IoTeX

以隐私为中心的区块链驱动的去中心化的物联网网络

更新日期：2018 年 3 月 11 日

版本 1.4

免责声明：本文旨在提供相关技术概览，所涉及内容不以完整性为标准，也非设计终稿。因此，非核心技术领域（如 APIs、协议、程序语言等）未有涉及。

摘要

目前，绝大部分物联网设备以中心化模式运作，而与其去中心化的特质相悖。因而也产生了诸多问题，如可扩展性受限、运作成本高昂、隐私问题频发、安全风险突出、使用价值缺失等。而区块链以其去中心化的内在特性，能够充分解决上述现行物联网所存在的问题。首先，区块链的可伸缩性能够在高性价比的前提下解决物联网可扩展性的问题。其次，区块链可将数据的访问限制在预先定义的特定范围内，从而消除存储于云端的物联网数据遭泄露和滥用的可能。再次，支持智能合约和通证系统的区块链具有激发设备之间自主合作从而创造使用价值的巨大潜能。然而，由于物联网的特有属性，如大体量设备数、异构性、有限的计算能力、存储和功耗等问题，现有的物联网技术时而捉襟见肘。

本文所介绍的 IoTeX 是以隐私为中心的区块链驱动的去中心化物联网网络，具有以下四大创新点：

- 前沿的链中链架构支撑起平衡性良好的分配网络，以高性价比的方式将可扩展性和隐私保护性最大化；
- 依靠轻量级私密地址、无需可信设置的环签名和 Bulletproof 技术的首次应用，在区块链中真正实现隐私保护；
- 具有即时最终性的高速共识机制大幅度提升网络吞吐量，并降低交易成本；
- 灵活的轻量级 IoTeX 系统架构，精准对接物联网在跨行业领域中的关键应用。

目录

1. 现有物联网的局限性

作为社会整体网络化的体现，物联网迎来了蓬勃发展之势。在物联网中万物互联，彼此裨益。然而，这场影响深远的变革才刚刚起步。据估计，物联网设备数量将以每年 21%的速率增长，到 2022 年，互联的物联网设备体量将达到 180 亿美元[6]。全球物联网市场将从 2017 年的 1700 亿美元扩张至 2022 年的 5600 亿美元，其综合年均增长率将达到 26.9%。 尽管业界专家和消费者纷纷认定物联网将是网络时代的下一次工业革命，物联网的大规模发展和普及仍然受到三大问题的掣肘。

1.1 可扩展性受限

物联网设备以中心化的方式与后端公共云服务或本地服务器群相连，以传输数据、接收控制命令。现阶段，物联网的规模受到现存后端服务器、数据中心等在扩展性和可用性上的限制，发展遇阻。运行大体量物联网所产生的高昂运营成本也不可能通过贩售设备来弥补。因此，物联网销售商通常无法提供足以应对现实需求的具有高性价比、可扩展性且安全可靠的设备和服务[26]。

1.2 隐私保护不足

据预测，物联网将为其终端用户提供接入诸多社会关键领域（如能源、交通、法律、民主等）的机会。由于物联网自动与现实世界直接相连， 并且在物联网扩展过程中，数据体量会呈数量级增长，隐私问题日益突显。常见的隐私风险如下[28]：

1. 身份识别：将（永久）标识符，如名称、地址、任何形式的假名等，与个人绑定；
2. 定位与追踪：通过不同方式获取个人定位；
3. 用户剖析：通过与其他档案和数据源的关联对比来收集用户个人的信息行利益推导；
4. 侵犯隐私的信息交互：通过公共平台传递隐私信息，在此过程中将隐私泄露给不恰当的受众；
5. 使用周期内的信息交接：设备在它的使用周期内存储大量的历史信息，在此周期内控制权的交替可能导致信息泄露；
6. 财产目录攻击：对私有物品的存有和特征信息进行未经授权的采集，例如：窃贼可通过调取财产目录数据判断何时行窃；
7. 关联：将原本各自独立的系统相连可导致数据源泄露关联主体在关联前未曾揭露也不愿揭露的信息。

以上这些潜在的隐私风险皆能归因于设备层面、通信层面、和更常见的中心化主体层面的数据泄露。

1.3 功能价值缺失

现存的物联网体系大多无法创造有意义的使用价值。“彼此互联”是提及最多的价值主张。而事实上，仅靠连接设备无法使设备智能化，也无法使之变得有用。就像个体细胞相互合作产生多细胞有机体，蜜蜂归属于蜂群，人类个体建立城市和国家那样，物联网更大的价值在于交互、合作，并最终实现异构实体间的匿名合作。通过合作，个体单位产生成倍于自身的价值。然而，根据[22]所示，85%的传统设备由于兼容性的问题缺乏交互和合作的能力。在商业和操作领域实现数据共享变得几乎不可能。

2. 区块链

2008 年，区块链技术首次进入人们视野。此项技术的初次应用（比特币）出现在一年之后。中本聪于 2009 年发表了一篇名为《比特币：一种点对点式的电子现金系统》的论文。区块链在本质上是一种分布式的交易数据库，所有在网络中的节点分享数据。这是比特币的技术创新，它在这种交易过程中担任着公共分类账目的角色。系统中的每一个节点都拥有现存链上的区块副本，其中包含了所进行过的一切交易数据，每个区块以哈希值与前一个区块相连，这些相连的区块就形成了区块链。每个区块链都包含四个维度，数据层、共识层、应用层三个水平维度以及一个垂直的治理维度。

数据层

作为底层水平维度，被记录的交易在节点间广播，完整的节点产生区块。作为区块链的基础，在区块链中发生数字资产与其伴随的价值的传输，通过椭圆曲线密码、哈希函数、默克尔树算法等加密手段实现账户安全。

共识层

共识层是区块链的中间水平维度，体现区块链点对点式的特征。在此层中，网络中所有节点通过工作量证明算法（PoW）、权益证明算法（PoS）或其变体、拜占庭容错算法（BFT）或其变体等技术对链的内部状态达成共识。区块链的可扩展性主要受共识层影响。通常认为，PoW（工作量证明算法）在扩展性方面不及 PoS（权益证明算法）。此外，双重支付问题和区块链可能遭受的状态篡改攻击还会直接影响共识层的安全性。

