

自主商业应用的区块链燃料

aergo

摘要

区块链是一种全新的技术形式，它首次引入了一个基于密码学的用于转账的数据库，该数据库规避了传统数据库经常出现的故障点和安全问题。其独特属性为基于区块链的产品和服务提供了打破许多行业中存在的固化商业模式（例如金融服务，制造业，零售业，保险业，医疗保健业，政府和物联网（“IoT”））。区块链技术为企业提供的技术改进主要体现在以下三个重要特征：

安全性 - 透明性 - 可信性

它通过使用分布式计算的点对点（“P2P”）网络来实现这一点，在该网络中使用高级密码学技术安全地部署和存储数据。引用瑞银前任首席运营官的话：“区块链是一项潜在的变革性技术，在未来 20 年里，它将像互联网在过去 20 年一样，将在我们的世界留下深刻的印记。”¹

区块链技术的优势并没有被忽视，它使许多当下的区块链应用得以实现。其中大多数都在使用和操作比较易于加入和参与的计算机网络。这些无需特别许可的部署方式通常被称为“公有区块链协议”（如比特币和以太坊）。但是，现有区块链的使用给现有业务带来了许多问题，主要是由于缺乏对其功能和开发的控制。虽然私有/联盟链旨在实现“适合目的”的承诺，但它们在基础设施方面需要投入巨大的成本，并且丧失了以开源形态发展的能力。

绝大多数公有和私有链的部署都处于开发的早期阶段（目前使用第三代技术），项目局限于关注公开区块链或仅关注私有区块链。因此，大多数仅用于简单的概念验证（“PoC”）测试用例。尽管有许多这样的项目，但由于企业技术集成的困难以及缺乏开发者友好且易于使用的软件工具，区块链堆栈的发展仍然停滞不前。许多技术实现还缺乏企业级可用性，这对于实际商业应用在公有或私有区块链上运行至关重要。区块链背后的技术需要更加成熟并且变得更容易使其成为广泛使用和部署的架构，它还需要足以提供其他服务和功能才能成为常用的业务平台。

无论谁能够提供支持企业技术所需的协议、开发者和第三方服务，都有机会像 TCP/IP 对于 Internet 一样，对互联网和“无服务器效用计算”的未来产生同样重要的影响。

AERGO 项目（“AERGO”或“AERGO 平台”）是一个非同寻常的突破者。它将成为第四代“企业就绪型”区块链协议，并结合使用新技术和更先进技术的 IT 平台。它提出包括一个综合的补充去中心化应用生态系统（“dApp”）和利用安全云交付模型的服务提供商。

¹ Alex Batlin, et al. (2016). 构建信任引擎 (Building the trust engine), 链接: <https://www.ubs.com/microsites/blockchain-report/en/home.html>

AERGO 的基础技术开源，因为它本质是一个开放和去中心化的系统。

AERGO 为其支持的开发者，企业和 IT 供应商而构建

AERGO 的平台旨在使企业和开发者能够在云端轻松设计、构建和部署自己的区块链应用程序。该平台旨在为创作者提供根据他们的需求定制区块链和应用程序的可能性，让他们可以选择在公共或私人网络上运行。考虑到私有和公有区块链实现的不同特征，两者之间的选择旨在为企业和开发者在设计特定目的的应用程序时提供他们所需的灵活性。AERGO 通过安全的云平台托管分布式网络所有内容，旨在通过使企业不必要建立硬件基础设施以运行区块链协议和应用程序，以减轻企业的开销。

AERGO 的核心技术基于 Blocko Inc. (“**Blocko**”) 的 COINSTACK²，后者是领先的区块链技术和企业信息技术集成服务公司，业务遍及英国，韩国和中国香港。基于 COINSTACK 的区块链系统已经部署到 20 多个生产系统中的 2500 万用户。Blocko 正在为 AERGO 准备和开发一些核心关键技术。它建议为希望部署和维护基于 AERGO 的新产品和服务的客户提供全面的 IT 集成和支持服务。

Blocko 所提供的服务包括：超快速和高效的区块链协议；一个新的强大的 SQL 智能合约引擎；高级 IT 集成 API 以及易于使用的开发者工具。这些部件旨在提供 dApp 编程和部署框架方面的支持，以允许开发者和企业安装、管理和使用这些应用程序。企业可以从公有链和私有链创新中受益，同时专注于构建，部署和管理新服务。简而言之，AERGO 项目旨在提供：

1. 为开发者和承包商提供先进，友好且易于使用的技术
2. 为企业提供安全，快速的公有和私有区块链云架构
3. 一个开放的生态系统，供第三方和企业连接与参与

AERGO, 自主商业应用的区块链燃料

² 第三代区块链平台(包括开发工具、区块链操作系统、集成 API)，官网：www.blocko.io

免责声明

本白皮书以及与本白皮书相关的任何其他文件涉及 AERGO 的预期发展和使用。它们仅供参考并可能随项目发展发生变化。

本白皮书描述了一个未来项目

本白皮书包含基于 Blocko Inc.信念的前瞻性陈述，Blocko Inc.已经将本白皮书作为其持续支持项目的一部分。本白皮书中设想的 AERGO 正在开发中并不断更新，包括但不限于主要治理机制和技术特性。AERGO 通证包含并涉及实验平台（软件）和技术的开发和使用，这些平台可能无法实现或达到本白皮书中规定的目标。如果 AERGO 完成，它可能与本白皮书中列出的网络有很大不同。对于任何计划，未来预测或前景的成就或合理性，我们不作任何陈述或保证，本文件中的任何内容均未被或不应作为对未来的承诺或陈述。

合格购买者

本白皮书中的信息是私下提供给特定潜在购买者的，不应由其他任何人接收或阅读。资格不受保证，可能受到限制。

提供不受监管的产品

AERGO 平台，AERGO 通证或任何在其上运行的通证并非旨在代表任何司法管辖区内的证券或任何其他受监管的产品。

本文件不构成发行证券或任何其他受管制产品，也不构成投资目的的提案，邀请或征集。购买条款并非旨在提供金融服务的文件或任何形式的招股说明书。

AERGO 通证不代表平台或软件中或与平台或任何其他公共或私人企业，公司，基金会或任何其他公共或私人企业或基金会相关的任何公司或知识产权中的股权，股份，单位，特许权使用费或资本，利润，回报或收入的权利。任何辖区内的其他实体。

本白皮书不是购买建议

本白皮书不构成购买 AERGO 通证的建议。不得依赖任何合同或购买决定。

风险提示

AERGO Token 并参与 AERGO Token 销售会带来重大风险。

在购买 AERGO Token 之前，您应该仔细评估并考虑风险，包括任何其他文档中列出的风险。

本白皮书中表达的观点

本白皮书中表达的观点和看法是 Blocko 的观点和看法，并不反映任何司法管辖区内任何政府，准政府，权力机构或公共机构（包括但不限于任何司法管辖区的任何监管机构）的官方政策或立场。本白皮书中包含的信息基于被认为可靠的来源，但无法保证其准确性或完整性。

英语是本白皮书的授权语言本白皮书及相关材料仅以英文发布

任何翻译仅供参考，未经 AERGO 或任何其他认证。不保证任何翻译的准确性和完整性。如果本白皮书的翻译版和英文版之间存在任何不一致之处，则以英文版为准。

无第三方合作或背书

本白皮书中对特定公司和平台的引用仅用于说明目的。使用任何公司和/或平台名称和商标并不意味着与任何一方有任何关联或认可。

您必须获得所有必要的专业建议

在确定是否购买 AERGO 通证或以其他方式参与 AERGO 项目之前，您必须咨询律师，会计师，税务专业人士和/或任何其他专业顾问。

本白皮书未经任何司法管辖区的任何监管机构审核。本白皮书中对特定公司，网络和/或潜在用例的引用仅用于说明目的。除明确提及的合作伙伴或提供商（如 Blocko Inc.）外，任何其他公司和/或平台名称和商标的使用并不意味着与任何这些方的任何关联或认可。

除非另有明确说明，否则金额以美元（“USD”）表示。

内容目录	
摘要	1
免责声明	3
执行摘要	6
企业市场机遇	
机遇	8
障碍	13
AERGO	17
AERGO CHAIN	22
AERGO 公有 & 私有存储库	32
AERGO HUB	34
AERGO MARKETPLACE	36
原生区块链资产与通证模型	38
通证分发和资金使用	39
发展路线图	40
执行计划	41
附录	
附录-A: 区块链和开放平台入门	43
附录-B: 区块链和效用计算	53
附录-C: 私有与公有企业区块链	60
附录-D: AERGO 团队和顾问	63
附录-E: 专业术语	67

执行摘要

当 Satoshi Nakamoto 在 2008 年向世界推出比特币时，这种全新的加密货币意味着在不需要银行介入的情况下直接在个人之间实现电子现金支付。十年后，这种 Nakamoto 为比特币发明的突破性技术正在被各行各业的企业所支持，以此作为从根本上改善未来产品，服务和业务的一种方式。

随着数字世界转向下一代应用计算模型（在开放网络和高度分布的生态系统中创造价值），区块链有可能成为构建这些系统和生态系统的主要企业平台之一。

在这个新世界中，人们可能会将注意力从开发者必须了解和满足复杂的 IT 架构以及相应的管理和操作功能。这有助于他们专注于前端的应用程序创新和价值创造，应用程序可以接触到并与终端用户（以及数十亿未来的物联网设备）进行交互。在这种“无服务器架构”中，大部分 IT 复杂性将被抽象或仅仅隐藏在开发者和最终用户之外。应用程序将作为容器和微服务在安全的私有云和公共云的组合上运行，由各种托管云合作伙伴交付。

为了实现成为这种应用计算世界的主要平台之一的承诺，需要逐步改变。不仅围绕区块链操作系统本身的核心元素，而且在创建一个全新的“企业区块链平台”和相关的生态系统。这些需要支持在区块链上创建，部署和管理基于安全分布式微服务的新应用程序。

要成为主流（以便公司和第三方能够在这个新世界中创造价值），技术，工具和方法需要强大，易于使用并保证低成本。

本文介绍了 AERGO：**下一代企业级区块链协议和平台**。AERGO 旨在成为众多行业中应用程序开发者和企业公司使用的核心主流 IT 架构和模型之一。可以预计，基于 AERGO 将会出现数以千计的创新的产品、服务和商业生态。

预计将出现数千种在 AERGO 上建立和运行的创新产品，服务和商业生态系统。

为了解释当前和未来的目标市场（即描述现有问题和未来的商机），本文总结了一系列重要的企业需求，以及快速发展的 IT，技术和区块链趋势。虽然描述了许多技术概念，但其中许多已被简化以便以商业友好的方式解释它们。我们还通过附录（例如附录 A 中的区块链“Primer”）提供了有关每个核心主题的更详细信息。

AERGO 的核心要素建立在 Blocko 开发的技术之上。Blocko 是一家领先的区块链公司，已帮助一些世界领先的公司安全区块链上设计和部署实际商业系统。Blocko 在过去的四年里收货

良多。Blocko 相信其现有的核心技术和先进的区块链生产能力可以构成一个新的先进区块链业务平台的基础，目前经过验证的技术已经有超过 2500 万用户使用³。

Blocko 正在为 AERGO 贡献其核心技术。它还可能为 AERGO 提供未来服务，包括为 AERGO 的未来客户提供咨询和维护服务。

随着开源平台开发水平不断提升，并实现在开发者和企业中更高水平的应用，预计其他公司可能会为 AERGO 提供与 Blocko 类似和互补的服务。

³ Gil, Jae-sik (2018). “新汉金融集团将打造基于区块链的单点登录应用 (Shinhan Financial Group to Build Blockchain-based Single Sign-On App).” ETNews.com, 2018 年 1 月 22 日, 链接: www.etnews.com/20180122000304.

机遇

万维网和 IT 技术产业正在发生的重大变化

科技产业充满希望。它也充满了流行语和“下一个大事件”。

事实上，在过去的 30 年里，我们所看到的是 Web 1.0 向 Web 2.0 的逐步演变和过渡。

Web 1.0 为我们带来了基本的互联网、拨号调制解调器、静态(慢速网站)和最基本的移动电话。

Web 2.0 改进并改变了这一点。iPhone 和 Android 智能手机的出现改变了客户相互交流信息的方式(Facebook 等社交媒体网络，或 Twitter、Skype 和 Youtube 等即时多媒体消息和视频服务)。它还改变了企业与市场沟通的方式(通过亚马逊进行电子商务，或通过谷歌进行搜索和广告等)。

Web 2.0 为我们带来了交互式、超连接、沉浸式、虚拟的、数字的在线生态系统，以创建和共享知识、协作和交互。然而，这些系统是建立在高度中心化的巨型平台上的。平台的所有者收集、挖掘和利用大量的用户、客户和业务数据(可能包括更重要的元数据)。数据成了新的石油。然而，就像石油生产一样，很少(企业)能进入生产领域，从这些生态系统中“提取”公允价值。

许多现有的 IT 供应商支持这个价值数万亿美国的行业。构建和销售这些技术和工具允许大型平台提供商在安全的中心化(数据库)系统中收集、管理、分析和货币化这些数据。

简而言之，Web 2.0 使新的商业模式成为可能，但最大的利益(和利润)主要流入少数几家数字全球大公司的资产负债表。

Web 3.0 和所谓的 Web 4.0 是其他流行词汇。不仅于此，他们描述的未来状态，承诺一个更“智能的网络”。其中数据被用来为客户提供个性化的产品和外部服务。其中许多服务将运行和链接在数十亿的移动设备及其他物联网设备上，这些连接也将越来越实时化。

与此同时，IT 技术也正在经历一些重大的强化和变革。在某种程度上，这是由于企业更广泛地采用更安全的云服务。这也是由于越来越多的开源平台被广泛采用(比如 Linux 作为操作系统和 Hadoop 或 TensorFlow 来收集和利用大数据)。软件程序员最常用的开发工具和中间件现在几乎都基于开源项目，越来越多的开发者希望在开源平台上创建新应用程序。

上述技术因素为开发基于低成本商品(如 IT 架构)的新服务提供了一种全新的方法。这就是我们所说的“效用无服务器计算 (Utility Serverless Computing) ”。

在这种“无服务器体系结构”中，开发者和企业研究的重点将从理解复杂编程语言转移开来，他们也将不再需要创建和管理复杂的 IT 架构。IT 的复杂性将被简化，或者只是对开发者和最终用户隐藏；从而研究使用的焦点就可以转移到应用程序和服务本身。这是一种心态的转变和注意力的转移。

预计到今年年底，全球 IT 支出将达到 3.7 万亿美元⁴；预计在三年内将超过 4 万亿美元。国际电信联盟单独估计，到今年年底，将互联网用户约 32 亿人，几乎占世界人口的一半。其中大约 20 亿人来自发展中国家。

这些用户将产生大量的数据，这些数据将四处流动。正如大型数字公司所意识到的那样，个人信息是一项极其宝贵的资产。在过去的 20 年里，中央服务器上存储了大量数据，其中谷歌、亚马逊、Facebook 和 Twitter 是最大的保管人。为了使用这些便利的服务，人们牺牲了隐私和数据所有权。不管他们是否意识到他们的身份、浏览习惯、搜索和在线购物信息都被卖给了出价最高的(广告)竞标者。

与此同时，这些技术和互联网创新正在发生，世界各地的消费者、企业和政府对个人和企业数据的收集、存储和访问(使用)变得越来越精明，并提出了更高的要求。在一些特定的司法管辖区(如：通用数据保护条例“**GDPR**”)⁵已经推出了新的法例。

今天，一些数字巨头已经创建了领先的解决方案，这些解决方案使他们能够在 Web 2.0 的机遇中获得不成比例的份额，这些解决方案提供了垄断性的数据饥渴 (data-hungry) 服务，这些服务运行在高度保护的 centralized 的封闭生态系统和数据库中。

