供不同银行服务的总账之上，这些总账被设计为基于账本所有权来匹配每一个服务应用。

日积月累，总账的数量和其上应用的不断增长将成为一个巨大的问题。

当这些银行之间庞大的兼容或不兼容的系统共存的环境中不可避免互相进行复杂的交易时，复合效应和风险就会产生。经历数十年的积累，这些系统已经成为巨大的昂贵的的胶结体，已无法从根本上精简。在各家银行增加新的服务和解决方案时，仅剩的办法是在已存在的系统上继续的打补丁，或者确认或改造每一种新型的解决方案，使它在失去部分优势和效用的同时适用于当前已存在的平台。

从技术的角度，中间件会成为这种复杂架构的最沉重的一层，它通过流与信息的大杂烩穿过所有不同的账本、应用与服务，从而来约束这个巨大的结构。随着管理与交易问题的产生，它不仅仅会引起运营风险，还会消耗大量的资源。

以上问题的产生使得核心银行解决方案的标准化、效率化改造势在必行。当前，标准化实施的环节主要在中间件层，业务系统依赖于这一层与其他机构协商对话。

银行之间的交易通过外部信息系统的服务实现，通常遵循服务机构的现实标准。一个占据统治地位的服务是SWIFT信息与交易系统。它被设计运行已超过40年，SWIFT系统是证实可用的技术实现。但按今天的标准来说，由于信息会多跳方式传输，且通常需要手工管理诸多信息，它的执行效率十分低下。

这样的解决方案不但挑战使用者的耐心，会引发运营风险，且成本高昂。一个银行与企业每年会花费数以百万美元计的金钱用于获得使用SWIFT系统的授权。与此同时，互联网作为一个开放的信息传输媒介，可以造就优秀的资金传输平台，能够达成有效与廉价传输。但它的应用层实现是一个巨大的任务，需要每一个人参与去转变现状，往往需要创意专家不计成本的努力。

3. 目标

我们看到的这些问题不是近期的问题。它是已经长期存在的行业难题，清算业务已经在过去的每时每刻都给核心银行系统带来繁重的业务负担。

区块链技术是可长期实现提高效率，降低成本，支持结算，实现高速合规匹配，提供更强大的可审计与可跟踪能力，加强结构化过程（又称为智能合约），在全球与本地交易中减少中间方环节的核心技术。

处于区块链平台满足以上需求的优势能力，任何金融机构都会了解和研究。区块链平台本身需要成为一个标准，且允许任何机构的附加应用通过它的遵从行业标准的指令集实现集成。

我们已经对金融行业分析了三年，远早于金融行业自身意识到区块链的影响以及其能扮演的角色之前。

我们三年的长期分析与评估得出重要的结论，即我们正在推出的区块链平台是解决当前问题的重要的方法集。这一宗旨的得出来自以下重要的结论：

- 智能合约在金融机构中早已存在。他们已经被纳入核心银行（自动）解决方案或基于协定或意向在内部或外部不同部分之间，手工地实现。这些智能合约花费了金融机构数十亿美元去建设基础设施，若要能够记录到一个新平台上将花费更多的资源、时间，面临更多风险。这是一个复杂的工作且不可能很快就完成。NEM已经认识到这点，而且能够按在接受固有核心银行解决方案的前提下解决业务问题。