应用层

以上两个水平维度构建了区块链的基本构架，而应用层对于区块链的实际应用至关重要，影响到包括区块链可扩展性和可用性的问题。举例来说，以太坊使用的智能合约具备可编程性，使

得个体能依靠分布式的“全球计算机”执行合约条款。侧链技术与合并挖矿也极大地推进了可编程性的发展。闪电网络[19]所代表的二级协议发展状态通道技术，进一步加强了区块链在此层面的可扩展性。此外，应用工具、软件开发工具包、框架结构、图形用户界面对区块链的可用性也尤为重要。应用层为开发者提供开发去中心化的应用软件(DApps)的平台，这是区块链实现其使用性和价值的重要环节。

治理层

与任何有机体一样，成功的区块链也将是环境的最佳适应者。在区块链系统只有通过演化才能生存的前提下，初始设计固然重要，但在足够长的时间段里，可变化的机制无疑是最重要的，此机制就是我们所说的垂直层面治理。

3. 区块链与物联网的机遇与挑战

信息感知与感应、信息转换与传输、以及信息处理是智慧体的本质。对于物联网而言，感知与感应层是自发式分布的，而后两个层面在现阶段尚未实现，这也是大部分可扩展性、隐私性以及可扩展性问题的根源。展望区块链的未来，我们希望它能成为物联网的脊椎和神经系统，精确而有效地应对前文提到的物联网三大问题。

3.1 存在的机遇

通过将区块链技术引入物联网，受益于区块链特有的属性：去中心化、拜占庭容错算法、透明度与不可篡改性，物联网可获得即时提升。表 1 归纳了区块链各属性与物联网各方面提升的对应关系。

表 1：区块链属性对物联网的提升

区块链属性	对物联网的提升
去中心化	可扩展性, 隐私保护
拜占庭容错算法	可用性, 隐私保护
透明度与不可篡改性	锚定信任
可编程性	可延展性

去中心化

去中心化的属性将用户与设备从中心控制与实时监控中解脱出来，因而在一定程度上解决了垄断市场的中心化主体加诸于个体的隐私风险-试着从各方面了解理解其用户/设备并以此获利，比如广告业等。在加密经济的大背景下，去中心化同时意味着“灵活性”，即“系统对工作量变化的应变程度，并基于此变化自动分配和撤销资源供给，从而使可获取的资源同当下需求达到最精确配比”。区块链与加密经济可以被设计成兼具灵活性和高性价比的组合以充分支持物联网的各种场景与应用。举例来说，在计算任务和激励机制同时充分时，可激活网络中更多的节点行进合作。

拜占庭容错算法（BFT）

拜占庭容错算法的目标是应对系统成员随机产生的失败，这样失败的例子不仅包括中断或脱机，也包括错误处理请求、破坏本地状态、和/或产生错误或不一致的结果。拜占庭协议模拟现实场景中电脑和网络因硬件问题、网络拥塞、网络中断及遭受恶意攻击等意外发生时电脑和网络会产生的错误。BFT 可在这些时刻作用于物联网，以达成最优安全属性。比如，中间人攻击（MITM）再也不会发生，因为不存在可被截获并篡改的单线通讯，几乎根除拒绝服务攻击（Dos）发生的可能性。

透明度与不可篡改性

区块链提供加密保证，使锚定于链上的数据永久处于透明且不可篡改的状态，这种保证可运用于多种场景，比如物联网世界区块链上的锚固状态可运用于审计、公证、司法分析、身份管理、鉴定、授权等各种领域。

可编程性

比特币具有基本的可编程性，只有在交易内嵌脚本成功运行时交易才能成功。以太坊强化了这一特征，实现了以高级编程语言编写并在小型虚拟机（EVM）上运行的图灵完备（Turning-complete）的智能合约。这样的可编程性也应当延伸到物联网设备上。现阶段，一些物联网设备只含有简单的硬编码逻辑，一旦发布便不可再进一步编程。

3.2 面临的挑战

区块链带来的机遇并不意味着任何区块链都适合投入物联网使用。实际上，由于不少挑战的存在，现存的公共区块链无一能应用于物联网。

原生隐私保障不充分

区块链所提供的原生隐私保障仅止于使用匿名性将链取代中心化服务器进行数据存储，从而消除物联网上的隐私风险。然而，一旦一台匿名设备与其身份相连，那么它匿名产生的任何信息就将被联系到其上。

世上没有万灵药

正如上文提到的，物联网是由目标和性能各不相同的异构性系统和设备组成的世界，不可能找到一个万能的解决所有场景问题的方案。例如，协同数百万个工业物联网节点的区块链应当注重其高度的可扩展性和巨大的交易量，而协同智能家居设备的区块链则应注重隐私保护和延伸性。从宏观层面看，物联网作为单类项的确在以极快的速度发展演进，从新技术的整合、新标准的制定、新设备的生产等方面看皆是如此。与之形成对比的是在微观层面上，个体物联网设备的效能、目标和运作环境也随着时间不断演进。

链上操作过于昂贵

在物联网世界，大量设备被视为弱节点：

- 由于能耗和算力限制不能进行基于工作量证明算法的挖矿任务；
- 由于能耗和存储容量限制无法存储大量数据（如十亿字节、兆兆字节、千兆兆字节量级存储）；
- 无法通过处理完整区块链验证所有交易；
- 由于在线时间与连接质量限制无法实时实现点间连接。

因此，大多现有区块链对物联网而言量级过重，并无法实现物联网设备交互的轻便性。

3.3 相关探索

最近发行的 IOTA 运用了名为缠结（Tangle）的新型技术，试图通过摆脱连续的链式结构将共识机制和交易生成机制分解开来。在这种新的模式下交易的发起者同时又是交易的确认者。交易的确认通过有向非循环图（DAG）实现，从而提高交易速度，实现零成本目标。而这种高效会导致失去全局确定状态，失去如支持轻量级用户的简单支付验证（SPV）和智能合约等功能。总部设在中国的万物链（ITC）[12] 沿用了与 IOTA 相同的缠结构架，因而具有相同的优缺点。与韩国现代集团合作研发的 HDAC 项目[9]也将物联网与区块链结合起来，将目光聚焦于物联网的细分领域，如设备认证和机器与机器（M2M）的交易等。