然而，在新兴的(更能感知数据的)下一代“效用无服务器程序计算”世界中，通过在更开放、更可信的分布式生态系统中获取价值，新参与者有巨大的机会创建创新的产品和服务。

随着这种体系结构方法的成熟，我们相信，在几乎涉及数字资产交换的行业的每个部门，将有越来越多的新业务项目采用这种方法。

例如，Everest Group 预测区块链将在未来几年内加速在银行业的应用(见第 57 页图 24)。

我们相信这个新世界是互联网的下一个阶段：以人为中心的去中心化互联网。

⁴ Anon. (2018). *Gartner 表示 2018 年全球 IT 支出将达到 3.7 万亿美元*. 链接: <https://www.gartner.com/newsroom/id/3845563>

⁵ EU Parliament. (2018). *欧盟通用数据保护条例*. 链接: <https://www.eugdpr.org/>

区块链的角色

尽管区块链在技术方面还很年轻和稚嫩，但它仍然为开发者和企业提供了最创新、最安全、最透明和最可信的方法，以在更加开放和可信的未来分布式生态系统中捕捉价值。

民主化就是这个想法。区块链提供了这个方法。

有史以来第一次，我们能够创建一个去中心化的网络体系结构，从而在没有第三方(控制)中介的情况下，安全地、高效地达成跨整个网络的共识(关于信任、数据完整性和治理)。

区块链系统旨在创建一个统一的、通用的、绝对可靠的、不可篡改的数字资产和相关交易记录(账本)。

它能够以比现在使用的工具更好、更有效的方式实现这一点。首先，区块链技术为加密编码的交易创建了一个可行的、去中心化的记录(分布式分类账)，这允许用故障中心点和其他安全问题替换传统的主数据库。区块链帮助的最关键领域是确保交易记录的有效性，它不仅记录在主寄存器上，而且记录在连接的分布式数据库系统上，所有这些数据库都通过安全验证机制连接。

第二代区块链技术允许一个点对点网络管理它们自己的“智能合约”——区块链上的计算机程序，一旦符合标准，就自动执行它们的条款，无需中介。

在平台层面，我们相信这有可能使许多数字生态系统的大部分得到根本性的简化和成本降低，同时使它们更加开放、安全和可靠。用户和业务数据以安全的分布式方式收集和存储。这也防止(现有的和未来的)科技巨头为了自己的商业利益而囤积和滥用相同的数据。

然而，也许最令人兴奋的开发领域将是运行在区块链系统上的 dApp。

dApp 是去中心化应用程序的缩写形式。dApp 的后端软件代码运行在去中心化的对等网络上。与此相比，典型的应用程序的后端代码运行在中心化的服务器上。

尽管主流互联网用户对数字应用程序对特定行业的好处仍知之甚少，但它们显示出了巨大的潜力。

使用 dApps 的服务支持创建以用户和业务为中心的 web，用户和客户保留对其数据、身份和数字资产的完全所有权。

dApps 的一些主要潜在好处包括:

- 供应链和价值链的大规模简化(消除“中间人”)
- 能够自动(随时)结算交易和完成交易

- 精准的现收现付业务交易
- 改进存储的数据和应用程序的安全性(就不变性而言)
- 业务增长(更快、更可靠的交易)
- 降低管理费用(如人员和设施)
- 交易欺诈防范(终极信任机器)
- 显著降低平均交易成本(更简单的总体架构)

对于 dApp 的无服务器实用程序计算实现，存在许多潜在的用例。

尽管无服务器 dApps 的采用仍在进行中，但早期指标显示，它们将成为企业通过基于安全和分布式云服务交付新服务的主要力量。

还有很多关于概念验证的文章，甚至还有一些(简单的)区块链的生产部署。然而，目前区块链面临着许多挑战，尤其是如果它要被企业规模的企业采用的话。

这些包括:

- 开发者和 IT 承包商很难为区块链编写应用程序
- 有太多相互冲突的实现模型可供选择
- 设计、测试、部署和管理能力对于扩展和运行 dApps 至关重要
- 它通常缺乏业务所需的性能或典型的数据控制
- 将一个新的区块链项目集成到现有的 IT 系统中是非常困难的
- 一个企业可能需要建立多个区块链

简而言之，企业可能会发现支持多个区块链解决方案非常困难。

附录-B 在无服务器效用计算世界中提供了更多关于区块链的详细信息。

走进 AERGO

如前所述，今天区块链面临着挑战。然而，我们坚信从长远来看，区块链上开源、安全、分布式的业务生态系统将会最终胜出。

企业商业和开发者需要的是一个功能丰富、开放且易于使用的水平企业级开发和部署区块链的“平台”。不仅仅是另一个区块链协议，而是一个功能齐全的生态系统，以支持和促进众多利益相关方之间的合作。

这个平台需要包括一个“中间件和标准化层”以将 IT 软件无缝连接到分布式无服务器区块链系统中。

为商业、开发者、系统集成人员和其他关键第三方构建的平台，这些第三方都在这些新兴的分布式生态系统中扮演重要角色。

在我们看来，这可能是区块链最具挑战性(但也是最令人兴奋的)的发展领域，我们将可以在未来三到五年看到它的实现。

在全球 IT 支出约 4 万亿美元的情况下，这样一个企业区块链平台可以为企业及其创造者创造并获取重大价值。

这是 AERGO 项目的基本原理和重点。

障碍

对于想要采用和使用公有和私有区块链环境的企业来说有几个关键障碍，而这类挑战或许正好可以解释为什么我们还在许多行业还没有看到在生产中大量部署基于区块链的系统。

缺乏可靠性

缺乏对 IT 基础设施的完全控制会给企业带来操作问题。公有链经常受到“硬分叉”的影响(即有时需要修改底层技术，从而创建原始软件程序的一个完全独立的变体)。当一个公有链遇到一个硬分叉时，dApp 应用程序将继续在新版本的协议上正常运行。当您考虑企业解决方案之间类似于蛛网的关系时，对简单用户应用程序的硬分叉可能会导致严重的商业失败。

硬分叉通常会增加 IT 网络本身的脆弱性，从而使其容易受到诸如网络重播攻击或拒绝服务 (“DDoS”) 攻击等问题的影响。例如，原始的比特币区块链协议已经有了很多硬分支(参见图 1)。

随着区块链应用的增长，底层技术需要改进(例如提供更高级的可扩展性)，这还需要运行软件的所有节点升级到协议软件的最新版本。我们相信未来区块链硬分叉意愿会随着区块链技术的需求而上升。这使得企业部署区块链不仅难度极大，而且在某些情况下无法满足企业对 IT 稳定性的需求。

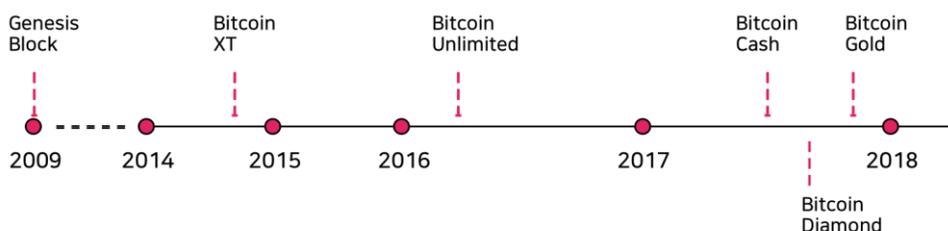


图 1. 比特币区块链硬分叉历史

区块链的另一个问题是交易费用的高波动性。我们看到比特币 90 天的平均单笔交易价格涨到了 110.96 美元⁶。截至 2018 年 3 月 18 日，约有 1000 笔交易在等待处理。这种波动性使得区

⁶ Blockchain Info. (2018). 90 天平均数：从 2017.12.19 至 2018.03.18。链接：<https://www.blockchain.info>

区块链上的商业应用不可预测且不可持续。一般来说，企业会因运营成本的不确定性而拒绝采用新技术。

信息技术集成困难

几十年来，各种规模的企业都在利用数字技术优化和转型。这种情况经常发生在不同时期，导致在层间进行测试和部署差异化系统。这进而导致了复杂的操作和工作流。因此，企业基础设施往往依赖于各种各样的技术和流程。

将一种新的颠覆性技术(如区块链)集成到传统的复杂(通常是专有的)系统中可能高难度、高风险且高成本。尽管安全断言置标语言(Security Assertion Markup Language, “SAML”)或 web 访问授权标准和身份验证参考体系结构(web access delegate standard and reference architecture for authentication, OATH)等开放标准会有所帮助，但要使一个新的 IT 系统能够完全使用 Active Directory、Oracle 或 SAP 等广泛使用的产品，是一项非常复杂的任务。

软件开发困难

像区块链这样的新技术常常引入新的编程框架和语言。由于大多数企业开发都倾向于以项目为中心，开发者几乎没有空间进行试验并学习新的语言和工具。

其中一些是复杂的理解，如 Solidity 语言。有了 Solidity 的基础，开发者就可以编写应用程序来实现智能合约中包含的自我执行的业务逻辑，从而为交易留下不可篡改的权威记录。在我们看来，许多公司根本不具备软件开发者使用这些新语言的灵活性或能力。

公司经常使用兼职承包商来交付 IT 项目工作。这些承包商中的许多人不太可能愿意为一个项目学习一门新的语言。如果这些任务是“外包”的，我们认为完全依赖外部第三方来编写和编写区块链重要的业务逻辑和规则是不明智的。

我们认为，企业区块链应该足够容易理解和编程，而不是强迫开发者学习新的语言来创建智能契约。这将允许开发者利用他们现有的专业知识和经验，使用熟悉的工具链(如 C++、Golang、JavaScript 和 Python)。

SQL 也是一种非常容易理解和被广泛接受的编程和管理数据的语言——但是在一些区块链实现中，它似乎几乎被遗忘了。

隐私问题

商界对数据隐私的要求高于目前公链提供的数据隐私要求。当一个方法实现数据隐私和改进安全公有区块链是实现一个加密和解密层在应用程序级别,企业区块链实现通常需要提供一种更健壮的,全面的方法来保护数据,特别是当它涉及敏感和/或受法律保护的信息。

例如,一项新的更严格的 GDPR 标准于 2018 年 5 月在整个欧洲实施。这将要求包括使用区块链(用于其业务)的公司,在设计系统时考虑与数据隐私相关的问题,通过设计实现安全性和数据隐私,而不是事后再考虑。

可扩展性问题

目前的许多区块链足以处理简单的可扩展性。然而,我们认为在许多大规模应用场景中,企业需要 IT 系统能够自动处理来自用户的渐进的或临时的需求。

这种需求可能需要更即时的本地计算资源,即所谓的垂直扩展系统(例如,对于特定的高吞吐量任务,需要更多的本地内存、存储、计算或网络容量)。一个例子可能是一项商业转账(例如,确保于特定的时间点合规交易所内完成特定股票的安全交易)在尽可能短的时间内执行。

当用户需求突然达到峰值时,这就要求 IT 基础设施立即在分布式系统外添加额外的计算机资源来共享额外的负载(在所谓的水平扩展系统中)。这里的一个例子可能是,网上立即出现了对刚刚宣布和正在进行的活动的门票的大量需求(例如,一个世界上最受欢迎的流行乐队之一的演唱会门票已经售罄,因此宣布了一个额外日期)。

互操作性限制

尽管该市场目前仍处于起步阶段,但已经有超过 100 种不同的公链协议被使用——主要支持比特币和许多其他加密的“altcoins”。同时,至少有 200 个定制开发的私有区块链被大型企业开发和使用。区块链的每个实现都是不同的。这降低了跨多样应用场景的规模经济可能带来的好处。

随着市场的发展和成熟(就像过去十年的云计算以及之前的另一个开源项目 Linux 所见证的那样),我们预测,许多区块链部署将会由于缺乏大规模采用而消失,保留下来的一部分将继续存在于更小规模和更专业化的应用中。最成功的项目最终将彼此集成,形成更大的区块链生态系统和平台。

我们相信，未来区块链内部和周围的大部分创新(以及其大规模采用)可能会围绕公共生态系统而不是私有链发展。

每一个区块链平台和生态系统都需要专业工具、IT 集成技术和部署技能。大多数公司将难以跟上能够处理这种互操作性和许多变体私有区块链的可管理性。

如前所述，与公链和私链相结合并协同工作是非常具有挑战性的。特别是这将导致性能下降，并失去这两种系统的重要特性(信任 vs.性能悖论)。

AERGO, 自主商业应用的区块链燃料

AERGO 是一个提出了区块链领域革命性概念的开源项目。

AERGO 平台

AERGO 寻求利用和扩展由现代云架构支持的公有和私有区块链。我们希望创建一个技术和操作框架，支持 dApp 开发者、云交付合作伙伴和企业公司的生态系统。

简而言之，我们的目标是创建一个允许各方创建创新和可信的业务服务的平台。

AERGO 的目标是围绕高性能、安全和易于使用的公链(我们称之为 AERGO 链)构建一个分布式的现代生态系统。

下面的图 2 描述了 AERGO 的一些关键特性。



图 2. AERGO 的关键特点

就像过去 10 年“混合云”的开发、演变和采用一样，AERGO 旨在促进基于混合区块链的产品和商业模式的创建。

AERGO 提议利用先进的技术，具体表现为一个简便易用的区块链协议。此协议旨在使其能够用于(i)公有、(ii)私有或(iii)公有+私有区块链体系结构配置的任何组合。如下面的图 3 所示。

AERGO 的目标是成为真正意义上的企业区块链。一个在公共网络和私有网络之间架起桥梁的网络。一个使用核心区块链技术和部署蓝图的平台，Blocko⁷已经在世界各地的实际生产系统中证明了这一点。

AERGO 还致力于为每个业务实现提供和支持一个开发者友好的、功能丰富的、多范式的、一致的基于插件的智能合约基础设施。

“设计”、“部署”、“使用”和“管理”是 AERGO 项目的关键设计原则。让事情变得简单并不容易，对于目前的区块链尤其如此。

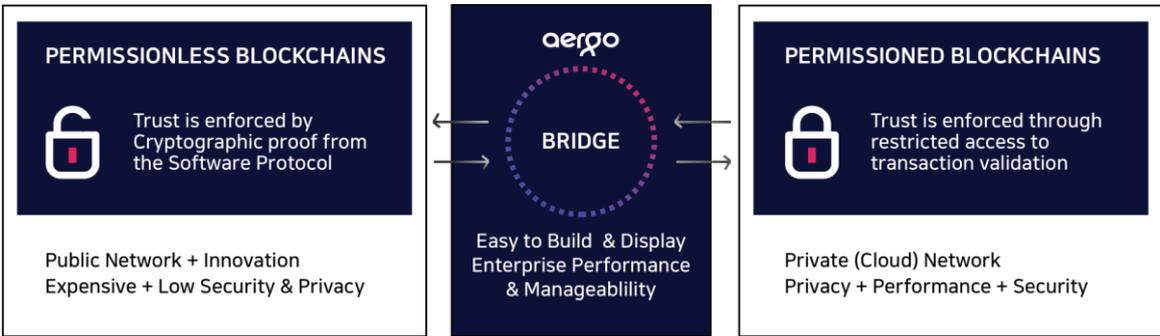


图 3. AERGO 为企业 IT 搭建了公链和私链世界之间的桥梁

AERGO 旨在将公链的实用性和创新性与私链提供的性能和安全性相结合。

正如云计算一样，我们希望开发这种技术，使企业能够在安全的公共基础设施上开发和运行他们的 dApp。当需要时，这些公司将能够轻松无缝地将这些应用程序的一部分(甚至全部)迁移到更高性能的私有区块链，且这些操作不会使它们失去此前部署公用区块链的任何好处。

为了实现这样一个全面的混合区块链体系结构，需要创新的技术和一个新的数据桥接框架(代理服务器)来使这些不同类型的系统协同工作。桥接代理将允许多个公链和私链网络之间的双向通信。