  该方法是将智能合约作为一个外部组件，可以中心化（若基于已存在的系统）

或者去中心化。这些智能合约的输出将通过一个安全的交易过程进入金融机构的分布式账本完成交易。

- 建设一个最小风险、时间和资源成本的价格低廉的平台，让金融机构可以在这个平台的应用同时以最小的影响继续原有的业务，达成健康迭代。

- 建立一个区块链平台，其有着多个总账用于多个应用案例，这些应用案例可以彼此独立，也可以相互关联，同时，允许这些账本之间无摩擦的交易。

- 建立一个唯一的抽象层让相同平台同区块链上的所有账簿能与现有的银行系统和解决方案集成。

- 认同私密性保护，允许使用区块链技术的每一个金融机构具备自己的完全权限去控制和管理其自己的区块链平台。

- 区块链可由直接交易实现无缝跨平台交易、支付以及清算，不需要上线任何昂贵的标准与协议驱动的信息系统。可减少清算基础系统以及协调工作、风险和错误。

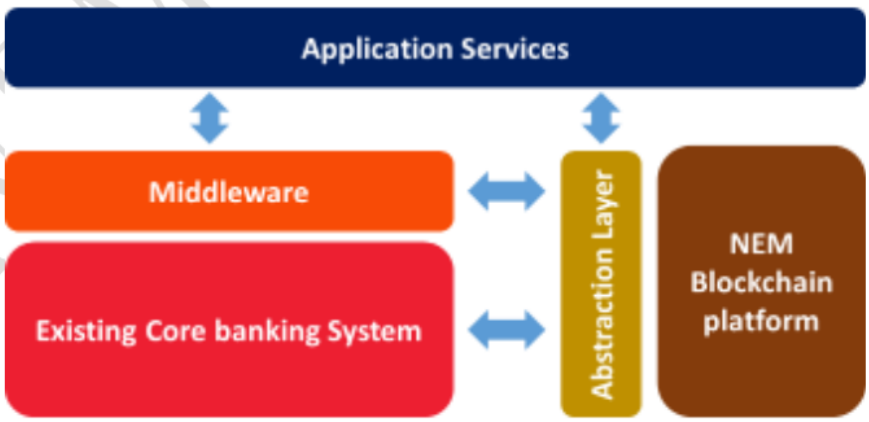

图1

4. 投石车（Catapult）

投石车是第二次迭代版本，也是2015年3月份上线的NEM区块链技术的全面扩展。它的发布被安排为几个阶段，开始于2017年第一季度。它的前任是已经经历多重测试的猕迅（Mijin）。Minjin和投石车都是许可区块链。他们在开发上的区别在于Mijin是NEM公有区块链的扩展或再版，投石车则会不同，会是NEM公有区块链和私有区块链的共同核心。为了支持金融业，它专门为区块链设计增加了关键特性和功能。

4.1. 突出特性

投石车是使用C++语言全部重新写的，从它的第一代NEM发行版继承了核心理念，并以现有的区块链研发经验和应用实践方向为基础延展了这些理念以提升实用性。最终目标是具有开放链接性的高性能，高安全性的企业级解决方案。目前已经开发出投石车的一些显著特性包括：

- 高度可扩展，基于企业级计算中常见的工业标准WEB分层架构而设计，区块链解决方案中尚未见到有如此完整的产品。
- 引入带有一个开放集成架构的高性能和高可扩展的API网关服务器层
- 创建为实时分析和大数据事物分析的高吞吐量消息队列
- API层nosql数据库的使用，使区块链更适合于高速消息会话
- 为区块链上资产交换提供托管服务——特殊的交互合同
- 高速交互（真正每秒超过3000笔交互）
- 根据账户进行权限许可，允许限制每个账户的访问权限
- 互通性——允许外部去中心化的和中心化的应用或者使用区块链进行交易的智能合同解决方案
- 商务规则——可根据对象的状态制定有限的一连串的事务的行为规则，比如不同预定义的不可篡改的和不可逆场景的手续费计算。
- 元数据——账户和资产应该有可以配置的元数据字段

作为以上的补充，当前已有的功能和特性已经在当前NEM发行版中出现，他们会被增强和移植到投石车项目中。它们包括：

- 一套内置的消息解决方案
- 在需要多人审批的情形程序激活或人工签署交互的方案
- 在同一区块链中多种类型资产的多重账本的实现
- 每个账户可以持有来自同一区块链中多个账本的多重资产，同一账户可以被银行提供的所有的产品和服务使用。例如，一个账户可以持有USD、EUR、GBP、黄金、利率互换交易、ETF单元等等。每个都有自己的历史交易记录和账目。
- 每个账户都可以被金融机构管控——允许有监管和实施AML控制机制来管理这些交易
- 冻结账户
- 带有全面审计追溯和追责制的交易回溯