4 IoTeX: 设计与构架总览

4.1 设计原则

IoTeX 的目标是成为物联网内注重隐私保护和可扩展性的中枢和神经系统。为了实现这一点，并应对上述提到的一系列挑战，我们的架构设计遵循以下原则。

职责分离(Separation of Duties)

将所有物联网节点直接连接成一个单独的区块链是不现实的。 除了不同的物联网应用程序需要不同的区块链属性设置之外，在单个区块链中，承载过多的物联网节点对其规模和算力的要求直线上升，对物联网设备来说量级过重。 相反，职责分离可确保每个区块链与特定组别的物联网节点进行互动，在有需求时才与其他区块链进行互动。 这与互联网的构架相似——异构设备首先形成一个内部连接的组，即内部网络。 较小的内部网络进而构成一个更大的内部网络，最终连接到互联网中心并相互通信。 “职责分离”通常会创建一个均衡的系统，以最大限度地提高效率和保护隐私。

奥卡姆剃刀原理 (Occam’s Razor)

每个区块链都有不同的用途和应用，应有针对性地进行设计和优化。 例如，专用于交易传递的区块链不需要受图灵完备（Turning-complete）智能合约；运行在信任区域中的区块链无需过分注重交易隐私。

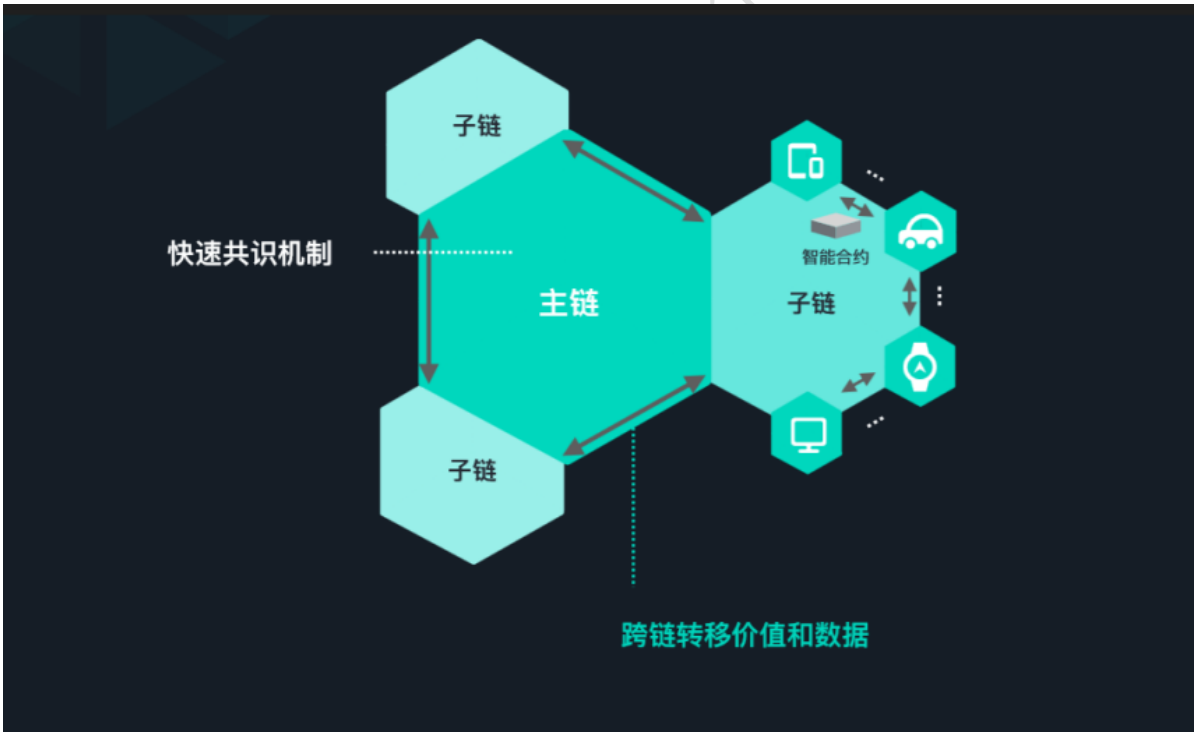
对物联网友好 (IoT Friendly)

如前所述，物联网世界充满了异构系统和节点，它们的算力、存储容量和功耗各不相同。 由于强节点可轻易完成弱节点能够完成的操作，因此应该以弱节点为设计目标优化区块链操作。例如，操作需以轻量级为目标，从而节省算力、存储空间和能源等相关资源。

4.2 链中链架构

IoTeX 是由许多分层排列的区块链组成的网络，这些区块链在保持互操作性的前提下共同运行。 在 IoTeX 世界中，如图 1 所示，根链(root blockchain)管理着许多独立的区块链或子链(subchain)。 子链与有相似性的物联网设备相连接，这包括功能目的、运行环境或信任级别的相似性。 如果一条子链在遭受攻击或遇到软件错误时无法正常运行，根链完全不受影响。 此外，也可以进行跨区块链交易，将价值和数据从子链转移到根链，或者通过根链从一条子链转移到另一条子链。

图一: IoTeX： 链中链，根链(rootchain)和子链(subchains)架构。



根区块链是任何人都可以访问的公共链，它有三个主要目标：

1.以保护隐私的方式在子链之间传递数值和数据，以实现子链间的互操作性;

2.监督子链，例如通过没收定金(bond confiscation)惩罚子链上的运营方(bonded operators);

3.结算和锚定支付，建立子链信任。

有了具体目标，根链将专注发展其可扩展性，稳固性，隐私保护功能和协调子链的能力。

子链具有成为私有区块链的可能，并且依赖于根链作为中间站与其他子链进行交互。子链需具备灵活性和延展性以适应物联网应用的多样化需求。子链很可能由在根链上存有定金的运营商运营。在另一种方案中，系统允许运营商提名一个或多个运营商在有/无特别绑定的前提下为其运作。运营商像根链上的轻量级客户端，作为子链上的完整节点来打包新区块。

详见表 2：根链和子链属性对照表。

表 2：根链与子链属性对照表

属性	**根链**	**子链**
公开性 VS 隐私性	公开	皆可
扩展性	必要	按需
稳固性	非常必要	必要
隐私保护	必要	按需
延展性	Turing Complete 非必要	Turing Complete
即时最终性	必要	必要