此外，对于开发、编译和嵌入智能合约至此类异构结构中的能力也有所要求。为未来和更全面的智能合约开发，这也需要一个非常高性能和高效的虚拟机引擎的支持。

下面的图解说明了这一原理。

⁷ Blocko 已经成功交付了 23 个生产中的区块链系统(为 20 家公司)，支持超过 2500 万用户。

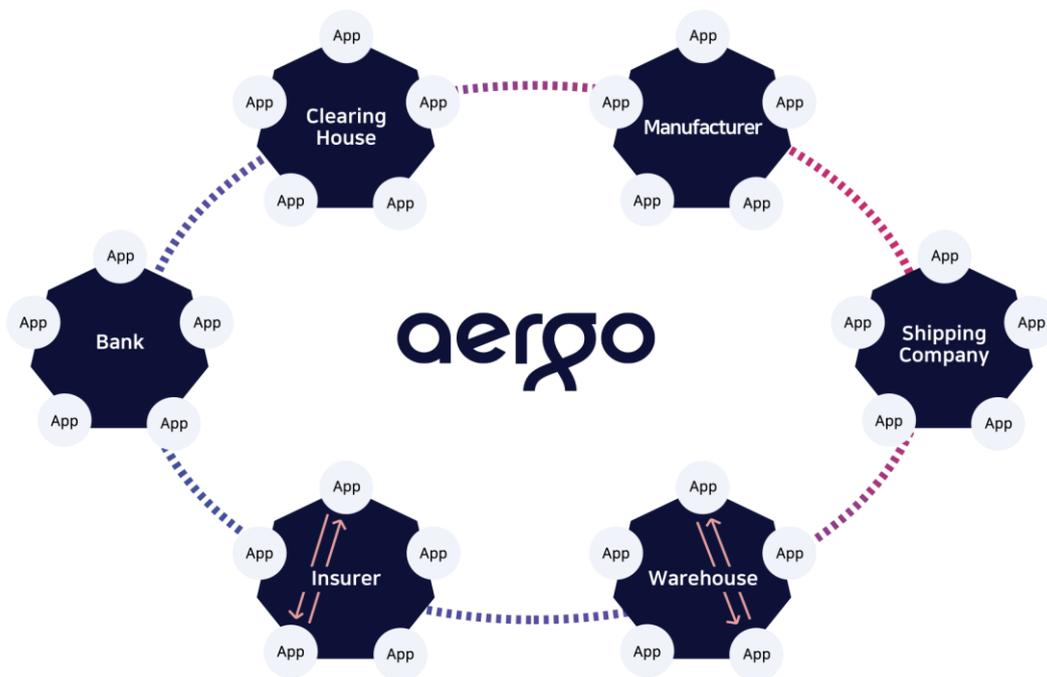


图 4. AERGO 生态系统网络展示了公链和私链之间的桥梁连接

AERGO : 总结架构

AERGO 计划利用 Blocko 现有的 COINSTACK 平台并在此基础上进一步发展。Blocko 的 COINSTACK 平台是一个得到充分支持的企业产品，现已被许多客户采用。

AERGO 的目标是提供一个用于在安全和高性能的云架构上开发、编排和部署 dApps 的完整框架。

Blocko 还将帮助培育一种技术和支持合作伙伴的“生态系统”。

AERGO 生态系统的主要利益相关者包括希望使用区块链的所有类型的企业及其开发者;以及提供增值服务的 IT 承包商、基础设施和服务提供商。

AERGO 还打算支持希望在 AERGO 技术栈中使用、开发、孵化和扩展核心功能和项目的开源开发者。AERGO 提议不仅会实现开源友好性，而且将实现完全开源。

这项计划的一个关键原则是吸引新的想法和项目来扩展 AERGO 生态系统的价值和效用。生态系统合作伙伴将包括支持团队和研究项目的特殊项目以实现这些创新。

AERGO 的核心元素如下图所示，这些元素一起构成了 AERGO 平台。



图 5. AERGO 核心元素

(I) AERGO CHAIN : *一个公有区块链网络*

AERGO 链是一种由节点提供商运营的企业区块链全球公共去中心化网络组成的新协议。

它打算包含 **AERGOSQL**，一个新的规范智能合约引擎，可以轻松创建高级智能合约，以支持创新的业务产品和服务。

总之，AERGO Chain 在概念上可以被认为是一个开源的区块链操作系统。

(II) AERGO HUB: *连接到 AERGO 链底层的公共接口*

AERGO Hub 旨在与 AERGO Chain 合作，并将安全的 dApps 连接起来。所创建的数据应用程序打算存储在以下两个存储库之一：

- **AERGO 公有存储库**是 dApps 的一个共享、开放和分散的底层基础设施(类似于 GIT 公有存储库，用于托管开源项目，或用于公共云计算的自动化构建服务器)。
- **AERGO 私有存储库**，是一种受控制的、安全的、私有的 dApps 基础设施。这旨在实现企业 IT 系统所需的访问控制、应用程序安全性和性能、数据遵从性以及服务质量 (“QoS”)⁸。

这两种类型的存储库都继承了业界测试过的实现框架和 COINSTACK 的 API 兼容性，并在全球客户端得到了验证。

⁸ Wikipedia, The Free Encyclopedia. (2018). *服务质量 (Quality of service)*. 链接: https://en.wikipedia.org/w/index.php?title=Quality_of_service&oldid=836944975

这些 dApps(以及其他为区块链优化过的支持软件、计算资源和服务)需要进行编排、供应、部署和管理，以便在 AERGO Chain 上使用。

意图通过 **AERGO HORDE** 实现的功能包括：为有意参与 AERGO Hub 生态的基础设施供应商服务的一个公共编排⁹、管理和软件框架。例如：区块链“节点供应商”或软件供应商。

总之，AERGO Hub 在概念上与当前公有云 web 服务中的技术非常相似。

(III) AERGO MARKETPLACE: 一个适配 AERGO Chain 的软件应用程序、计算资源和其他服务的一站式商店

- AERGO Marketplace 软件、计算和其他服务旨在作为支持 AERGO 平台的生态系统的一部分在 AERGO Chain 上运行或与之合作
- 这些合作伙伴服务通过 AERGO Hub 公共接口访问
- 这些服务将通过 AERGO Horde 进行管理

AERGO – 具体功能与性能

下一节将更详细地描述 AERGO 平台中上述(以及其他相关)关键技术实现。

虽然这对一些读者来说可能过于技术性，但我们希望通过至少概述这些核心功能，AERGO 的一些独特和创新能力得以被感知。

详情请参阅详细的 AERGO 技术白皮书 www.AERGO.io。

⁹ Wikipedia, The Free Encyclopedia. (2018). 编排 Orchestration (计算 computing). 链接: [https://en.wikipedia.org/w/index.php?title=Orchestration_\(computing\)&oldid=831362994](https://en.wikipedia.org/w/index.php?title=Orchestration_(computing)&oldid=831362994)

AERGO CHAIN

AERGO Chain 计划成为一个公链协议，旨在解决目前在公链上暴露出的问题。AERGO Chain 计划部署一个委托权益证明 (“DPOS”) ¹⁰ 治理模型。为了提高服务的可靠性和质量 (“QoS”)，提出了一种基于分数的自主委托算法。

AERGO 的目标是提供一个基于 SQL 的智能合约平台以提高区块链的可用性。这可能是解决区块链的许多主要和当前集成困难中最关键的组件之一。

我们认为，面向企业的区块链协议层需要包含如分布式版本控制和并发控制等高级特性。这些构成了用户如何创建公有的，特别是私有的 dApp 存储库的基础。这些新特性将有助于增强未来企业区块链的私密性。

智能合约的一种新的并行处理能力旨在让 AERGO Chain 每秒处理数百万笔交易。AERGO 旨在优化区块链网络的扩展，以满足区块链上运行的各种产品和服务的需求。我们相信，它也将能够参与和利用并行吞吐网络结构，以及支持多核和超高速缓存的内存计算机环境的多线架构。

AERGO Chain 正在开发的许多技术都基于 Blocko 的 COINSTACK 操作系统的核心功能，以及它们在为大型企业客户在现有计算机网络、安全及私有数据中心上构建生产中系统的经验教训。

共识算法

也许区块链最具决定性和最重要的特性之一是所选择的共识算法。共识算法是验证要添加到区块链中的区块信息是否是真实版本的关键程序。

如果没有一致的共识算法，任何参与者都可能向区块链添加信息，从而破坏整个系统的合法性。

虽然这些共识算法涉及复杂的数学和逻辑(可能超出了读者的范围)，但重要的是至少要了解正在为高性能 AERGO 平台开发的所选模型的基础知识。因此，在下一节中我们将提供最相关技术的简单描述。

¹⁰ Mycryptopedia. (2017). 解释委托权益证明 (DPoS). 链接: <https://www.mycryptopedia.com/delegated-proof-stake-dpos-explained/>

AERGO Chain 支持多样的共识算法，允许用户自定义或选择共识算法以最佳地满足他们的业务需求。然而，本文提出了一种基本的、默认的 AERGO 选择共识算法作为委托权益证明 (“DPOS”)。

我们相信这个算法类提供了增强的可扩展性和一个合算的操作模型。此外，AERGO DPOS 算法将旨在促进和支持企业和重要的区块链节点提供商参与到网络中。这将有助于整个网络的长期生存能力、效率和可持续性。

工作量证明

区块链社区(公共文章和其他参考资料来源)普遍认为，工作量证明(“POW”)是区块链最真实、最有用的共识算法。POW 的优点是简洁、易于理解，并且有可能成为最民主的共识方法。

然而，POW 有一些非常严重的缺点。

POW 可能会让电力和控制权最终掌握在少数几家大型矿工手中。我们还认为，网络的可预测性、稳定性和可持续性是企业的基本要求。它们是大型 IT 系统中操作 QoS 的主要影响因素。

为业务而设计的公有区块链将必须消除外部力量损害 QoS 和将控制权交给少数(或者可能是坏的)参与者的可能性。

质押证明

围绕质押证明(“POS”)出现了各种算法，包括 Ethereum 平台的潜在开发。有些工作还没有解决和落实。目前正在进行许多努力，以解决涉及 POS 的一些最重要的技术问题(例如无物质押)。

然而，我们认为 POS 本身不太可能成为主流的共识方法，除非它解决了某些挑战，如发生所谓的分叉 (“coin slashing”)。例如，如果一个错误(或 bug)破坏了 POS 规则，它将导致所谓的 coin slashing，从而创建一个非常不受欢迎的区块链硬分叉。

公链的硬分叉直接影响网络的可靠性。它们还会显著增加运行在公共网络上或与公共网络管相关业务的运营安全风险。本报告第 13 页的图 1 显示了比特币之前发生的分叉。

委托权益证明

委托权益证明(“DPOS”)是一种很有前途的替代共识算法。DPOS 是一种先进的网络(能源)高效模型，已被许多著名的区块链项目(如 EOS、Steem 和 BitShares)使用。

它促进了去中心化(因为它不需要大型的、专业的-通常是集中-的矿池)。DPOS 还为网络中的

通证持有者提供了好处以帮助确保将恶意参与者从网络中移除。这种结合了社会性和技术性的民主化形式认可有价值的参与者并支持网络中的善意行为。

实际上，这是一种自我监控和正向促进的模式。

我们相信 DPOS 既容易理解又降低了硬分叉的可能性。我们还认为，在一个参与者是企业 and 基础设施提供商的网络中充当节点会进一步降低硬分叉的可能性。

对商业流程 QoS 的重要需求也将大大增强。

总之，POW 只提供纯粹的经济激励。相比之下，被选为 AERGO 共识机制的 DPOS 寻求将经济激励与社会共识相结合。

智能合约

AERGO Chain 旨在支持经过测试且易于使用的多范式智能合约基础设施。它包括以太虚拟机。这种混合方法为不同类型的智能合约操作提供了可交互性。

AERGOSQL

AERGOSQL 是一个术语，用于描述在 AERGO 链上和链内运行的智能合约。

AERGOSQL 试图提供用于存储和访问数据的相关数据模型，以及用于编写智能合约的类似 SQL 的脚本语言。

我们坚信这种基于传统的、易于理解的且易于使用的 SQL 技术的新方法将使广大开发者和商业用户能够从区块链中受益。

下面的摘要显示了一个简单的示例，展示了生成的编码模型。

```

CREATE IF NOT EXISTS accounts (
  owner VARCHAR NOT NULL PRIMARY KEY,
  balance NUMERIC (15, 2)
);

CREATE OR REPLACE FUNCTION
transfer (sender TEXT, to TEXT, amount NUMERIC)
RETURNS text
AS
$$
DECLARE
  sender_bal NUMERIC ;
BEGIN
  SELECT balance INTO sender_bal FROM accounts WHERE owner = sender ;
  IF NOT FOUND THEN
    RETURN 'Sender not found' ;
  END IF
  IF sender_bal < amount THEN
    RETURN 'Not enough balance' ;
  END IF
  UPDATE accounts SET balance = balance + amount WHERE owner = to ;
  IF NOT FOUND THEN
    RETURN 'Receiver not found' ;
  END IF;
  UPDATE accounts SET balance = balance - amount WHERE owner = sender ;
  RETURN 'OK' ;
END;
$$

```

图 6. AERGOSQL 编码模型案例

为了实现最佳性能，AERGOSQL 意图采用先进的创新技术，比如 LLVM 编译基础设施(提供智能 JIT 编译¹¹)和高性能 b-tree 数据结构部署(比如用于数据存储的开源 WiredTiger¹²)。

智能合约执行是 AERGO 内部的一个效用程序(在 AERGO Chain 上被标记为原生数字资产)。智能合约执行(包括此任务所需的计算能力)将使用 AERGO 作为运行成本。

分支和合并

¹¹ Wikipedia, The Free Encyclopedia. (2018). *LLVM*. 链接: <https://en.wikipedia.org/w/index.php?title=LLVM&oldid=841209654>

¹² Michael Cahill. (2015). *WiredTiger 的技术介绍*. 链接: <https://www.mongodb.com/presentations/a-technical-introduction-to-wiredtiger>

合并分支的过程是分布式版本控制系统中最复杂的概念之一。对于区块链(必须处理实时数据), 合并的实现难度更大。

由于其非破坏性的过程, 我们相信 AERGO 的分支将是一个简单和直接的过程。然而, 合并需要两种不同的方法:

(I) 自动合并

- 默认情况下, 自动合并是合并两个分支的预期过程。自动合并类似于块链中的块重组过程。在这种情况下, 合并源的块被合并到到交易中, 并被合并目标的合并池吸收。最终, 合并池将导致一个新的块附加到合并目标的最佳块上。在此过程中, 与合并目标分支不一致的交易将自动从新块中排除。

(II) 一致合并

- 一致合并只有在使用指定的一致合并逻辑创建分支时才会发生。一致的合并类似于版本控制系统(如 Git)¹³提供的合并功能。与自动合并(默认情况下舍弃不一致的交易)不同, 一致合并依赖于预定义的冲突解决逻辑来管理不一致的交易。冲突解决逻辑被实现为一个系统级的智能合约。

我们相信 AERGO Chain 将为习惯使用 Git 等版本控制系统的用户提供友好的语法和语义。可以通过 AERGO CLI 客户机以及 RPC(远程过程调用)API 访问这些功能。

AERGO Chain 的目标是实现开发者友好性, 它需求允许开发者使用熟悉和理解的技术、工具和方法。

并发控制

并发控制是区块链网络的关键功能。当在区块链网络中调度重要的块创建交易时, 它确保 DPOS 协商一致算法是确定的(即完全可预测的)。

AERGO Chain 的目标是为交易序列化提供两种机制。这些是(i) 区块级序列化和(ii) 矿池级序列化。

(I) 区块级序列化

¹³ Wikipedia, The Free Encyclopedia. (2018). *Git*. 链接: <https://en.wikipedia.org/w/index.php?title=Git&oldid=841769346>

- 由于区块链的每个分支都由一系列的块组成，所以可以通过一个块接着一个块的堆叠来序列化事务。
- AERGO 计划提供基于块高度的多版本并发控制(MVCC)。一旦指定了分支和块的高度，就可以跨存储库中的不同节点提供一致的读取。
- AERGO 的 MVCC 功能旨在两种解决方案：用于连续读取的快照隔离和通过行或文档版本控制的锁定。MVCC 只适用于块级序列化。

(II) 矿池级序列化

- 访问 AERGO 节点的人可以利用委托计划创建区块的确定性。这是核心 DPOS 共识所提供的特性。它允许执行同步转账，为交易的最终性提供了强有力的保证。
- 由于 AERGO 网络中的每个委托节点都可以应用统一的序列化顺序将新的事务处理到内存池中，并创建新的块，客户端无需等待块间隔的完成来检索交易的结果。因此，执行交易的延迟从几秒减少到几毫秒。