最终结果是，投石车解决方案会成为健壮和高度可定制，并可以被金融机构长期作为核心操作平台的基础而使用的区块链解决方案。

设计背后的原则是提供通用和核心的区块链解决方案为银行构建更健壮的系统作为基础。更进一步说，它允许在不对现有系统造成大幅改动的前提下子系统按计划向区块链迁移。可以允许局外系统和非核心解决方案系统在不对银行系统造成风险的情况下率先进行移植。新的和老的适应性强的产品和服务可以使用区块链来开发、移植和发行。

这个高度灵活定制的解决方案给予了银行可常规或应急上线解决方案的协调性，提供在发展区块链驱动的系统的同时仍可以保持传统系统可用性的机会。

它的API网关允许区块链很容易融合到其他中心化（新的和已有解决方案）或者去中心化（其他组织创建的以共识为基础的平台）系统的智能合同系统，内部流程驱动解决方案及现有结算，支付，清算系统等。

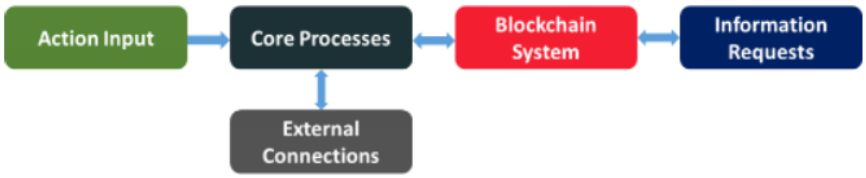

图2

4.2. 共识

投石车的区块链平台和绝大多数区块链同样由共识系统驱动。由预制以P2P协议配置互相通讯的节点构成它的网络（支持公网或者私网）。所有交互以广播方式发起后，每个P2P节点记录这些交互然并相互验证。在每个成为块时间的间隔周期后，这些请求被打包在一起，这些交互会进行一次哈希过程（数字指纹），并将它连接到上一个区块，最终作为区块链中的一个新的区块被加入链。私有账本本身不存在挖矿，它遵从股权证明（Proof-of-stake）核心算法，公有链基于重要性证明（Proof-of-importance）核心算法。

NEM区块链解决方案内置保证节点信誉的机制（Eigentrust++声望管理算法），因此得以保障网内没有被篡改的节点，保障每一个P2P节点的声望和可靠性。

NEM区块链解决方案还创造了一套基于区块链时间的全新P2P时钟同步算法，来保证每个节点和其他节点在正确的时段。

4.3. 前景- 用例

此区块链有意设计成来满足一组JSON RESTful API工业标准的开放系统。因此它可以达成兼容任何符合消息标准(例如ISO20022或者FpML标记语言)的应用程序。投石车将它作为定制输入的进程，去实现对总账中的交互的更新和广播。这种高度协调的集成和互操作方法让已有应用和解决方案的重用成为可能。