4.3 根链(Root Blockchain)

根区块链与 Bitcoin [17]和 Monero [16]一样使用基于 UXTO 的模型，原因如下：

- 由于无需随机数(nonce)或序列号，交易排序变得不重要，这让共识方案要求门坎不高并且能够平行处理交易;

- 应用现有的隐私保护技术，例如环签名(ring signature)和零知识量证明(ZK-SNARKs)来隐藏发送方，接收方和交易数量。

根区块链由哈希值链接(hash-linked)的区块组成，一个区块则是由一个以哈希值链接前一个区块和一系列交易区块头组成。根链主要允许两种类型的交易：（1）基本交易，包括 P2PKH，P2SH，Multisig 等，以及支持跨区操作的高级交易，如 BondedRegistration，Lock，ReLock，Reorg 等。经验证的交易被添加到具有动态大小、上限为 8MB 的区块中。 每三秒钟产生一个基于共识方案的区块，详见下一节。 该根链因基于堆栈程序代码(stack-based script)和丰富的操作码，故而不需满足图灵完备（Turning-complete）的要求。

4.4 子链(Subchains)

IoTeX 通过低层基础设置（如 Gossip 协议和共识机制）为分布式物联网应用程序开发度身定制了可发展和增补的子链架构，可根据应用需求定制相对应的子链验证模型、规格、参数和交易类型。

IoTeX 子链使用以账户为基础的设计模型，使其易于追踪交易状态。子链包含类似于以太坊两种类型的账户，即常规账户和合约。由与根链相同的共识机制产生的有效交易被添加到区块中，以达到同等的结算速度，提高跨链通讯的效率。子链使用根链通证、IoTeX 通证或自行定义通证。开发者在子链上定义的通证可以通过通证销售或通过公共交易平台公开发行。

子链支持智能合约，并且运行在轻量级且高效的虚拟机之上。我们目前正在测评 Web Assembly（WASM）[27]，这是一种用于构建高性能网络应用程序的新兴网络标准。 WASM 效率高，速度快，并且可以像 EOS 项目[5]做过的一些尝试那样通过修改来达到不可逆化和沙盒化目标。我们同时也在探索其他可能性。通过智能合约，连接到相同子链的物联网设备以两种方式共享状态，

首先，设备可以根据其子链的状态与物理环境进行交互，例如，灯泡可以根据子链上的“时钟状态(clock state)”亮灯和灭灯;

或者，当物理环境发生变化时，设备可以更改子链状态，例如，恒温器读取传感器上的数据，通过智能合约来更新温度数值。

4.5 跨区块链通信

物联网应用将高频使用跨区块链通信。 处于某一子链中的物联网设备总是需要与其他子链中设备进行合作。 我们致力于快速和低成本跨区块链通信设计以应对物联网设备在算力和存储空间上的限制。 更多信息请参阅我们的白皮书初稿[11]。

5 内置隐私保护交易机制

比特币和以太坊本身提供的隐私仅限于使用匿名地址，两者交易细节皆是透明的。 任何人都可以轻易从透明的账本了解交易金额，被转让的资产以及该交易与其他交易的关系。在这种情况下，发送方的隐私，接收者的隐私和交易细节隐私三个方面是需要解决的议题。 如表 3 所示，各种加密方案可用于解决以上所提的隐私问题。

表 **3**：区块链的隐私保护技术

技术	隐藏发送方	隐藏接收方	隐藏账户
隐藏地址	否	是	否
佩德森承诺协议	否	否	是
环签名	是	否	否
zk-SNARKs	是	否	是

IoTeX 的隐私保护技术通过隐藏接收方的地址，使用环形签名(Ring Signatures)保护寄送方的隐私和使用佩德森承诺协议(Pedersen commitment)来隐藏交易金额，进行了以下创新和改进：

- 使用轻便型的隐藏地址让接收方不用扫描整个区块链来确认交易;
- 优化环签名，使其更体积更轻便并更具有可信任程度。

5.1 以可传递支付码隐藏交易接收方

隐藏地址技术源于 Cryptonote 协议[21]，它利用“半轮(half round)” Diffie–Hellman 密钥交换协议解决接收方的接收问题。这个技术的局限性在于目前接收方必须要扫描网络中的所有交易（这在物联网世界中并不理想），或是要依靠可信的完整节点（在一定程度上泄露隐私）的帮助以完成接收。 支付代码的设计旨在解决隐藏地址的上述缺点，但仍有泄露交易隐私的缺点。 为

了进一步减少隐私泄漏，我们在原始付款代码技术的基础上设计了可传递的支付代码。欲了解更多详细信息，请参阅我们的原版白皮书 [11]。

5.2 保密交易机制

图 14 显示了比特币区块链上的一个典型交易。本质上，区块链交易只是一个元组 ({pkin,i}, {pkout,j }, {vi,j }),，其中{pkin,i}是输入地址，{pkout,j }是输出地址，{vi,j }是输入和输出地址之间的交易金额。由于比特币交易是以明文形式存储在公共账本中，因此引发了很多安全和隐私问题。保密交易的目标（见图 1）是使只有交易的发送方和接收方能够知道{vi,j }值，并没有其他人知道交易双方以及{vi,j }值。此外，保密交易可以允许网络实体验证每个交易的有效性，但是交易的实际金额不会被泄露。区块链上的保密交易的实现需要许多先进的密码技术。我们的目标是提出一种能够在通信和计算成本之间实现良好交易的创新型保密交易机制。有关更多信息，请参阅我们的原始白皮书[11]。

5.3 通过 Bulletproofs 模型证明交易金额范围

Bulletproofs 模型是为了替代佩德森承诺协议(Pedersen commitment)而被提出的。这是一种新的非互动零知识证明协议模型(noninteractive zero-knowledge proof protocol)，它仅需非常短小的证明签文（proofs）并且不需要仰赖可信任的节点，因此可以在没有额外计算量的条件下，将范围证明(range proof)的大小从线性减小到次线性，并进一步减少交易体量。由于 Bulletproofs 模型很好地符合 IoTeX 的设计原则，我们将把防弹协议(Bulletproofs)整合到 IoTeX 中。