矿池级序列化如下图所示。

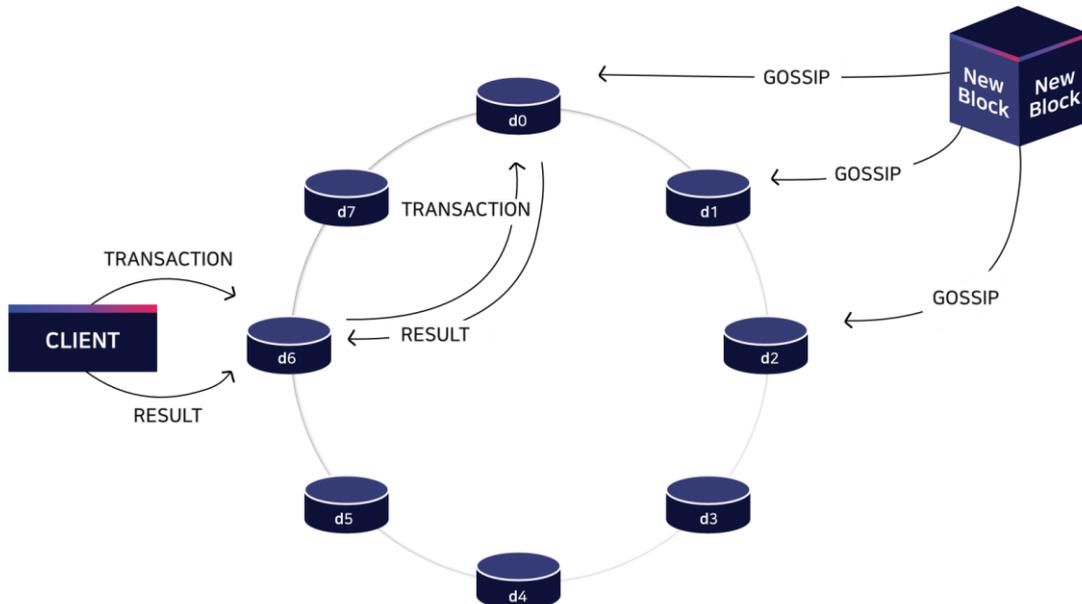


图 7. AERGO 链中的池级序列化

并行性

AERGO 的性能最大化计划通过旨在通过合并区块和区块级别的并行过程实现。

区块链系统的性能主要取决于:

- (i) 创造和共享新区块的效率;
- (ii) 每个节点处理新区块所需的时间。

整个分布式协商共识协议都参与到区块链的块创建过程中。虽然已经研究了分布式共识协议(并在各种区块链项目中受到关注),但我们认为,现有系统中每个节点的实际块创建过程往往设计和实现得很糟糕。

性能不佳的节点在公有区块链实现中有时是可以接受的(如在比特币和以太坊中)。然而,像 AERGO 这样的企业级区块链需要更高的性能。理想情况下,这应该是接近实时的。因此,需要谨慎地实现每个节点,就像使用协商共识协议本身一样有效。

AERGO Chain 意图将并行度的概念引入到块处理的各个阶段,以实现系统性能的最大化。

区块链系统中的并行性包括细致分析和理解每个块中包含的交易之间的从属关系。它还需要一个高效的体系结构,比如那些受到阶段式事件驱动架构 (Staged Event-Driven Architecture “SEDA”)¹⁴启发的体系结构。

下图描述了这种(重要的)并行性形式。

¹⁴ Wikipedia, The Free Encyclopedia. (2018). *阶段式事件驱动架构 Staged event-driven architecture*. 链接: https://en.wikipedia.org/w/index.php?title=Staged_event-driven_architecture&oldid=812633632

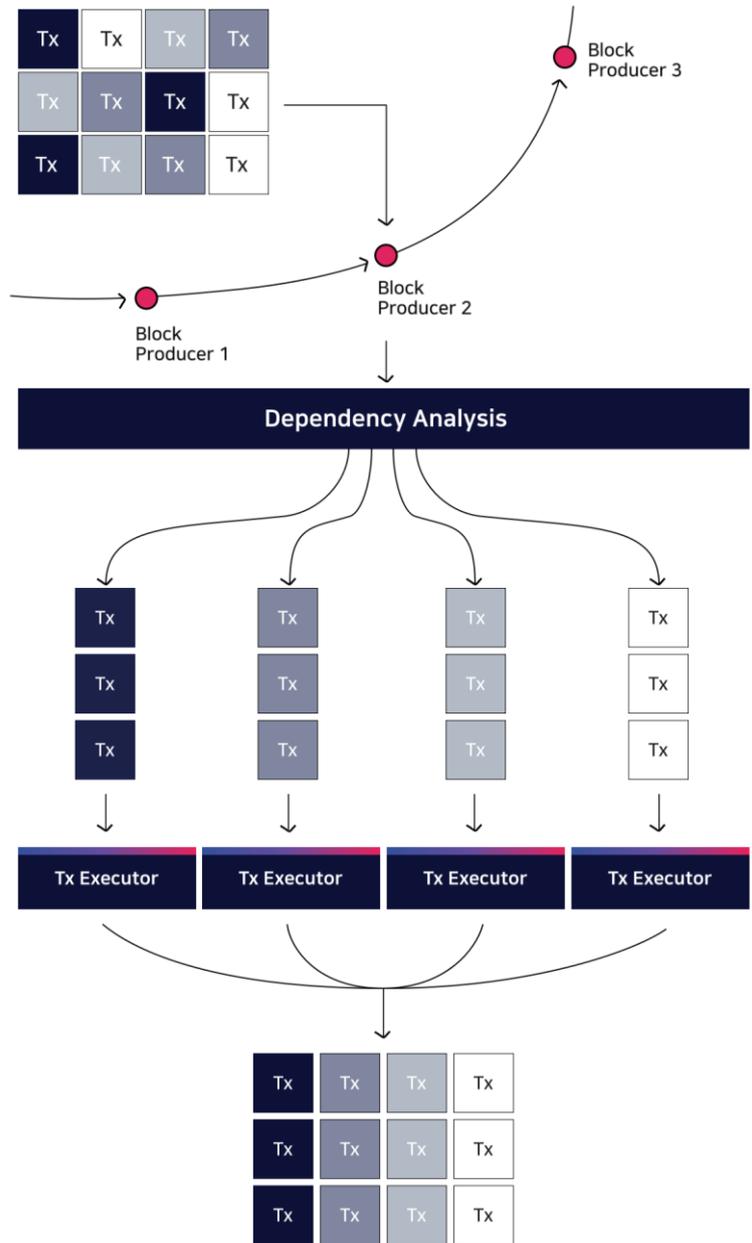


图 8. AERGO 并行

从属关系分析

从属关系分析是实现 AERGO 并行处理能力的关键因素。

AERGO 旨在执行交易和区块之间的从属关系分析，以创建执行顺序的数据结构。它的度量结果的不确定性受交易影响的状态机。数据结构格式称为确定性转账树(“DTT”)。有关 DTT 的进一步信息可以在 AERGO 技术白皮书中找到。

AERGO 文件系统

AERGO 独有的文件系统(“**AERGOFS**”)旨在进一步增强 AERGO 的可扩展性，特别是在前面提到的 IT 系统的纵向和横向扩展。

AERGOFS 计划像现代分布式文件系统一样运行。它的目标是为 AERGO 链提供结构化和非结构化的数据存储能力。与 Hadoop 分布式文件系统(“**HDFS**”) ¹⁵的块数据存储不同，AERGOFS 旨在为大量文件提供服务。

AERGOFS 基于 Facebook 的 Haystack¹⁶技术。

我们的设计目标是，AERGO Chain 将通过提供易于使用的 GIT 类私有存储库，支持并使其开发者和用户有足够的权限访问底层账本数据。

这是为开发者提供的一个重要功能。

基于域的分区

基于域的分区是确保 AERGO 可扩展性的最基本策略。域分区是通过 AERGO 的分布式版本控制功能来实现的。

与传统的区块链实现不同，AERGO 提议能够通过分支自由地分叉和合并数据。这被称为分布式版本控制(**DVC**)。因此，分布式账本可以通过不同的存储库在逻辑和物理上进行分区。

这种方法已经被其他已建立的分布式版本控件(如 Git 或 Mercurial)成功地使用。例如，广泛部署的 Github 系统能够承载数千万个存储库。

然而，基于域的分区的有效性主要取决于数据的结构和使用。当一个存储库需要处理无限制的数据扩展时，通过分支对数据进行分区是非常困难的。

因此，AERGO 的目标是通过使用 AERGO 文件系统(AERGOFS)和 AERGO Hub 来利用额外的可扩展性方法和功能。

分布式名录

¹⁵ IBM. (2018). *Apache Hadoop 分布式文件系统*. 链接: <https://www.ibm.com/analytics/hadoop/hdfs>.

¹⁶ Peter Vajgel. (2009). *大海捞针：有效存储数十亿张照片*. 链接: <https://code.facebook.com/posts/685565858139515/needle-in-a-haystack-efficient-storage-of-billions-of-photos/>

分布式名录(“DD”)是一个核心功能，计划作为 AERGO 实现中的构建块使用。

存储库中的每个 DD 都管理一个独立且隔离的名称空间。每个名称空间依次包含关于存储库中驻留的不同分支和标记的信息，以及区块链上各种标识符的有效性。

每个 DD 都是一个单独的区块链，具有自己的创世区块和最佳区块。与传统区块不同，DD 块的大小受到限制，它们之间的创建间隔相对较长。此外，由于 DDs 用于管理元数据，所以它们需要紧凑。

就其方面和功能而言，DD 可以与数据库中的数据字典、Hadoop 的 zookeeper 或 CoreOS¹⁷ 的 etcd 相媲美。

综上所述，**AERGO Chain** 的目标是成为一个强大的 **区块链公共互联网**。

¹⁷ Lawrence Hecht. (2018). *CoreOS, Red Hat and Kubernetes Competition*. Available: <https://thenewstack.io/coreos-red-hat-kubernetes-competition/>

AERGO 存储库 - 公有 & 私有

AERGO Chain 旨在支持创建“开箱即用”的公有和私有存储库。

存储库是开发者代码托管平台的一种形式。它们包含为项目开发的实际软件程序代码。它们还用于版本控制和协作。存储库允许开发者和其他人在任何地方合作开发新项目。实际上，随着时间的推移，存储库管理一个项目或一组文件。

存储库实际上是 AERGO 链上区块链的最小形式。存储库可以是私有链或公链，独立于 AERGO 链运行。

AERGO 中的公有存储库和私有存储库都可以免费使用，对存储库的访问由创建者建立和控制。通常，公有存储库对公共网络中标识的任何人都是开放的。私有存储库只允许进入特定私有网络的开发者和用户访问。

下图描述了这一点。

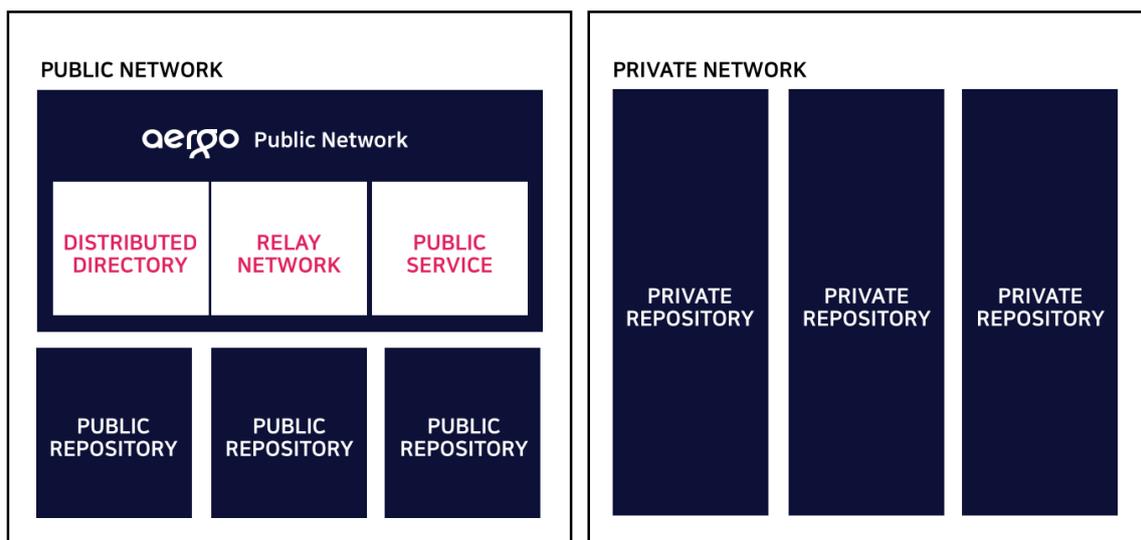


图 9. AERGO 公有与私有存储库

AERGO 公有存储库

AERGO 公有存储库的目标是成为 dApps 的共享、开放和去中心化的底层基础设施(很像 Git 中的公有存储库，用于托管开源项目，以及用于公共云计算的自动化构建服务器)。

它对读写是开放的，或者它甚至可以选择性地授予匿名用户权限。一个常见的配置是创建一个 AERGO 公有存储库作为只读匿名访问。

AERGO 私有存储库

AERGO 私有存储库的目标是成为一个受控制的、安全的、私有的 dApps 基础设施。这确保了完全的访问控制、应用程序安全性和性能、数据遵从性，以及 QoS，所有这些都是企业 IT 系统所必需的。

AERGO 私有存储库保证了对存储库中读写的完全访问控制(只有具有正确权限的用户才能在这些存储库中工作)。通过从远程父分支创建新分支，用户可以将新创建的块保存在与公有隔离的私有分支中。只有当将权限授予包含分支的特定存储库时，用户才能访问各自存储库中的块。

AERGO 还支持重要的类 GIT 的数据模型和命令结构;这允许自由分支或合并块等功能。

在每个存储库中，建议不同的分支可以指向区块链中内容的不同快照，以便创建特定的状态。还可以创建新的分支。

最后，AERGO 中的“最佳链”概念类似于主分支。

两种类型的存储库(公有和私有)都继承了经过行业测试的实现框架和 COINSTACK (Blocko 完全支持的企业产品和经过行业测试的 API 框架)的 API 兼容性。

下面描述了 AERGO 中的分支和合并。

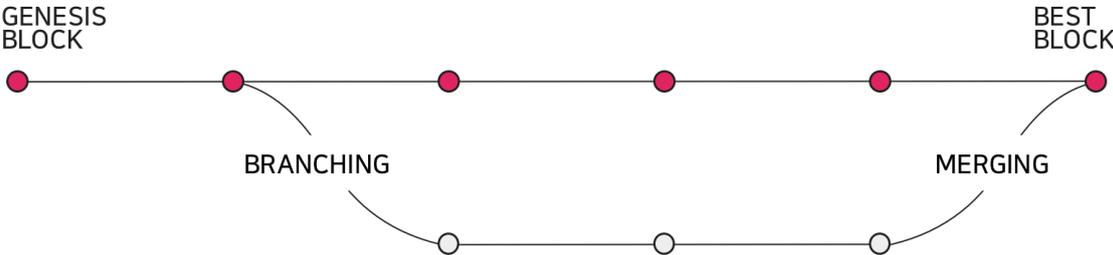


图 10. 分支和合并

为了创建和连接到 AERGO 公有存储库和私有存储库，用户可以利用 AERGO Hub 中的特性和服务。

AERGO HUB

AERGO HUB 被提议成为一个公共接口，企业公司和 dApp 开发者可以通过它访问计算能力来运行他们的业务或应用程序。

AERGO Hub 计划与 AERGO 链中的 dApps 进行连接和合作。dApps 是在前面描述的两个存储库中创建和存储的。AERGO HUB 的目标是在本质上类似于当前经过验证的公共云服务(如 Amazon AWS)。

它们提供了许多高级功能(如下面的图 11 所示)，例如:

- 1) 软件微服务支持;
- 2) 内容分发网络(“CDN”)¹⁸;
- 3) 无服务器数据库;
- 4) 智能语言机接口(将区块链与单独的数据源连接，如单独的数据库);
- 5) 智能网关，智能路由数据流量/消息到区块链