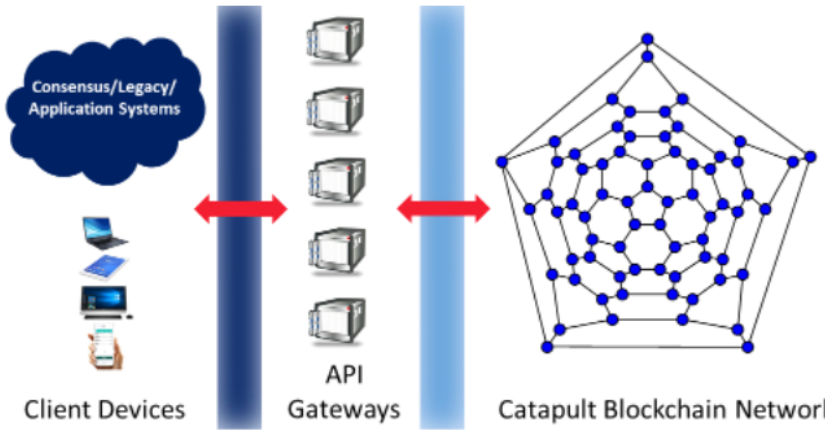

图3

4.3.1. 共有基金 – 传输代理

我们现在研究共有基金购买典型契约和结算的解决方案。

在典型的公募基金方案中参与者如下：

- 共有基金经理
- 过户代理人
- 客户

合法契约规定，造成出售和购买一个或多个共有基金中最小资产分割单元的关键点，包括但不限于以下：

- 净资产价值（NAV）推导
- 投资细节和条件
- 股息
- 折扣
- 管理费

- 受托人费用
- 转让费
- 佣金

这种传统意义上的合法契约将被转换成运算应用程序，其输出将导致对数据库的一个或多个写入，随后是一系列自动或手动的行为。

买卖的发起会创建一个请求，该请求或者被手动处理或者自动触发一系列操作。这些操作最终导致的结果是：

- 等待结算
- 结算后，份额过户
- 颁发所有权证书

图4

过户代理人的功能是管理这些资产的销售，购买和分配。这项工作是乏味却重要的。而这个角色可以在区块链中实现完全的自动化。

每个份额持有人，当她在区块链购买共同基金的份额时，将获得证书，她拥有的每一个份额都记录在区块链中。 每个交易变得不可篡改和不可逆。

费用及股息将通过API调用从区块链的其他应用程序自动计算并提取。

原始合同文档的hash将会存储在区块链中，而文档本身可以存储在分布式文件

系统中。订单处理是另一种解决方案，其输出将通过API调用区块链数据所得。用户余额可以由用户通过访问相同的前端应用程序通过API从区块链中读取并调用。数据分析功能也通过消息队列调用API提取区块链提取的数据来实现。 付款和结算更可以通过在区块链中的用户帐户直接完成。

区块链系统是一种无边界系统，可以在相同的一组节点设定多个总账本。这是一个非常强大的系统，在完成跨越国境的统一账本的同时，允许多个国家监管机构在其中运作，满足自己的一套监管规则-国家提供的相关条件（智能合约），监管过程可以去中心化或中心化实现。

智能合约模板可以独立实现，并应用于任何资金账户。

区块链解决方案有其结算机制，可以很容易地实现自动化，减少结算时间到几乎瞬间，且无需干预。

虽然这一解决方案已经在NEM项目的版本1中提供，但投石车系统将基于上述改进将其性能提升到更高的层次。

4.3.2. 利率互换协议

当双方决定交换利率合约时，首先会达成协议。它是由当事人之间进行的定量探讨并达成一致的结果。该协议可以在区块链中实现数字公证的，并且将hash存储区块链中，同时协议存储于分布式文件系统上。

图5

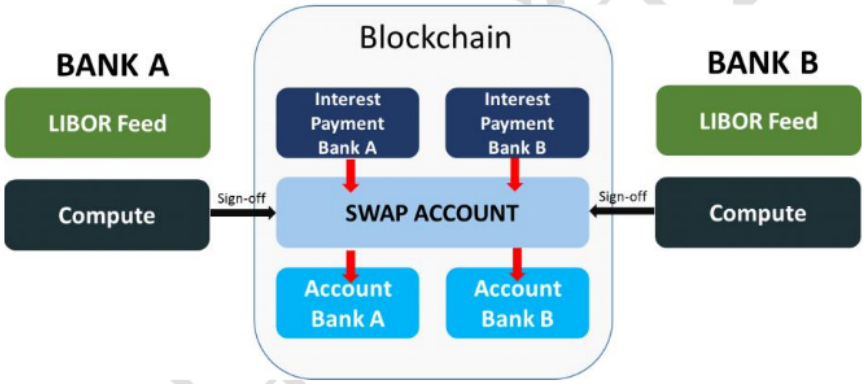

图6

运算结果可以基于模板化的分布式智能合约来共同约定，或者由参与者单独运算。区块链将基于这些运算操作的输出触发支付。

4.4. 扩展

上面是可以使用NEM区块链实现的许多使用情况中的两个例子。在金融机构中，一切工作都围绕着一个总账，它是所有流程的核心要素。 通常情况下，对账问题，延迟，风险和失败的原因是缺少具有多个子分类帐的中央分类帐系统，它可以在总账平台中协同工作。 即使根据现有中央分类帐系统要求分类帐单独更新中央分类