6 即时最终性的高速共识机制

6.1 技术背景

工作量证明算法（PoW）是实现大多数区块链（包括比特币和以太坊）全球共识的支柱。工作量证明算法（PoW）使在计算上很难构建一个有效的区块并将其附加到区块链上。区块链变得越长，就越难扭转区块链以前记录的任何交易。攻击者必须拥有基于 PoW 的区块链网络整个计算能力的 51%，才能操纵该区块链。

虽然 PoW 为大型分布式区块链的全球共识提供了一个优雅的解决方案，但它也有一些固有的局限。 维持共识整体计算成本很高，相当于 51%的攻击成本。这意味着即使大部分区块链参与者都是诚实的，他们仍然需要使用大量的电力来维护区块链，这不适合倾向于节能的物联网网络

环境。另外，在单个设备级别上，使用 PoW 通常会花费大量的 CPU 周期和内存空间，这为嵌入式物联网设备的硬件制造和成本设置了较难的要求。

6.2 共识机制：随机授权股权证明机制 (RoII-DPoS)

为了设计和开发 IoTeX 的快速高效的共识机制，我们计划采用以下技术。

6.2.1 股权证明机制

为了避免以上提到的因 PoW 所带来的问题，我们建议使用权益证明算法（PoS）作为区块链达成共识的有效替代方案。PoS 的基本思想是随机选择一组节点对下一个区块投票，并根据它们的资金量大小（即权益）对他们的投票进行加权。 如果某些节点行为不当，系统可能会没收其链上的资金。藉由这种方式，不用通过高计算成本的 PoW，区块链依旧可以更高效地运行，除此之外可以实现链上的经济稳定性：参与者拥有的权益越多，其维护账本共识机制的动机就越大，其节点行为不当的可能性也就越低。现在已经有一些根据权益证明算法（PoS）研发的设计和使用，例如 Tendermint [24]，已被许多应用程序采用[25]。

6.2.2 授权股权证明机制

授权股权证明（DPoS）改进了 PoS 的思想，即授权股权证明允许参与者委托一些代表来代表他们在网络中的部分股权。 例如，Alice 可以向网络发送消息，委托 Bob 代表她的股权并代表她投票。 DPoS 为我们的物联网应用提供了以下优势：

- 小股权参与者可以将他们的股权集中起来，让他们有更高的机会共同参与区块链中的投票，然后分享奖励。
- 资源受限的节点可以委任代表，因此并非所有节点都需要保持联机才能达成共识。
- 代表可以是具有强大电力供应和网络条件的节点，也可以动态随机选择，因此我们在链上将获得更高的整体可用性，使网络达成共识。

使用 DPoS 的加密货币包括 EOS [5]和 Lisk [14]。

6.2.3 拜占庭容错算法

实用的拜占庭容错算法（PBFT）是 Castro 和 Liskov 在 1999 年提出的一种有效的抗攻击算法，用于在分布式异步网络中达成协议。 我们计划使用 PBFT 作为我们 DPoS 共识机制的基础投票算法，因为它是一种简洁而且研究得非常好的算法，它提供了快速的结算性，这对于构建高效

与可扩展的区块链至关重要。 正如 Castro 和 Liskov 的原始论文所证明的那样，只要低于三分之一的网络节点出现故障或恶意行为，PBFT 就可以为链提供可用性和安全性；同时，PBFT 的网络成本非常低，仅为未复制网络系统成本的 3%。

基于 PBFT 的加密货币包括 Stellar [23]和 Zilliaq [29]。

6.2.4 基于随机功能可验证的随机共识机制 (RoII-DPoS)

如上所述，为了效率考虑，当要提出或选举新块时，系统将随机选择一小组节点。 这种随机选择算法的设计非常重要，因为它影响了整个共识过程的公平性和安全性。 最近一组麻省理工学院的研究人员-Yossi Gilad 等人提出了 Algorand [8]算法，这是一种基于可验证的随机函数（VRFs）的有效 PoS 共识算法。

VRFs 的概念是由 Micali et al. [15]提出的，指的是可以随机输出公开可验证的数据。 通过使用 VRFs，参与者可以私下检查他们是否被选中于每轮提议或投票，然后发布他们的 VRFs 证据和区块提案或投票。通过使用 VRFs，我们可以提高网络效率并避免有针对性的攻击，因为所有被选参与者只需向网络广播一条消息。

6.3 轻量级用户定期检查点的创建

在物联网网络中，我们预计很多设备都是轻度使用的客户端，也就是参与者不会在本地记录完整的交易历史。以比特币为例，目前存储完整比特币区块链需要的空间已经超过 100GB [1]，因此许多嵌入式低成本物联网设备可能无法下载完整区块链。 为了缓解这一性能问题，以太坊的发明者 Vitalik 建议在区块链上创建定期检查点：epochs [3]，例如每隔 50 个区块设置一个 epochs。 每个检查点都可以基于前一个检查点进行验证，这样轻量级客户就可以更快地同步整个区块链。

7 IoTeX 网络中的通证机制

本地数字通证（IOTX）是 IoTeX 网络生态的重要组成部分，它被设计成完全服务于 IoTeX 网络。在 IoTeX 主网启动之前，通证是以兼容 ERC20 标准部署于以太坊网络上的，待到主网发布后，通证会完全迁移至 IoTeX 主网上。

IOTX 通证作为一种虚拟加密“燃料”被用于在 IoTeX 网络上实现某些功能（比如执行转账和运行分布式应用），通过消耗 IoTX 通证激励社区参与者,维持 IoTeX 网络上的生态。在 IoTeX 网络上执行转账和运行分布式应用以及验证添加区块/信息需要占用很多的计算资源，因此我们需要

激励这些提供服务/资源的网络参与者（即挖矿）以保持 IoTeX 网络的完整，IoTX 通证还被作为一种汇率单位用于支付占用计算资源所产生的费用。IoTX 通证需要 50 年才能挖完，挖矿奖励会随着时间的推移而线性下降。