图 11. AERGO Hub Functional Illustration

综上所述，**AERGO Hub** 是进入 AERGO 链的公共接口。

¹⁸ Wikipedia, The Free Encyclopedia. (2018). 内容分发网络. 链接:
https://en.wikipedia.org/w/index.php?title=Content_delivery_network&oldid=841886968

AERGO Horde

AERGO dApps(以及所有其他为区块链优化的支持软件、计算资源和服务)需要经过编译、补充、部署和管理才能使用。

我们意图通过 **AERGO Horde** 来实现这一点。这是一个为基础设施和其他想参与 AERGO Hub 生态系统的第三方供应商（如区块链节点提供者或软件供应商）提供的公共编译管理和软件框架。

这些供应商将需要安装 AERGO Horde，以便作为一个节点(实际上，这允许他们“连接”他们的服务到 AERGO 生态系统)。AERGO Horde 将是一个开源的公共域软件项目。

AERGO Horde 为可管理性和效率提供了自己的专业操作系统 **AERGO OS**。

这提供了与嵌入式高性能 Linux Kernel 和相关服务交互和工作的特定接口和组件(如下图所示)。

— AERGO OS

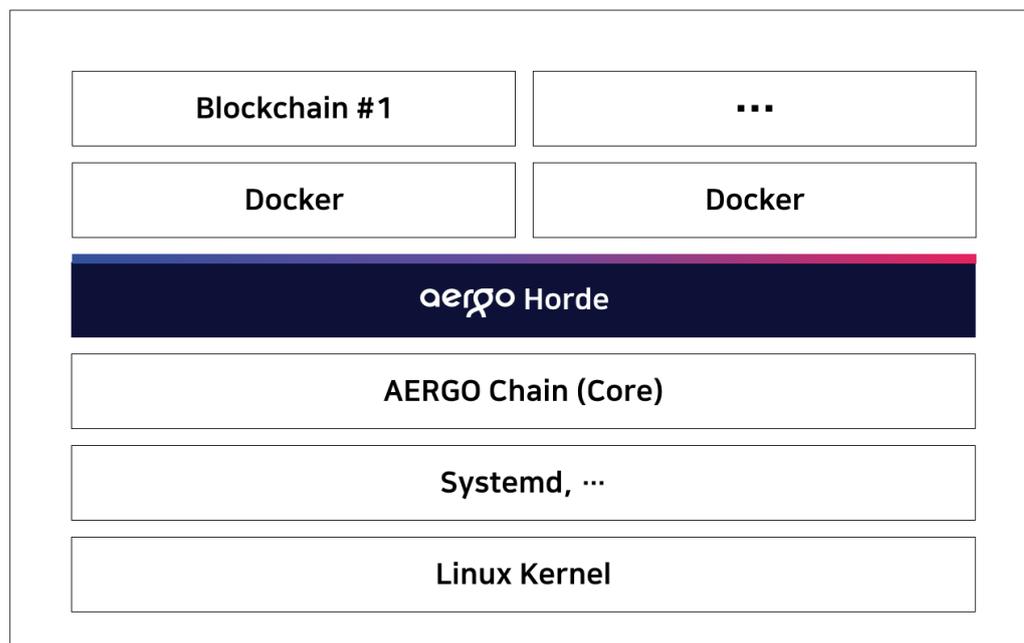


图 12. AERGO OS 构架

使用 AERGO OS，我们相信节点提供者将能够执行许多非常有趣的系统级任务，例如检查节点信息、监视资源可用性和生成的块信息。

AERGO MARKETPLACE

AERGO Marketplace 计划成为一个一站式商店，提供为 AERGO Chain 优化的软件应用程序、计算资源和其他服务。

AERGO Marketplace 软件、计算和其他服务旨在兼容并运行于 AERGO Chain 或与之合作。

建议通过 AERGO Horde 公共接口访问 AERGO Marketplace，并通过 AERGO Hub 进行管理。

下图描述了这个流程。

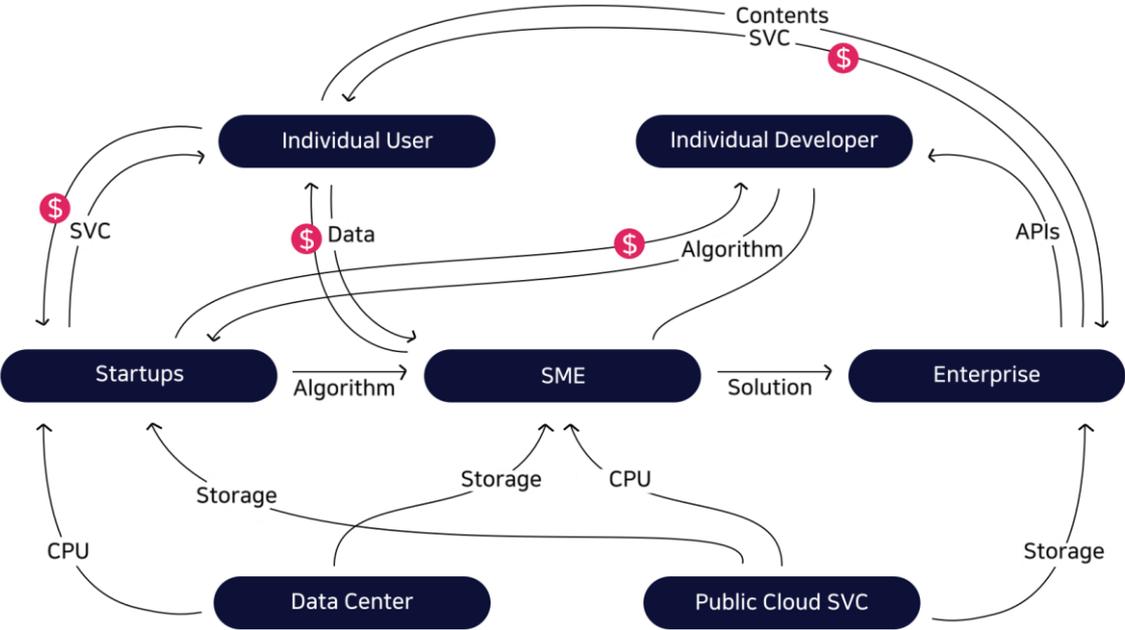


图 13. AERGO Marketplace 演示图

我们建议启用第三方，如服务供应商、独立软件供应商和云基础设施供应商，这样他们就可以向 AERGO 的用户提供他们的产品和服务。

AERGO 的最终用户将是软件开发者，以及希望构建、管理和运行区块链项目的所有类型和规模的企业。

虽然本质上类似于传统的云市场，但我们的目标是确保 AERGO 市场显著降低其用户的进入壁垒。这包括个人软件开发者、IT 承包商和公司(从小型中小型企业到大型跨国企业)。

我们还计划为希望使用 AERGO 解决具体问题的国家和地区政府机构提供支持。这方面的一个例子是提供一个基于区块链的安全匿名公民投票系统(就像 Blocko 与 COINSTACK 已经为韩国

的一个地方政府省份实现的那样)。

AERGO 市场将作为一个商业和合作伙伴生态系统运行。我们计划提供广泛的数字功能，可用于开发和部署创新的区块链解决方案。

随着时间的推移，AERGO 市场将提供的数字功能的例子包括，可能包括：

- 计算能力(CPU)
- 存储(可扩展-超快)，固态内存
- 内容分发网络(CDN)
- 机器学习算法
- 数字内容(新算法和新软件微服务)
- 专业数据库
- Smart Contract 和 Smart Oracle(模板)
- 区块链 IT 集成蓝图
- 数字身份蓝图
- 文件时间戳(DTS 图纸)
- AERGO 区块链培训

AERGO 平台将考虑涵盖其他模块，并欢迎有兴趣参与和合作 AERGO 生态系统的各方提出新想法。

总之，我们的目标是使 AERGO 市场成为一个充满活力、开放和可持续的生态系统。一个充满新技术和创新的市場;无论是由单个开发者还是大型软件供应商提供的。

这些服务将得到推广，并有望用于在安全区块链上运行的下一代业务。底层 IT 架构还将基于低成本的分分布式实用程序计算部署模型。

AERGO 代币 [原生区块链资产和通证模型]

AERGO 代币 (“AERGO Token”) 是一种在 AERGO 平台上运行的效用型通证，其目标是服务于多种不同的功能。一般来说，AERGO 通证旨在成为 AERGO 生态系统内的交换媒介。这些通证旨在授予持有人在 AERGO 生态系统中某些可用服务的权利。

更具体地说，这些通证的用途是：

- 运行 smart contract (AERGOSQL);
- DPOS 共识算法
- BLOCKO Coystack 4.0 技术支持的支付方式;
- AERGO Hub 服务的支付方式;
- AERGO 市场上服务和资产的支付方式;和
- AERGO 域的支付方式

AERGO 通证也可以在平台内转让。

AERGO 主网将于 2019 年初上线(目前的目标发布日期是 2019 年第一季度)。

最初，持有 AERGO Token 可用于访问和购买 COINSTACK V4.0 (Blocko 最新的经过验证的企业区块链平台发行版)上的产品和服务。

下面的示例描述了 AERGO 通证的循环和使用。

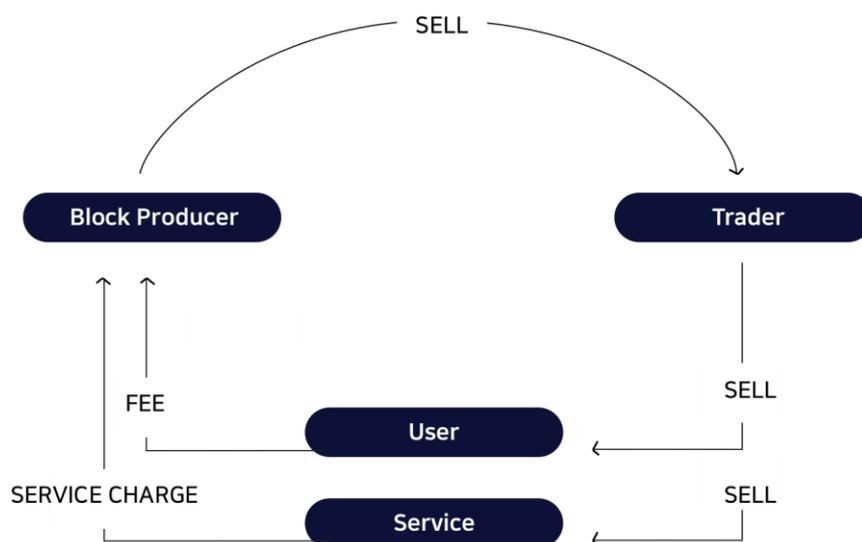


图 14. AERGO 原生资产流通

通证分发和资金使用

总供应

总共将发行 5 亿枚 AERGO 通证。

通证的分配和使用将按照下表进行，但可能会有所更改。

通证销售比例	30%
AERGO 社区奖励和战略合作伙伴	30%
通证发行者保留	25%
顾问及主要支持者	10%
通证发行机构和附属机构的雇员	5%

所得款项用途

出售代币的收益将用于开发和推进 AERGO 的技术项目以及合作伙伴的生态系统开发方面。

下表列出拟议收益的细目，但可能有所更改。

研发	40%
生态系统孵化	30%
市场营销	15%
战略联盟和业务发展	10%
杂项	5%

发展路线图

提出了 AERGO Chain 的路线图和发布时间表；下图描述了 AERGO HUB 和 AERGO Marketplace 的构建。

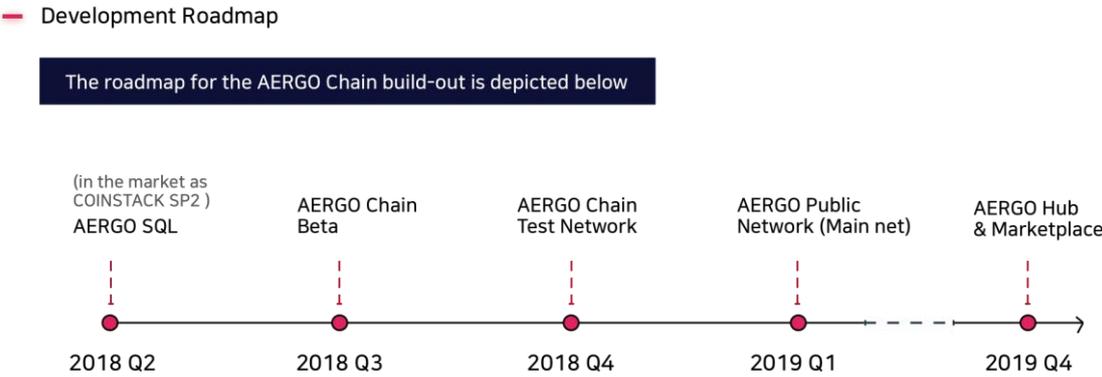


图 15. AERGO 发展路线图

这个路线图可能会改变。

它还可能受到已经对使用 AERGO 表示兴趣的特定的早期测试人员和早期采用者企业客户的影响。这可能导致某些功能比上述计划建议的更早(或更晚)发布。

执行计划

我们认识到 AERGO 项目有非常宏伟的长期目标。AERGO 平台的关键组件将会频繁发布。重要的组件已经在进行高级开发。

作为 AERGO 整体计划的一部分且为了启动项目，我们打算使用和利用 Blocko 的以下组件。

Blocko COINSTACK 和 Blocko 专有技术的贡献

Blocko 公司计划为 AERGO 平台贡献一些现有的产品、服务和技术。它还将利用一些对 AERGO 未来功能感兴趣的现有客户。

这些贡献（以 Blocko 为基础的）预期将包括：

- Coystack 作为 AERGO 协议的一个关键的初始基本元素

我们的意图是，AERGO 协议将继承它的一些关键功能和经过验证的功能（比如 API，它的目的是向后兼容）。

- 已验证的企业部署模型

如果能让未来的企业客户测试和采用 AERGO，那么能够提供安全且符合数据隐私的部署框架（例如，经过验证和测试的用应用案例）是非常重要的。

Blocko 将与 AERGO 及其用户共享这些经过生产测试的部署框架。

- Blocko 现有的（和未来的）企业客户

Blocko 迄今已为 20 多个付费客户提供安全保障，并基于其 COINSTACK 版本的区块链实现了更多的生产系统。

Blocko 建议与其现有客户接洽，将 AERGO 作为对其现有部署的增强。这对于那些最初由于缺乏运营控制和隐私问题而放弃连接公共区块链的公司来说尤其有用。

- Blocko 市场和直接支持基于 AERGO 的实施

Blocko 建议将 AERGO 作为首选开放协议呈现并积极推荐，AERGO 可以为客户配置并连接到自己的 COINSTACK 解决方案，AERGO 还将直接支持企业部署基于 AERGO 的产品和服务。

- Blocko 作为 AERGO 的战略技术合作伙伴

Blocko 公司打算为 AERGO 提供技术开发和直接技术支持。

AERGO 还将受益于 Blocko 的领先优势和已投产的工业研发、IT 集成和支持能力(目前总部位于韩国、香港和伦敦)。Blocko 集团继续在全球扩张,并打算在世界上许多其他国家和地区开展业务。

➤ Blocko 现有的基础设施和区块链合作伙伴

Blocko 将帮助创建 AERGO 生态系统。它的一些技术合作伙伴已经表达了参与并帮助启动 AERGO 生态系统的愿望。这些合作伙伴包括:一家专业的 SQL 开发公司、一家云基础设施提供商和一家大型国际电信公司。

➤ 其他支持第三方生态系统活动

新技术创新、精心策划的增值合作伙伴、支持开源和软件开发者都是 AERGO 生态系统的关键元素。发现并与这些 AERGO 持币者(以及他们的扩展)合作是项目的基本部分。