帐，它通常会导致更多的问题，也可能是一个综合的噩梦。

识别这些问题的根本原因并提供必要的平台不仅可消除许多风险和问题，而且还将允许金融机构接受和催生新的和更精妙的服务产品，同时解决这些服务产品日益上升的成本问题。

NEM技术解决了这个问题，并且设计保证了不可篡改和不可逆的交易的绝对最终性和完整性。 任何交易的撤销只能由另一个反向交易来完成，并且可以通过完整的审核跟踪进行控制。

API服务器网关的存在使得区块链能够作为需要使用分类帐的应用程序的核心。因此，它构成了允许标准合规的应用程序，包括传统和新的分布式智能合约，与分类帐无缝集成的开放系统。

投石车系统的设计以每个私人实体机构或金融机构为应用场景。 在NEM计划中有一个并行项目来开发特殊的路由系统，以允许使用公共分类帐系统和实体的私有区块链中相互操作。 这种公共分类帐系统使用NEM区块链技术并实现无缝交易，从而不需要具有多跳转结算和支付系统。 它开辟了一个以更少摩擦及通过帐户到帐户完成支付交易的新维度。

每个金融机构能够选择操作其自己的独特的私有区块链，金融机构能够限制数据的隐私性。 公共分类帐系统的存在允许金融机构的互操作性，使他们能够无缝地结算和相互支付。

事实上，公共分类帐系统是可以独立存在的，只要提供一个无缝的解决方案，不需要银行拥有私链的前提下就可以参与。 毕竟它是一个允许记录结算和付款的分类帐。

它要求采用稍微不同的规则，而不是传统的结算和付款方法。 此外，它符合如今实行的监管框架。

可以看出，NEM区块链技术是一个帮助金融机构从传统解决方案过渡为由区块链技术提供支持的解决方案。

NEM项目团队强烈认为这是前进的方向。 它使金融机构拥有低门槛使用区块链技术，金融机构将逐渐开展在区块链技术上工作并最终熟悉它。

5. 总结

投石车项目已经进入后期开发。该项目会在多个阶段发布，在4.1节所强调的特点将会在每个阶段被添加进来。计划在2017年第一二季度发布第一版。解决方案的增强是独特并且强大的，同时在区块链设计上定义了全新的标准。

NEM强大的抽象层可使与现存的银行标准有异的操作方式也能完美融合，这体现NEM着眼的方向不是破坏当前金融机构已经使用的解决方案，而是与金融机构现有的系统无缝衔接。当前运行标准依附于解决方案的系统，如FpML和ISO20022，只需要通过抽象层与区块链整合来使用输出。这种部署方法允许金融机构在一段时间内移植它们的系统，这会更好的满足他们的业务，并尽可能最小化损耗地将它们需要的标准转到区块链平台。与此同时，投石车解决方案可凭借快速和廉价的区块链部署，用于金融机构的成长、扩张、以及产品创新。

6. 与其他组织对比

投石车是一个定位独特的解决方案，是NEM和Mijin解决方案的首次迭代。而其他大部分准商业项目都是衍生和附加到现有区块链之上的解决方案，这些方式结合的方案整体产品臃肿。

我们现在以三个与NEM项目领域可能有交集的项目进行论说。以太坊(Ethereum)和比特币(Bitcoin)目前是已走向生产阶段的方案，Corda当前仍在概念论证阶段。

6.1. 以太坊

此项目是以以太虚拟机为前提的，拥有自己的编程语言来运行加载到区块链上的智能合约。一份智能合约一旦加载到区块链是不可变且不可逆的，如果它本身有

缺陷后果可能是很严重的。此外，智能合约往往需要依赖外部的数据源，如Oracle数据库，以便提供输入到程序中来改变程序的状态。这些状态的改变是写入区块链存储。

我们的解决方案中没有类似以太坊的智能合约，因为我们的观点是作为一个独立的使用，这应该留给银行去决定他们将想怎样去具体使用。在某种程度上，我们优化区块链完全做的正是其设计。比如，单一总账解决方案和有很多特性的多总账解决方案，不但适用于金融业，而且在一般情况下也满足了一系列的金融行业以外的行业。某种程度上，随着被认可和更多的使用，我们也在区块链上建立了某种“智能”，使其可直接使用。这种“智能”的托管式解决方案是基于双方签署的可交换资产基础之上的，如果任何一方不签署，就不存在资产交换。