IOTX 通证是 IOTEX 网络中不可或缺的一部分，如果没有 IOTX 通证，那么就没有一种汇率单位去支付这些费用，从而使 IOTEX 的生态系统无法持续。

IOTX 通证作为一种支付单位具有不可逆的功能，将被用于 IOTEX 网络参与者的转账交易中。引入 IOTX 通证的目的是为生态系统中的网络参与者提供一个便捷安全的支付结算模式。IOTX 通证并不代表任何股权、参与权、投票权、职位、以及 IOTEX 基金会的收益。基金会及其分支机构，或其他公司、企事业单位不会给通证持有者承诺任何利润以及投资回报，也不会在新加坡或任何相关管辖区内构成有价证券。IOTX 通证只能在 IOTEX 网络上使用，并且通证持有者没有被授予任何明示或暗示的权利，除了正确使用 IOTX 通证以促进 IOTEX 网络和谐发展。

关于 IOTX 通证，需特别注意：

(a) 基金会及其任何附属机构没有对通证进行退款或者变现（或者替换成等值的其他虚拟货）或者其他任何支付方式的义务；

(b) 通证不会使通证持有者获得基金会（及其任何附属机构）任何形式的权利、收益或资产，包括但不限于基金会有权获得的未来收益，股票，股权或股份，证券，任何投票、分配、赎回、清算、产权（包括所有形式的知识产权），或者与其他金融、法律同等的权利，或者与 IOTEX 网络参与者、基金会、服务供应商有关的任何知识产权。

(c) IOTX 通证并不是一种货币（包括电子货币），有价证券，商品，债券，债务或其他任何一种金融工具或投资;

(d) IOTX 通证不是基金会或其任何附属机构的贷款，也并不是基金会或其任何附属机构所欠债务，且没有任何预期的利润;

(e)基金会及其任何附属机构不会授予 IOTX 通证持有者任何权利或者收益。

8 IoTeX 驱动的生态系统

IoTex 区块链支持多样的物联网生态系统，包括共享经济、智能家居、自动驾驶汽车与供应链等。不同类型的开发者用不同的方式使用 IoTex。IoTex 支持的开发者包括物联网硬件制造商、物联网设备控制系统开发商、智能家居应用程序开发商、共享经济设备制造商、供应链数据整合商、数据众包供应商、自动驾驶车辆开发商等等。本章将描述部份可由 IoTex 驱动的生态系统。

8.1 共享经济

近年来，许多公司集中发展共享经济：大到如优步、Lyft、滴滴等叫车平台，以 Airbnb 为代表的房屋共享，又如摩拜、ofo 等运营的共享单车，小到移动充电宝或雨伞等小型物品的共享。即使其中几家公司正受到其商业模式的限制，这些共享都使得人们的生活更加便利。比起商业模式，我们更专注于分析他们的技术架构。在所有的共享经济分类中，共享汽车服务是唯一无法避免人类操作的领域，因此这并非是由物联网推动的经济类型。尽管如此，在未来自动驾驶技术成熟且广泛运用后，物联网技术也将带动共享汽车服务。

所有由物联网驱动的共享经济都具备一些相似处:它们都需要一道在定金或租金支付后方能打开的锁，那么运用物联网设备来完成整个共享与退还流程就会是相当可行且高效的。在中心化的世界中，共享经济是由中心化的云端服务推动，这种做法存在三个缺点:

1. 控制大笔押金的公司有不守信的可能。近期，在中国发生了许多起用户无法从共享单车服务运营商处取回押金的案例。

2. 共享经济并非完全由社区驱动。许多共享服务是由单一公司主导，这将导致社会资源的浪费。以共享单车为例，当共享单车公司倒闭退出市场后，所有单车将无法合理处置。

3.由于中心化特性，用户数据将由单一公司储存并控制。这会产生云服务器或客户端被黑客入侵并盗取用户数据的风险。

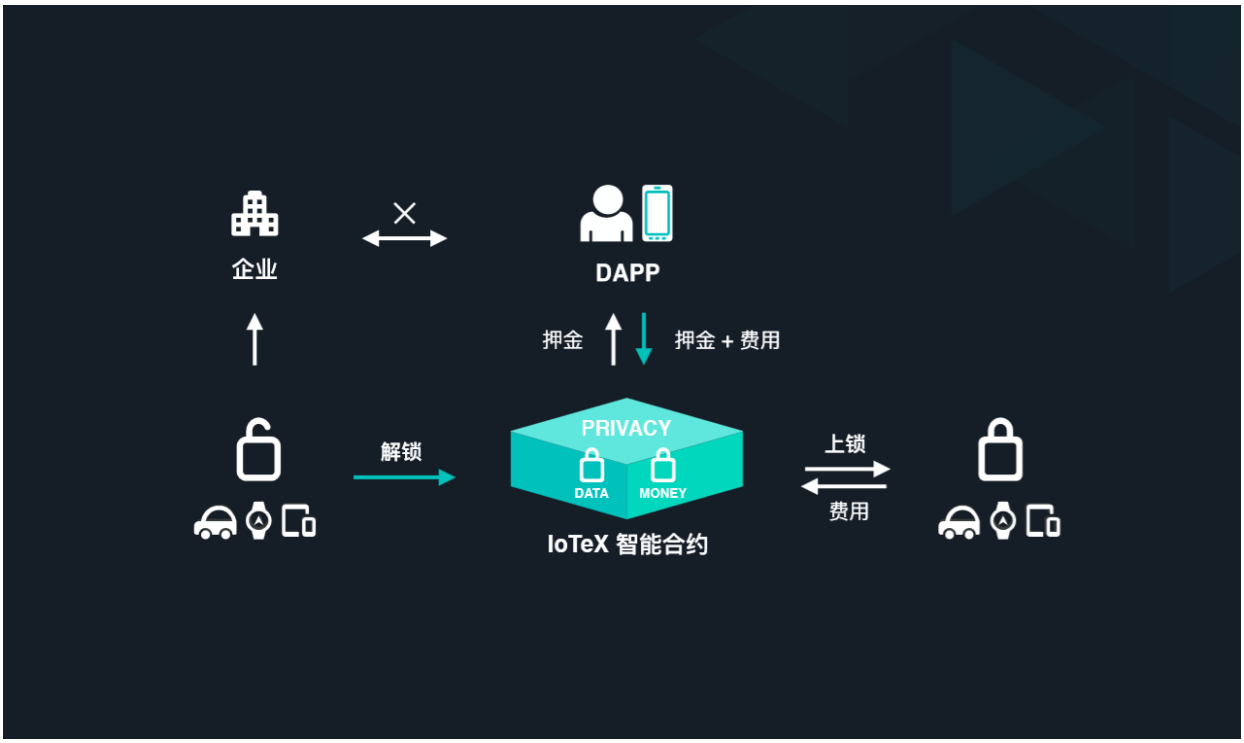
身为基础设施的 IoTeX 可在避免上述缺陷的前提下驱动这类应用，并使共享经济去中心化且更有效率。一个由 IoTeX 驱动的共享经济将具备以下的优势:

1. 押金支取完全由智能合约处理。由于无任何一方可以操控资金，押金的退还过程将受到保证。用户不必为了使用服务而信任某家公司。

2. 每件共享的事物都自主地认知到自身的价值与任务。在这样的生态系统中，共享的事物归谁所有无关紧要。每个人都能够拥有共享生态系统并为之作出贡献。这类经济能够由社区经营，从而让公司能够专注于物联网锁的维护和社区管理。这种轻量级的商业模式使得公司得以迅速成长，服务更广大人群。

3. 再次强调，用户不必信任某公司对其数据进行管理。用户的数据将存储于区块链并获得隐私保护。

图 2: IoTeX 驱动的共享经济



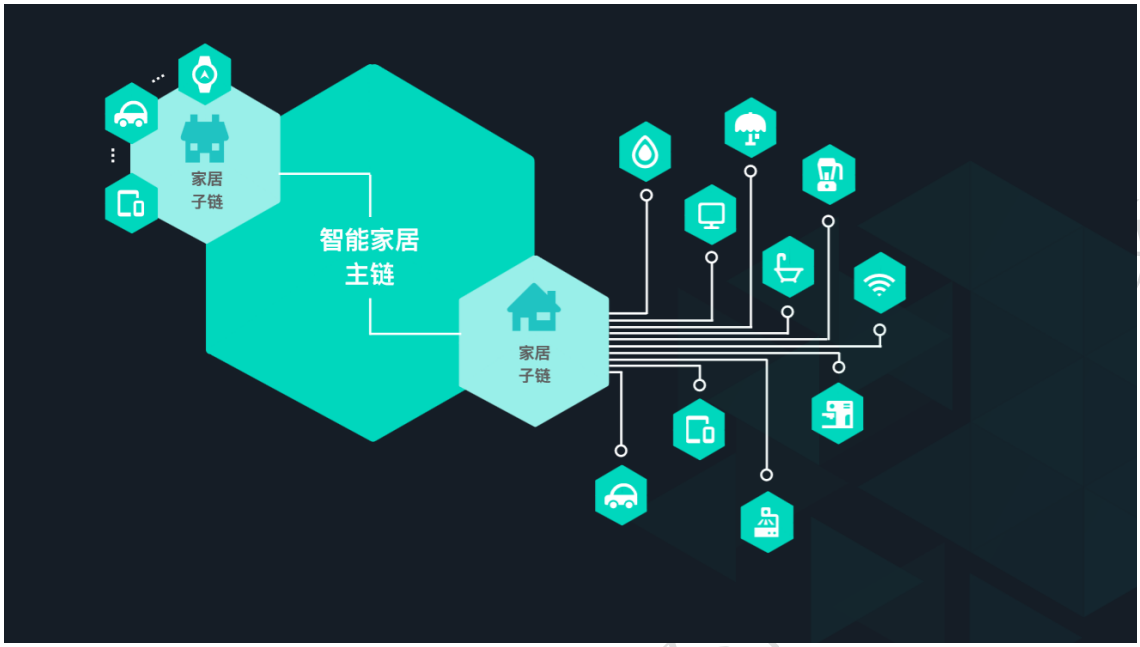
8.2 智能家居

现存的智能家居市场中，许多物联网设备制造商仍在使用过时的技术开发产品，耗费心力发展云服务。由于这样的发展方向难以避开云服务，导致开发与维护的成本高且成效不显著。而在 IoTex 区块链上部署他们的产品将会大幅缩减工程与云计算上的成本，同时大幅提升其设备的效能。举个简单的例子，智能灯泡在使用云端技术的情境下，从用户下指令到改变灯泡的状态许要两个阶段的运作。制造商并非云技术专家，他们通常无法提供最优质的云服务，使得整个改变灯泡状态的过程需耗时一到三秒。这迫使他们使用大型 IT 公司提供的云服务。使用这些服务有以下三个缺点:

1. 制造商无法完全控制云服务的可获得性。
2. 尽管他们一次性售卖物联网设备，却必须不断向云端服务商付费。
3. 云服务、客户端或内网可能被黑客攻击，用户数据被窃取的风险，造成家庭安全隐患。

相比之下，IoTeX 区块链能够在本地管理设备并在有需要的时候与网络上的公共链进行交互。公共链由社区维护，所以物联网制造商无需支付维护费用。IoTeX 区块链具有隐私保护机制，可以避免数据外泄。 即使在内网不安全的情况下，仍能避免黑客取得控制权。

图 3：以 IoTeX 为基础的智能家居



此外，为了方便物联网制造商在 IoTeX 区块链上部署他们的设备，IoTeX 将与物联网芯片制造商合作开发专属芯片来缩短物联网设备的设计与制造周期。物联网制造商只需将芯片整合进他们的设备即可。

8.3 身份管理

物联网的发展已经对身份认证与访问控制服务 (Identity and Access Management, IAM) 运作方式产生影响。就事物的身份认证而言，IAM 必须能够运行用户对设备、设备对设备，与/或设备对服务/ 系统。得益于 IoTeX 区块链的不可篡改性，一个实现身份认证管理的直接方式是将 IoTeX 区块链作为去中心化的公钥基础设施 (PKI)，其中每一个实体都会分配到一个 TLS 证书形式的加密身份验证，从而获得隐私保护。这个短生命期的证书由内嵌于设备中的长生命期的证书签发，并在 IoTex 区块根链或子链上发布。用户或其他实体能够访问并且信任这个锚定在区块链上的短生命期证书，进而鉴真连接到线上的实物，确保设备、服务与用户间的安全沟通，并且保证其完整性。

此外，内嵌于设备中的长生命期证书能够像传统的 PKI 那样建立层叠结构，上层设备可对下层设备签发证书。在层叠结构中，凭证的撤销与转移将成为可能。举例来说，假若一个设备出现问题，它的上层设备或再上层设备能够签发一个撤销指令发送至区块链，区块链可进而使该设备的凭证失效。