这还将涉及在关键工业和政府部门发展战略、技术和 IT 服务关系。

很大一部分资金将用于促进和发展上述 AERGO 的持币者生态系统。

为了支持和指导这些努力,该项目还获得了一个经验丰富的咨询小组的服务。

这个小组包含了一些在以下领域处于世界领先位置的专家:区块链、分布式数据库、效用计算、数字通信、云计算、大数据、机器学习/人工智能、虚拟化、开源技术、开源许可、计算机编程、安全、开源商业发展、金融和投资银行、政府关系和战略合作伙伴的业务发展。

AERGO 团队可以在附录-D 中看到。

附录

附录-A：区块链和开放平台入门

比特币是迄今为止最著名的数字货币。它已经获得了公众和政府监管机构的高度关注。这是由于它经常用于匿名(有时是非法的)交易和它的价值波动。

比特币和市场上出现的许多其他山寨币(“altcoin”)本身并不是本文的重点,而是这些通证运行和存在的新技术架构。这项技术就是区块链技术。

在非常简单的层次上,区块链只是一个分布式(在多台计算机上运行)且安全的数据库。与 Linux 或 Hadoop 一样,公链也是开源的;也就是说,这项技术不是由任何一家软件公司拥有的,而是由世界各地的开发者在一个开放和透明的过程中开发的。

区块链是一种巧妙的技术,它使用复杂的密码技术和智能(所谓的共识算法),以确保在其账本系统中批准和接受交易的自主方法。共识算法还影响事务和数据如何共享,以及如何被推送到区块链网络中的计算机上。区块链技术提供了防篡改版本,因此记录在其系统中的事务是可信的。这种信任适用于双方之间很少(或实际上没有)信任的一方。

具有革命性的是,区块链作为一个中介,在很大程度上是一个免人为操作系统。尽管数据库技术已经使用了 50 多年,但以前从未有人这样做过。

支持区块链的系统旨在允许创建一个单一的、通用的、可信的、完全不可篡改的数字资产和相关交易注册。区块链可用于提供基本服务,这些服务对于任何需要交易数字资产(甚至只是数据)的系统都是必不可少的。它可以用比现在使用的工具更好、更有效的方式实现这一点。首先,区块链技术为加密交易创建了一个可行的、去中心化的记录,即分布式账本,它允许用传统的(可能不太安全的)主数据库被替换为大量的分布式数据库。我们相信,这有可能使许多数字系统的大部分得到彻底简化和降低成本,同时使它们更加安全和可靠。

区块链技术还允许创建数字资产或通证,这可以提供一种直接和明确的价值转移机制,同时保持数字网络的优势。

我们也相信区块链技术提供了比我们现在使用的更好的方法来建立和使用身份。身份可以以密文方式存储,区块链网络中的个人可以在保护隐私的同时同时验证自己的身份。

通过提供独特的、不可伪造的身份,以及不可侵犯的所有权记录,区块链可能大大简化实物资产

的直接转让过程，并增强了资产来源的可靠性。

区块链的编程能力是通过所谓的“智能合约”实现的。智能合约是事件驱动的计算机程序，具有控制底层价值单位的能力。简而言之，它们是旨在自动执行和解决任务的程序。它们是允许 dApp 从区块链系统释放大部分值的应用层(参见下面的图-16)。

智能合约使企业能够将金融交易或其他数字协议的价值合并到一种加密保证的业务逻辑形式中，使其能够自主执行和转移价值。简而言之，业务任务被编译并安全地嵌入到区块链本身中——用于自动执行、自动检查、自动执行和自动记录。

因此，智能合约被编写并直接编译到区块链中，即它们实际上嵌入到区块链本身中，以便在调用时自动执行。

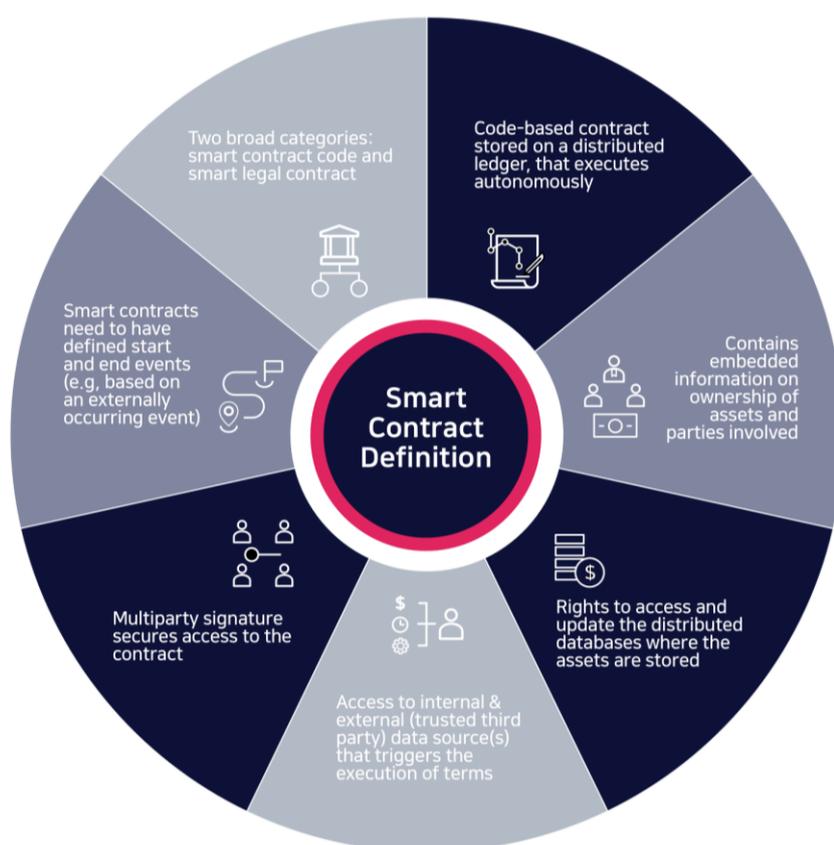


图 16. 智能合约¹⁹

区块链不能访问网络之外的数据。因此，智能合约的一个重要补充能力被称为预言机 (Oracle)。

预言机(在区块链上下文中)是外部代理或程序，它们查找和验证真实世界发生的事件，并将此信息

¹⁹ Everest Group. (2016). 智能合约：实现区块链的好处。 链接: <https://www.everestgrp.com/2016-10-smart-contracts-realizing-benefits-blockchain-36282.html/>

提交给区块链供智能合约使用。它们提供外部数据并“触发”智能合约。实际上，智能预言机是第三方的“数据输入”，它们以安全和可信的方式提供这些信息。

智能预言机实际上可以是软件预言、硬件预言、共识预言以及入站和出站预言。由于这些是第三方服务，因此需要额外的关注(和技术)才能使这些服务得到信任。

为企业提供可信和安全的信息(当企业在基于区块链的系统中使用智能合约时)对系统用户非常重要。错误会带来严重的后果。智能合约是自动执行的，在区块链中没有所谓的回滚(由于其核心的不可变性特性)。

综上所述，智能预言可以看作是真实文字数据与智能合约之间的“接口”。图 17 描述了整个区块链信息技术(“IT”)堆栈。

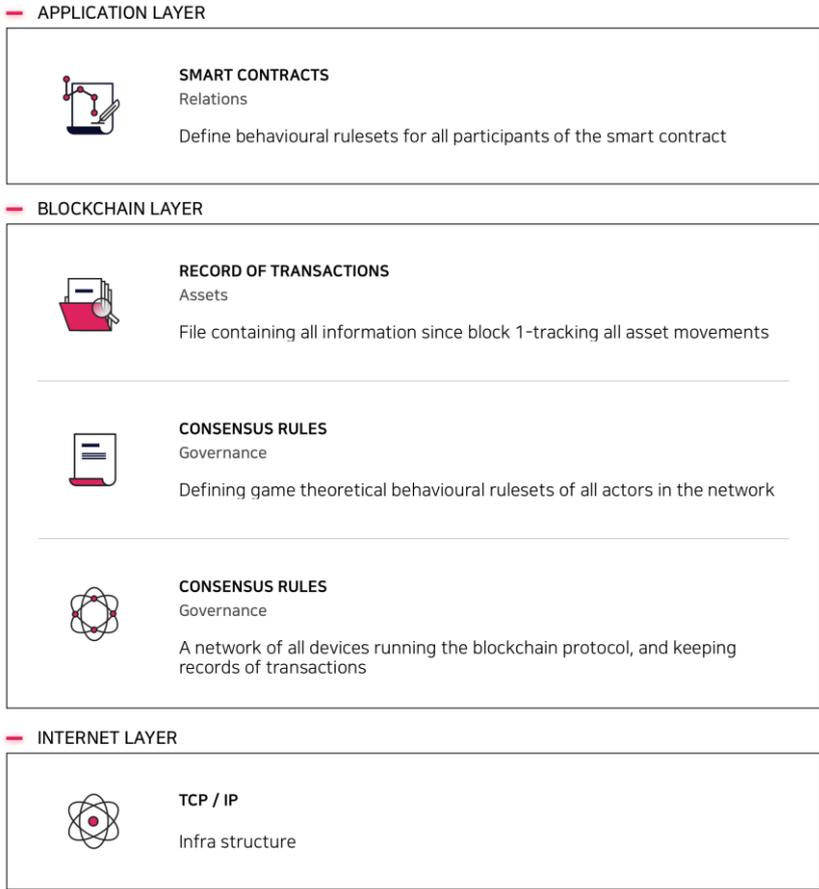


图 17. Blockchain IT 堆栈

图 18 中描述了区块链的重要业务功能。

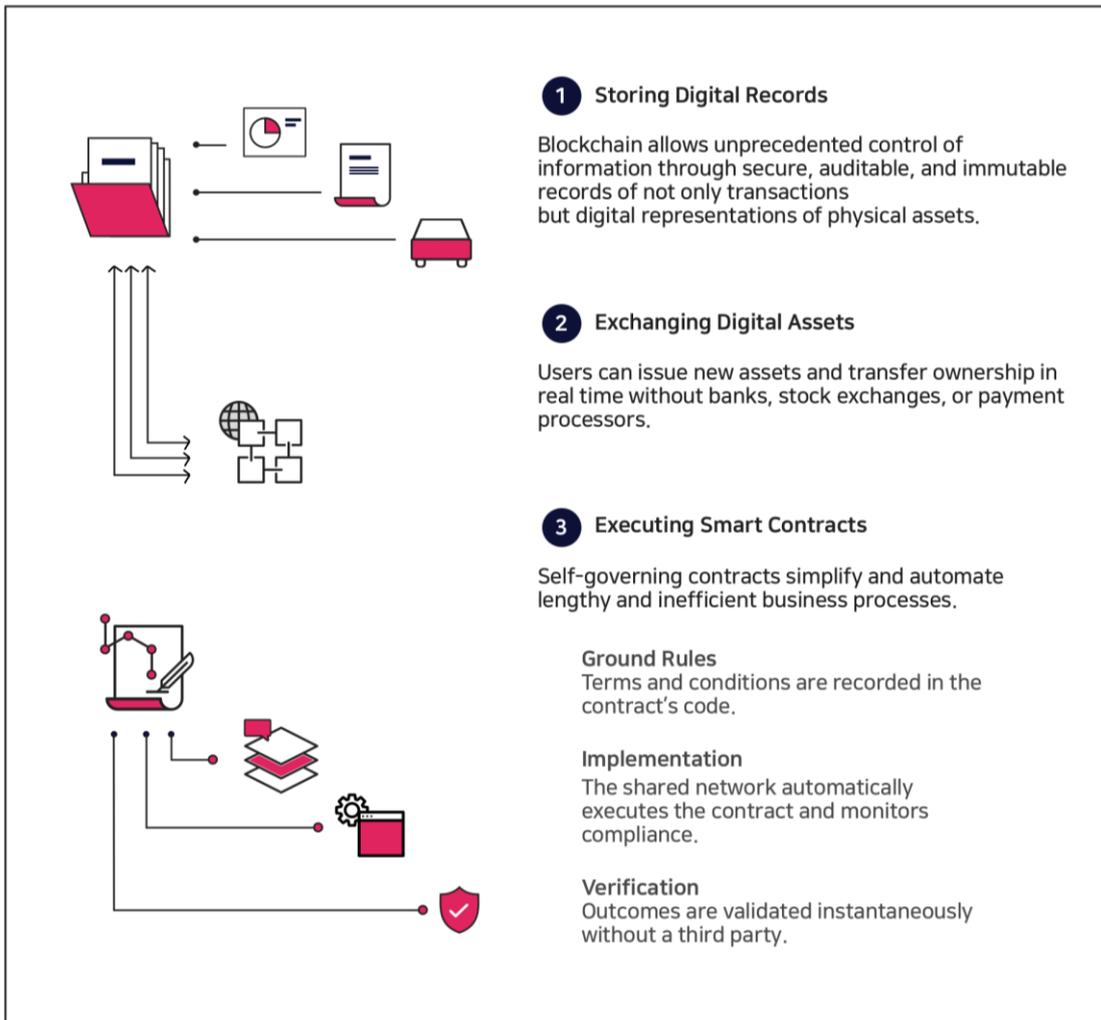


图 18. 区块链在商业中的应用

两种形式的区块链(即公有协议和私有协议)的主要区别特征包括每个系统中的信任和控制级别。信任和控制常常因区块链体系结构的性质和所使用的软件共识算法的不同而不同。控制性的增加常常会导致去中心化信任的减少,反之亦然。随着部署的增加,性能吞吐量也成为区块链的一个严重问题。

公有链,如比特币,提供了最大程度参与的潜力,并增加了网络中更多计算机“节点”的参与。大规模节点的网络运行区块链共识算法增加了去中心化的信任。然而,在这种情况下,如果单个实体占据了这些计算机资源的多数地位,控制权就会成为一个严重的问题。运行当前生成协议和工作量证明共识算法的大型区块链网络效率非常低。它们需要消耗大量的能量来运行节点并验证新交易。交易转账的分发也非常缓慢(特别是对于业务关键操作)。

在私有链(如 Hyperledger Fabric)中,对哪些方(节点)是特定区块链网络的一部分有更严格的控制。使用最先进的计算机、内存和固态硬盘可以提高吞吐量;与节点之间精心设计的网络接口