部署一个存在不可改变和状态不可逆的智能合约，尤其是如果它还需要100%的完整性证明和测试时，只会导致大量的资源浪费。这是在任何软件解决方案项目中从来没有过的。项目越复杂，就越容易产生缺陷。一个轻微的错误都能导致一个系统性的失败，没有金融机构会有可能去考虑部署这样一个智能合约。

方木栓配不进圆孔(智能合约不适合金融机构)。区块链之上的智能合约就是一个例子。而现在的实际情况是，大部分金融机构已经很好的定义了中心化的智能合约，而且已经使用了很多年。这些中心化的智能合约全部可控并且能够停止，纠正错误后，可再次运行。输出是最终和明确的。任何此类单边或多边合同在多方之间进行相互验证。而在区块链上的智能合约是不可能做到这一点的，即智能合约不能被另一个程序放入区块链。

一个智能合约是无法孤立地工作的。它仍然依赖于外部的输入或Oracle这样的数据库。它不能在“虚空”的和依赖一个有信任问题的第三方输入中执行，这首先就是不可靠的。这本身是个悖论，因为一个分布式的智能合约解决方案的主要价值主张本身就是一个不可靠的智能合约平台，这种平台是不可能存在的。事实上，在

区块链上有智能合约可能会成倍的增加实施成本。因此不提倡为了实现智能合约为目的不择手段。

6.2. 比特币

比特币是第一个区块链项目并且是一个用去中心化的区块链管理交易的概念性证明。投石车像比特币项目一样在区块链上有着相同的哈希和存储及交易实现方式。事实上，大多数的区块链项目遵循这一原则。

NEM与Bitcoin不同的是在区块链上构成共识和竞争区块创建权的方法。其他差异是：

- 系统架构：NEM更易于扩展。
- NEM没有未消耗完的交易输出。它遵循使用一个标准的、带有多重资产账目的账户总账约定，即一个账户多总账，全部输入、输出都通过该账户。
- 业务逻辑：比特币是一个普通的总账目。比如，NEM拥有链上的交易签名，在广播到区块链之前，不依赖额外的中心化的服务器去给予交易签名，这赋予了NEM一个非常强大的工具。
- 比特币没有一个内在的、内置多总账解决方案的作用。
- 大多数比特币提供的是在解决方案上打补丁的解决方法，这些方案又必须依赖第三方的提供者。这从而引入了涉及服务水平和质量依赖、安全、性能和可靠性等另一层面。
- 机器竞争：比特币被设计的目的是挖矿。它们使用工作性证明作为必要的元素来保护区块链的安全。对于一个可授权的区块链解决方案，为了挖一个块，是不需要竞争的。NEM的方法是既简单又强大的确保区块链安全的方式，相较比特币区块链的运转需要巨大电能损耗，NEM仅需要非常少的计算资源和能源去管理和维护。

- 比特币的吞吐交易量太低而没有实际的金融应用。比特币的交易率是每秒一位数的量级。NEM的投石车交易率是4位数。
- 比特币的确认时间太长，从而不适合金融业。

6.3. Corda

R3CEV组织创建的Corda处在概念阶段，从目前已知的来看，他们是走以太坊的路线，但在管理Oracle数据库和无状态功能的可分享总账方式上跟以太有一些微妙的差别。他们目前建议使用Java虚拟机去开发他们的解决方案。如果他们的实现可行，NEM应该可以使用相同的写入过程和输出智能合约的结果到投石车总帐系统中。

翻译： NEM 中文社区长江一号（KevinLi）、六翼の炽天使、Rafe、Thilon

校对： NEM 中文社区 Ronel

原文链接：https://www.nem.io/catapultwhitepaper.pdf