9 潜在研究方向

IoTeX 团队目前致力于如下研究方向：

面向隐私保护的计算：

这里列出在这一技术方向上我们正在积极探索的几个领域：

- 区块链上一组节点如何进行面向隐私保护的计算
- 在合约内容加密的情况下由虚拟机执行面向隐私保护的智能合约。尽管全同态加密[20]以及不可区分的代码混淆技术[7]在理论上能够实现面向隐私保护的智能合约，最近提出的基于零知识证明的方案例如 Hawk[13]为面向隐私保护的智能合约在实际系统中落地提供了解决方案。
- 进一步减少 IoTex 的区块链隐私保护技术所需的算量与存储需求。
- 针对 IoTeX 目前使用的隐私保护技术研究后量子版本，例如后量子环签名技术

状态裁剪与转移

因为许多 IoT 设备的存储空间有限，我们正在评估不同的方法来安全地裁剪存储在子链上的信息，以减少存储内容。对块和交易信息的压缩并非难事。此外，以一种高效和隐私保护的方式将信息从子链转移到主链(因为后者在存储方面更强)上也是一个有趣的话题。

区块链治理与自我修正

虽然 IoTex 区块链为维持其帐本共识的支持者们提供奖励，但到目前为止还没有一种链上机制可以精确修正治理协议的规则并对协议的发展提供奖励。我们将进一步研究区块链治理与自我修正机制以解决此问题。

树状架构的区块链

目前 IoTeX 系统为两层式区块链架构，在将来它可以利用 Plasma 和 Cosms 的技术扩展成树状结构。我们计划进一步评估现有方案旨在将 IoTeX 打造成为可以支持复杂层次化结构的区块链项目。

10. 结论

在白皮书中，我们介绍了一种可扩展的、注重隐私保护并具有延展性的物联网区块链，并且介绍了它的架构以及如下核心技术：

1.运用链中连架构最大化扩展性和隐私；

2. 运用轻量级秘密地址、长度固定的环签名（无需“可信启动”）以及 Bulletproofs 机制保护交易隐私；

3. 运用可验证的随机函数以及权益证明实现高速共识机制；

4. 构建灵活的轻量级 IoTeX 系统架构。

11. 特别鸣谢

在此感谢在此白皮书撰写过程中给予我们及时反馈并提出宝贵意见的各位导师、顾问，以及许多致力于物联网、密码学、虚拟货币领域的专家和伙伴。

参考目录

[1] *Blockchain Size*. https://blockchain.info/charts/blocks-size.

[2] Benedikt Bu¨nz et al. *Bulletproofs: Efficient Range Proofs for Confidential Trans- actions*. Cryptology ePrint Archive, Report 2017/1066. https://eprint.iacr.org/2017/1066. 2017.

[3] Vitalik Buterin. *Light Clients and Proof of Stake*. https://blog.ethereum.org/2015/01/10/light-clients-proof-stake/.

[4] Miguel Castro, Barbara Liskov, et al. “Practical Byzantine fault tolerance”. In: *OSDI*. Vol. 99. 1999, pp. 173–186.

[5] *EOS*. https://eos.io/.

[6] AB Ericsson. “Ericsson mobility report: On the pulse of the Networked Society”. In: *Ericsson, Sweden, Tech. Rep. EAB-14* 61078 (2015).

[7] Sanjam Garg et al. “Candidate indistinguishability obfuscation and functional encryption for all circuits”. In: *SIAM Journal on Computing* 45.3 (2016), pp. 882– 929.

[8] Yossi Gilad et al. “Algorand: Scaling byzantine agreements for cryptocurrencies”. In: *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM. 2017, pp. 51–68.

[9] *HDAC Blockchain for IoT*. https://hdac.io/.

[10] *Internet of Things (IoT) Market by Software Solution (Real-Time Streaming Analytics, Security Solution, Data Management, Remote Monitoring, and Net-*

work Bandwidth Management), Service, Platform, Application Area, and Region
- Global Forecast to 2022. https://www.jasper.com/sites/default/files/ cisco- jasper- hidden- costs- of- delivering- iiot- services- en_2.pdf. 2016.

[11] *IoTeX IoTeX Whitepaper*. https://IoTeX.io/white-paper.

[12] *ITC Blockchain for IoT*. https://iotchain.io/.

[13] Ahmed Kosba et al. “Hawk: The blockchain model of cryptography and privacy- preserving smart contracts”. In: *Security and Privacy (SP), 2016 IEEE Sym- posium on*. IEEE. 2016, pp. 839–858.

[14] *Lisk*. https://lisk.io/.

[15] Silvio Micali, Michael Rabin, and Salil Vadhan. “Verifiable random functions”. In: *Foundations of Computer Science, 1999. 40th Annual Symposium on*. IEEE. 1999, pp. 120–130.

[16] *Monero – Private Digital Currency*. https://getmonero.org/.

[17] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. 2008.

[18] Serguei Popov. “The tangle”. In: *IOTA* (2016).

[19] *Raiden Network*. https://raiden.network/.

[20] Ronald L Rivest, Len Adleman, and Michael L Dertouzos. “On data banks and privacy homomorphisms”. In: *Foundations of secure computation* 4.11 (1978), pp. 169–180.

[21] Nicolas van Saberhagen. *Cryptonote v 2. 0*. 2013.

[22] Samsung. *Samsung ARTIK and Successful Strategies for Industrial IoT Deploy- ment*. Samsung, 2016.

[23] *Stellar*. https://www.stellar.org/.

[24] *Tendermint*. https://tendermint.com/.

[25] *Tendermint Ecosystem*. https://tendermint.readthedocs.io/en/master/ ecosystem.html.

[26] *The hidden costs of delivering IIoT services*. https : / / www . jasper . com / sites/ default / files / cisco - jasper - hidden - costs - of - delivering - iiot-services- en_2.pdf. 2017.

[27] *WebAssembly*. http://webassembly.org/.

[28] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. “Privacy in the Internet of Things: threats and challenges”. In: *Security and Communication Networks* 7.12 (2014), pp. 2728–2742.

[29] *Zilliqa*. https://www.zilliqa.com/.