耦合。然而，这往往导致去中心化信任程度较低，因为网络往往比公有协议的规模小得多。需要更新和更创新的共识算法(图 19 描述了这两个模型)。

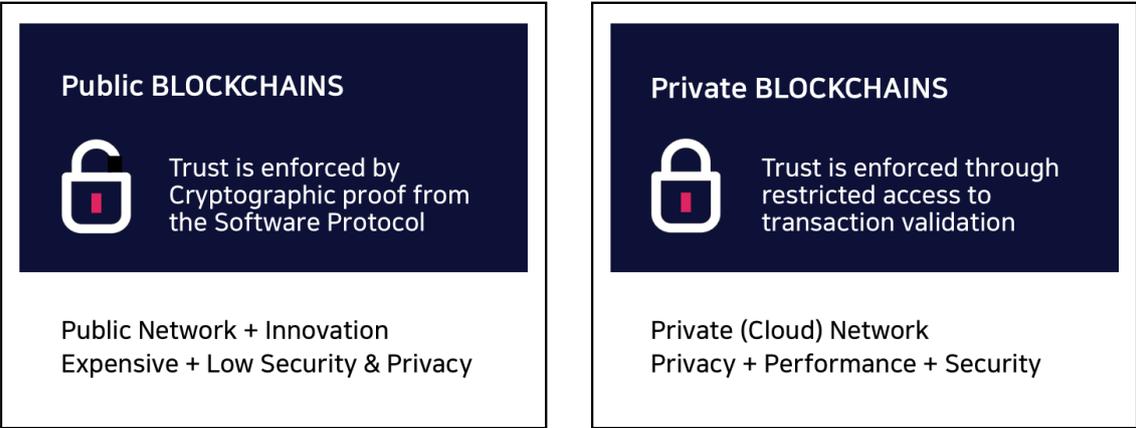


图 19. 无许可公链与需许可的私链对比

决定企业选择公有链还是私有链取决于几个关键的考虑因素：

比如在两者之间仔细权衡

- (i) 必须最大限度地增加对交易的信任
- (ii) 对系统的控制
- (iii) 总体性能吞吐量

例如，在信任和安全至关重要的银行业，私有区块链正被设计用来取代现有的数据库和系统。如下图所示。

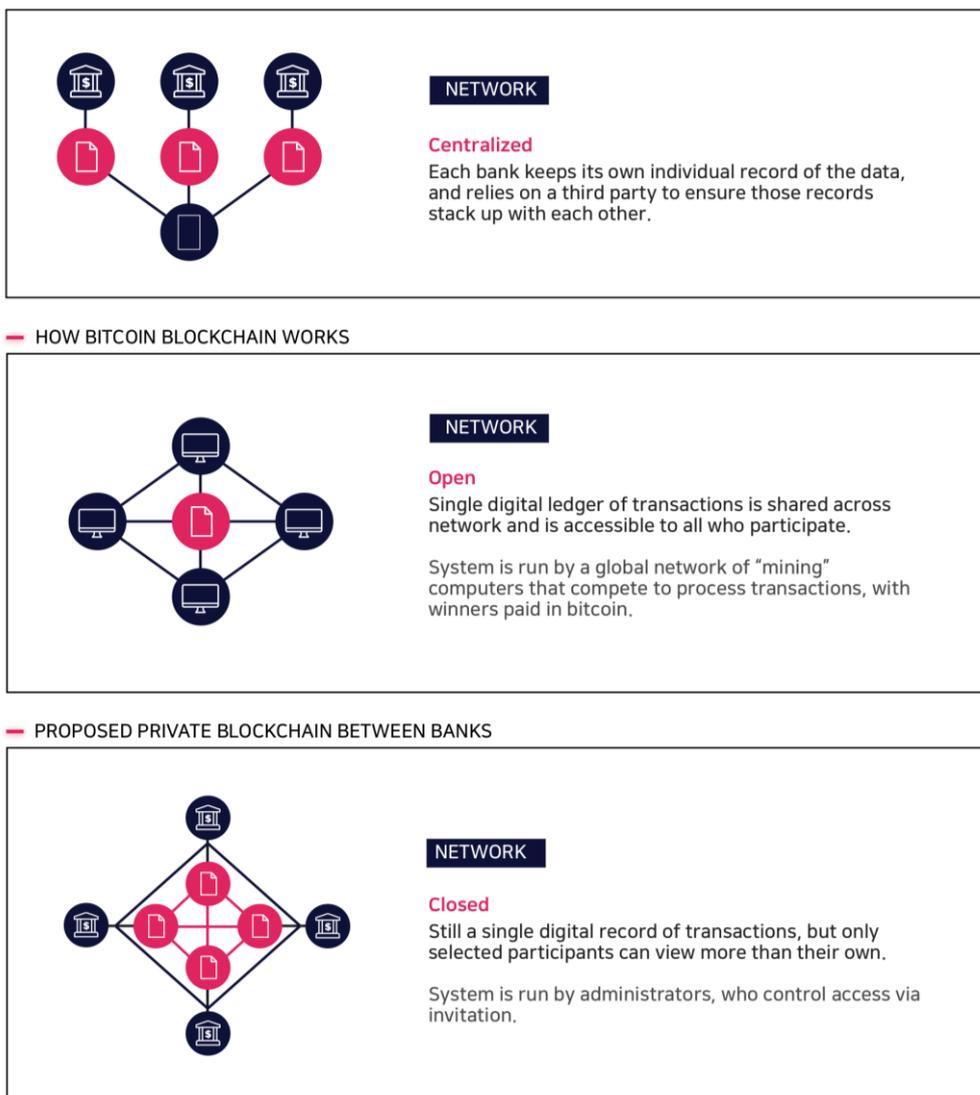


图 20. 区块链网络在银行业中的应用示例

市场和用户往往对到底支持哪一种方式感到困惑。这可能(在一定程度上)解释了为什么仍然有许多不同小产出和大规模的区块链部署。

虽然区块链是(P2P)实现的一个很好的例子，但它并不总是存储大量数据的理想方案，因为：

(1) 可扩展性:区块链可能很慢;和

(2) 数据保护:区块链可能带来一些与数据私隐有关的挑战(例如被遗忘权)，特别是在数据没有得到适当的保护和/或不受适当的管理访问控制的情况下

这些领域目前正在区块链中进行大量的开发，并有望在未来几年找到合适的解决方案。

尽管如此，我们坚信区块链将成为下一代互联网和去中心化网络的驱动力。它可以在没有中间人的情况下实现真正的交易，比特币是它第一个经过验证的用例。

相同的区块链技术可以让每个行业的公司在更开放的商业生态系统中构建新的去中心化服务。

开放平台是未来趋势

创新的 dApp 的结合，运行在一个由无服务器的实用计算架构主导的区块链上——结合使用安全的电子商务服务的大规模的移动应用——我们相信将允许这样的“平台”在未来几年改变许多行业和商业模式。

只要看看东亚，就会发现这样一个开放的、开发者友好的、第三方友好的生态系统的最大例子——非常成功的微信 Wechat²⁰应用程序。

虽然它本身不是区块链的参考模型，但它可能是未来开放生态系统构建和运行的参考模型。更重要的是，它展示了当一个现代的数字平台(如 AERGO)向用户、开发者、商家、第三方和企业开放时，如何创造新的商业价值。

微信是腾讯于 2011 年推出的一款即时通讯应用，目前已经发展成为中国用户的生活方式平台。它每月有 10 亿活跃用户，现在它向用户提供的服务是 Facebook、WhatsApp、Messenger、Venmo、Grubhub、亚马逊(Amazon)、优步(Uber)和苹果支付(Apple Pay)在西方共同提供的。

微信具备强大的用户吸纳能力，成为一个占据统治地位的应用程序。

在以移动应用为主导的中国，微信打造了一种“移动生活方式”，涉及用户生活的方方面面，用户平均每天打开微信 10 次，每天²¹花在应用上的时间约为 40 分钟。它最初是由腾讯(中国三大科技巨头之一:百度、阿里巴巴和腾讯)于 2011 年推出的一个纯粹的短信应用程序，现在已经从一个“应用”演变成了一个“平台”。

微信从中国移动优先市场非常强大的网络效应中受益——无论是直接的还是间接的。平台上的用户越多，其他用户就越想加入，以便与朋友和家人联系。许多亚裔美国人最初只是为了和他

²⁰ Tech Node. (2017). 微信用户和商业生态系统报告 2017 版。链接: <https://technode.com/2017/04/24/wechat-user-business-ecosystem-report-2017/>

²¹ Lily Kuo. (2014). 微信一点也不像 WhatsApp—这使得它更有价值。链接: <https://qz.com/179007/wechat-is-nothing-like-whatsapp-and-that-makes-it-even-more-valuable/>

们在中国的亲戚保持联系才加入微信的。

微信明智地向第三方开发者开放了这个平台，他们开始在微信平台上提供补充或全新的服务。在这里应用范围效应的经济性，平台上的用户越多，越来越多的第三方开发者希望在其上提供服务，反之亦然。

由于其强大的网络效应，而且几乎不需要连接到不同的应用程序或服务(即低所谓的“多归位 multi-homing”环境)，微信成为了一个应用程序平台，或者更确切地说，是一个控制所有应用程序或服务的生态系统。

下面的列表显示了微信对用户的一些激励——以及参与其生态系统的品牌/商家/第三方开发者。

对于用户，微信提供了一个集成的应用程序，允许他们：

- 给家人和朋友发短信/语音信息
- 在社交媒体上分享东西
- 关注名人和品牌
- 预定出租车
- 订购送餐服务
- 预约医生
- 买电影票
- 玩游戏
- 给同事转账(红包)
- 支付账单——水电费、餐厅账单等。
- 寻找地理定位优惠券
- 阅读杂志文章
- 认识身边的陌生人

对于商家/品牌——微信提供了一个集成的应用程序，允许他们通过为这些商家提供支付、位置、直接消息、语音、用户 IDs 等 APIs 来推动用户参与。

商家还使用微信作为 CRM(客户关系管理)平台——发布新闻和提供量身定制的促销活动。微信拥有超过 1000 万个(认证)的官方账号，包括名人、银行、媒体机构、医院、药店、汽车制造商、互联网初创公司、个人博客等。

该平台对开发者也非常友好。他们不会被迫停留在微信的标准外观和感觉之内，因此他们可以开发全新的差异化服务。其结果是，用户无需离开微信平台就能获得完整的互联网应用体验。

2014 年微信的年度生活消费总额预计为 18 亿美元（来源：腾讯），主要由娱乐和官方账号推动。

微信生态系统如图 21 所示。

也许最重要的是，微信不收取用户登录该平台费用——它对用户来说是完全免费的。此外，微信试图通过审查和认证所有在平台上提供服务的商家来确保对生态系统的信任。

我们的理解是，微信背后的团队现在正在探索如何使用区块链为他们的平台构建和添加更多新的安全增值服务。

在微信的一个名为“朋友圈”的模块上，马化腾(中国互联网巨头腾讯的 CEO 兼董事长，也是微信的幕后支持者)在最近的一篇帖子中宣称，“现在是区块链去中心化网络的时候了。”他表示，这项技术可能会破坏现有系统，就像“当前的 TCP/IP，分组交换能够击败 AT&T²²等巨头”。

VC Andreessen Horowitz²³写了一篇非常详尽的关于这个真正创新的开放平台生态系统的文章。

²² Sohu. (2018). 马化腾结识了一些朋友，并评论了物理学家对区块链的看法。链接: http://www.sohu.com/a/218207096_117373

²³ Connie Chan. (2015). 当一个应用程序统治所有: 微信和中国移动的例子。链接: <https://a16z.com/2015/08/06/wechat-china-mobile-first/>

Map of the WeChat mini program 小程序 Ecosystem



01/18 - Made by @tgenaitay le wagon

Tell us what we missed! >> shanghai@lewagon.org

图 21. 微信小程序生态系统图

附录-B: 区块链与效用计算

在不久的将来，我们相信开发者的关注点将从必须理解复杂的编程语言，以及必须满足复杂 IT 体系结构管理和操作中转移出来。这将使他们能够在流程的前端专注于应用程序创新和价值创造；应用程序与终端用户(以及未来几年数十亿的物联网设备)进行接触和交互。

在这种“无服务器架构”中，许多 IT 复杂性将被抽象出来，或者只是对开发者和最终用户隐藏起来。理解这一概念对于充分理解本文非常重要，这也是未来基于 AERGO 的系统将提供的基本价值之一。

无服务器架构指的是主要依赖于第三方 IT 服务(称为后端即服务，“BaaS”)的应用程序，或者依赖于运行在所谓软件容器(功能即服务，“FaaS”)中的定制代码的应用程序，比如使用 Amazon AWS Lambda 的应用程序。通过将许多行为转移到流程的前端，该体系结构降低了 IT 操作成本，并提高了最终用户的性能。

“无服务器”并不意味着应用程序在没有计算机服务器的情况下运行。这意味着拥有系统的人不需要购买服务器，不需要提供它们，或者不需要任何虚拟机来运行后端应用程序代码本身。

下面的简单示例(图 22)描述了一个典型的三层 web 应用程序(不使用无服务器架构)。

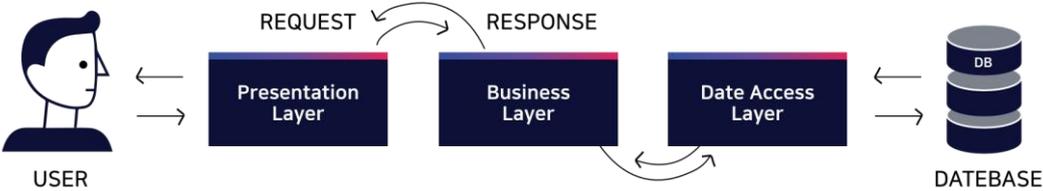


图 22. “3 层” 网络应用示例

该体系结构由三个不同的层组成:所谓的前端展示层、业务层和数据访问层(通常称为后端)。当终端用户在展示层上执行任何操作时，它将调用业务层来处理该操作(例如验证操作)。然后调用与数据库交互的数据访问层。然后返回对业务层的响应，业务层将响应传递回展示层(即实际的用户界面)。

这个周期是许多第一代基于网络的三层应用程序的典型周期。设计这样的系统需要开发者对整个系统具有复杂的知识，并且要考虑到所有东西是如何交互和协同工作的。实际上，他们的大

部分时间都花在使各种元素协同工作上(通常导致专用接口实现)。这与来自 Amazon (AWS)²⁴ 的更现代的无服务器体系结构形成了对比。

体系结构也有三层：展示层、应用程序层和数据层。最大的区别是，每一层都通过标准化接口（所谓的应用程序接口(API)）与它上面或下面的层连接。

因此，理解无服务器体系结构的另一种(更简单)方法是，在一个系统中，后端 IT 业务逻辑可以运行在任意第三方供应商的服务器基础设施上，而开发者不需要担心这些基础设施。

这并不意味着没有服务器来运行您的后端逻辑，而是您不需要维护它。这种无服务器架构是由 Amazon、Azure 和谷歌等第三方供应商提供的。实际上，它在过去十年中催生了云计算。无服务器架构有两种不同的模型：

- Baas 或 MBaaS(其中 M 代表 mobile)；和
- FaaS

使用 BaaS 或 MBaaS，后端 IT 逻辑将由第三方服务提供者运行。应用程序开发者不需要提供或维护运行这些后端服务的服务器或基础设施。在大多数情况下，这些后端服务在启动后将持续运行。应用程序开发者只需要向主机供应商支付订阅(或在未来支付“IT 通行证”)。在大多数情况下，这种订阅持续数周、数月，或者可以每年重复运行一次。BaaS 的另一个重要方面是，它运行在共享的计算机基础设施上，相同的后端服务将被多个不同的应用程序(在所谓的多租户中)使用。

第二种变体 FaaS 如今甚至更受欢迎。大多数领先的(当前一代)技术，如 AWS Lambda 和 Microsoft Azure，以及谷歌云，都属于这一类。使用 FaaS 平台，应用程序开发者可以实现自己的后端逻辑，并在无服务器框架中运行它们。在服务器中运行此功能将由无服务器“框架”处理。这个框架将接管所有可伸缩性、可靠性和安全性方面的工作。不同的供应商提供不同的选项来使用流行的编程语言(如 Java 和 C#)实现这些函数。

对于运行应用程序的开发者或企业，可以使用第三方提供者的服务(如 Amazon API 网关和 AWS Lambda)。这允许开发者构建一个安全、可伸缩和高可用性的无服务器生产应用程序，而无需担心底层数据库层的身份验证、搜索、更新和导航等关键功能的复杂性。FaaS 与 BaaS 的区别不大：

- 成本仅与实际使用的资源数量有关(例如每分钟的级收费)；

²⁴ 无服务器计算和应用程序。链接：https://aws.amazon.com/serverless/?nc1=h_ls

- FaaS 非常适合流量波动较大的应用场景;并且
- FaaS 功能运行时间很短(通常只有几分钟)

理解开发者何时将通过 BaaS 使用 FaaS 的一个简单方法是，开发者何时需要对应用程序如何工作、执行和可扩展性进行最终的控制。

这些创新的应用程序将与其他类似的应用程序连接和交互——同时更小、更紧凑、更移动。这就是所谓“微服务”模型的本质。

这些技术目前正被服务于领先的数字业务的非常先进的开发者所使用(例如在 B2B 和 B2C 移动电子商务和大众消费应用程序，如社交媒体、游戏和通信)。在未来的几年里，这些技术将变得普遍;有各种各样的开发者和公司，而不仅仅是像 Facebook、亚马逊(Amazon)、谷歌、苹果(Apple)和阿里巴巴(Alibaba)这样最先进的公司。

无服务器架构将简化未来后端 IT 系统的维护，同时为处理不同类型的基于分布式微服务的 dapp 提供成本和性能优势。

简而言之，开发者不再把自己视为“水管工”；他们希望专注于创造性的增值应用。

然而，尽管有很多好处，但在处理这些形式的无服务器架构时，需要仔细考虑一些方面;如:

- 供应商固定可能会导致某些问题(例如频繁的强制性 API 更改、价格结构和其他未来的技术更改)；
- 跨网络的速度问题可能会发生，对满足多并发用户的企业级服务水平协议(“SLAs”)的能力提出挑战；
- 由于服务器情况不稳定，使用此类框架维护应用程序状态的稳定非常具有挑战性；
- 不适合运行长时间运行的业务流程，因为这些功能服务将在一段时间后终止；
- 还有其他一些非常重要的限制，比如每秒处理交易数(“TPS”)；经常受所使用的协议和网络内内部连接的 IT 服务的速度所限制;例如内存访问速度、网络速度、稳定性和网络响应时间(延迟)；
- 端到端测试或集成测试难度较大，因为这些动态函数向上自旋且会根据需要显现或隐匿；
- 对生产系统及其行为缺乏适当的监控和调试能力，开发者无法对其性能有充分的信心。

尽管目前存在这些限制，但我们相信，在不久的将来，运行基于 AERGO 的区块链(在无服务器基础设施部署模型中)的基于微服务的 dApps 将成为新兴的分布式效用计算世界中许多新服务的主流部署模型之一。

总之，我们相信无服务器架构的好处对于区块链在未来几年的发展将是极其重要的。

它们提供了以下能力:

1. 使用多个业务应用程序作为服务功能，降低开发成本;
2. 减少操作成本，因为开发者不必考虑基础设施和维护成本;
3. 快速缩放资源(如有需要)，并以完全灵活和自动的方式提供应用程序的水平缩放;
4. 管理和操作 IT 资源要容易得多，因为所有实际的 IT 参与都是由第三方供应商管理的，因
5. 此不需要为这些任务投入资源和时间;
6. 为无服务器的 dApp 应用程序提供内置的可用性和容错性。

向着新的无服务器应用程序的转换的过程已经开始（参见下面的图 23）。

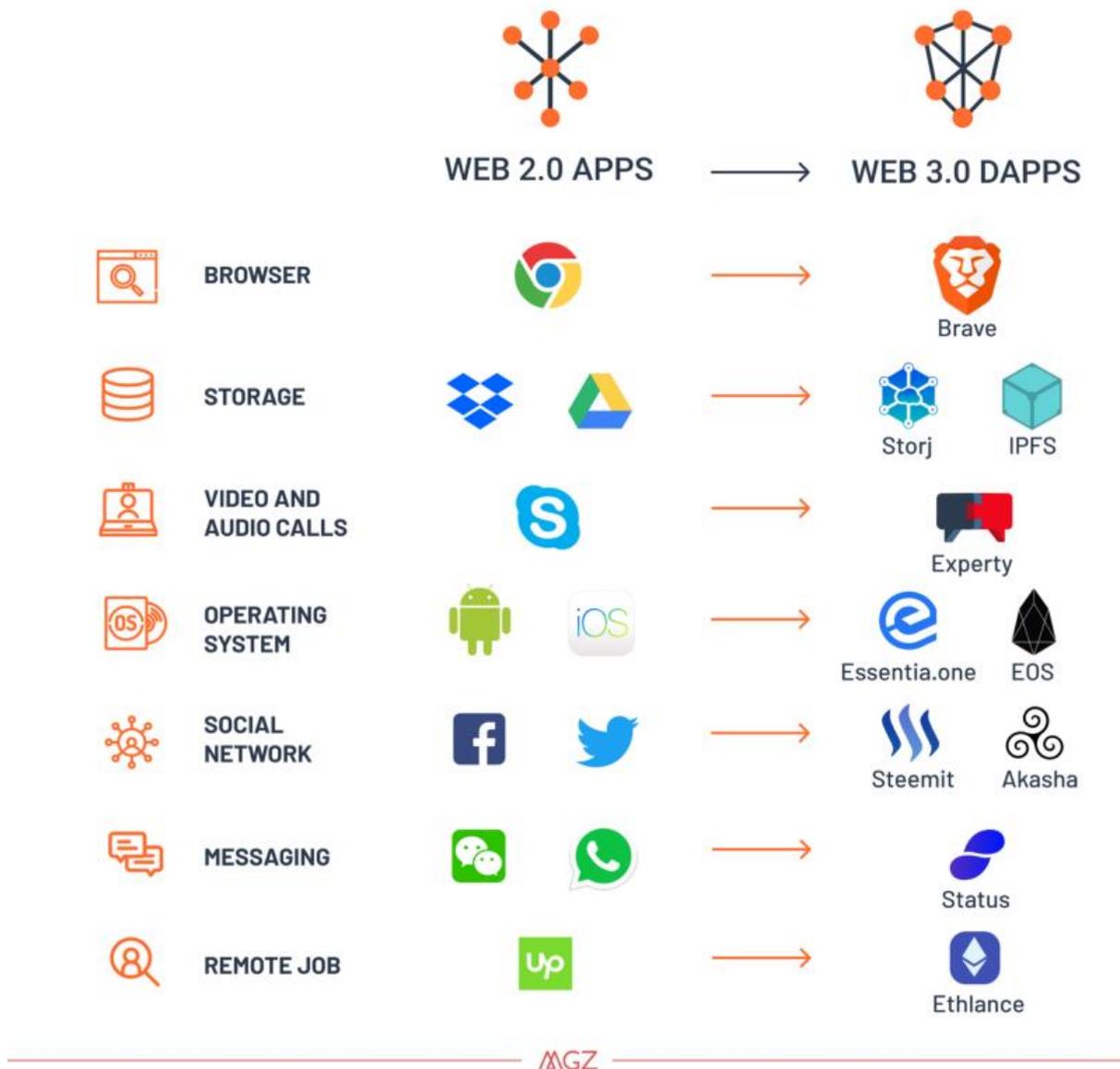


图 23. 从 Web 2.0 过渡到 Web 3.0²⁵

虽然采用无服务器 dApp 的工作仍在进行中，但早期迹象表明，它们将成为企业通过安全分布式云服务交付新服务的主要力量。

目前一些关键任务和大规模的业务应用程序可能不是无服务器计算的直接目标(因为一些安全功

²⁵ Matteo Gianpietro Zago. (2018). 为什么 Web 3.0 很重要，您应该了解它。链接: <https://medium.com/@matteozago/why-the-web-3-0-matters-and-you-should-know-about-it-a5851d63c949>

能和生态系统工具仍然需要成熟)。然而，许多潜在的无服务器计算案例表明，它越来越有可能成为未来公司的“全案”决定。事实上，它将在许多方面类似于云计算在各行业的应用。

随着这种体系结构方法的成熟，我们相信，在处理数字资产和安全数据交换的几乎每个行业部门，将有越来越多的新业务项目采用这种方法。例如，Everest Group 预测区块链将在未来几年内加速在银行业的应用（见图 24）。

Defining Blockchain

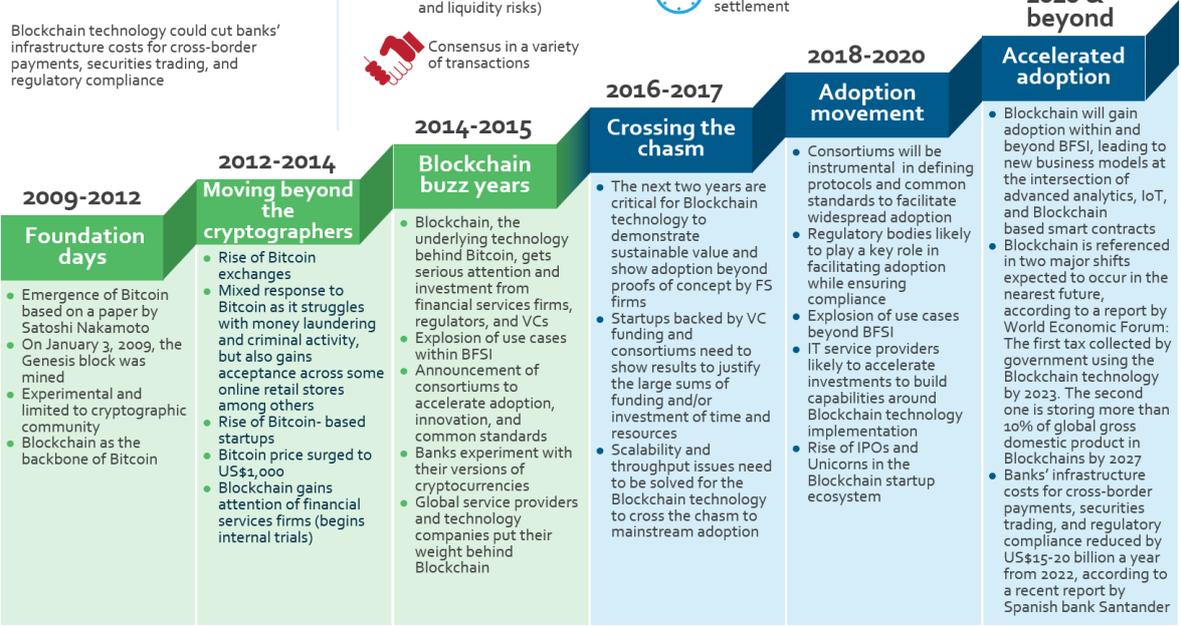
A distributed ledger technology

Blockchain is a cryptographic, or encoded ledger – a database of transactions in the form of blocks arranged in a chain. These are validated by multiple users through consensus mechanisms (such as proof-of-work in Bitcoin mining) shared across a public or private network.

Blockchain technology could cut banks' infrastructure costs for cross-border payments, securities trading, and regulatory compliance

Potential benefits of Blockchain technology for the financial services industry

- Reduce costs of overall transactions and IT infrastructure
- Irrevocable and tamper-resistant transactions
- Reduction in systemic risks (eliminate credit and liquidity risks)
- Consensus in a variety of transactions
- Ability to store and define ownership of any tangible or intangible asset
- Increased accuracy of trade data and reduced settlement risk
- Near-instantaneous clearing and settlement
- Improved security and efficiency of transactions
- Enabling effective monitoring and auditing by participants, supervisors, and regulators



Everest Group Blockchain in BFSI – Looking Beyond the Hype

图 24. 区块链在银行业的应用 (Everest Group)²⁶

今天，许多 dApp 是由使用特定(可能不成熟的)垂直区块链解决方案实现的不同公司构建的。几乎没有标准化，可能导致未来的分裂。这将导致企业在许多不同的业务和产品线中利用区块链带来不必要的成本、复杂性和风险。

²⁶ Everest Group. (2016). 定义区块链。链接: <https://www.everestgrp.com/2016-05-blockchain-technology-bfsi-benefits-market-insights-20805.html/>

今天的碎片化程度和复杂性可以从下图中看到。

WEB 2.0 → WEB 3.0 COMPARISON LANDSCAPE. WELCOME INTERNET OF BLOCKCHAINS

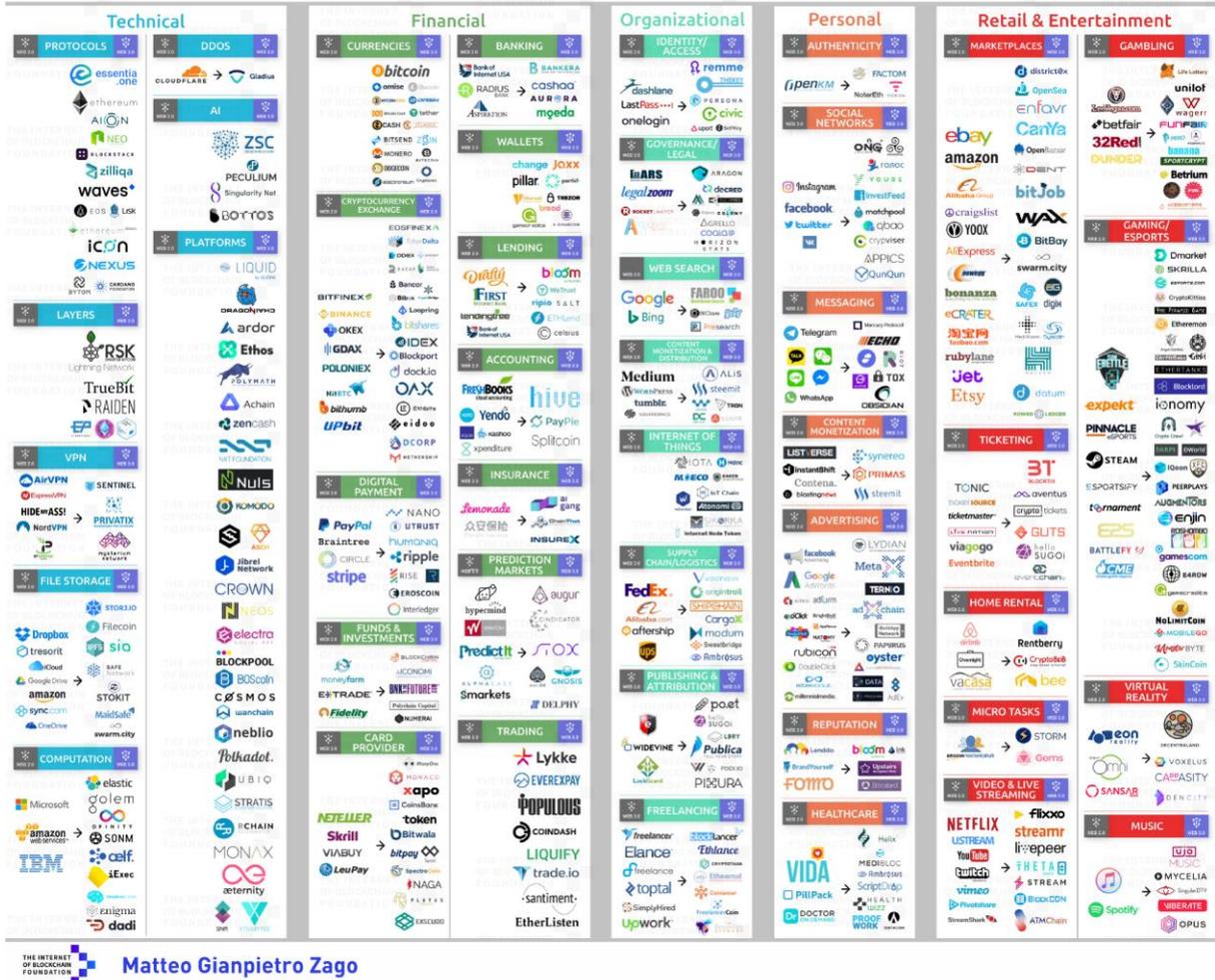


图 25. 区块链解决方案的复杂场景 (今天)²⁷

企业将面临挑战，因为他们将发现很难支持多个区块链解决方案（如第 14 页开始的“采用区块链的障碍”一节所述）。

²⁷ Matteo Gianpietro Zago. (2018). 为什么网络巨头们担心 Web 3.0 呢。链接: <https://medium.com/@matteozago/why-the-net-giants-are-worried-about-the-web-3-0-44b2d3620da5>

附录-C: 公有 VS 私有企业级区块链

公有和私有区块链协议有很多相似之处:

- 这两种网络都是去中心化的点对点网络,每个参与者都维护一个共享的、只包含数字签名交易账本的副本
- 在这两种情况下,区块链协议都提供了数据完整性和不变性(即区块链中包含的数据(特别是其记录的状态)在创建后不能修改——即使网络中的某些错误或恶意参与者)。
- 双方都通过一种称为共识的协议来保持副本的同步
- 即使有些存在错误或恶意参与者(例如,他们在一个不可信的网络环境中工作),两者都对账本的不变性提供了一定的保证。

公有链

在概念层面上,公有和私有区块链之间的主要区别与谁被允许参与网络、执行协商一致协议和维护公开账本有关。一个公共的区块链网络是完全开放的,任何人都可以加入和参与这个网络。网络通常有一个激励机制来鼓励更多的参与者加入网络。比特币是目前最大的公有区块链网络之一。

现有公链的一个缺点是,大规模维护分布式账本需要大量的计算能力。更具体地说,为了达成共识,网络中的每个节点必须解决一个复杂的、资源密集型的加密问题(称为工作证明 **PoW**),以确保所有节点都是同步的,并保持信任。

这个过程是复杂的,缓慢的,消耗大量的能源(电力)。

对特定用户来说,另一个不利之处是许多现有的公链的开放性,这些区块链几乎没有为交易提供隐私(可能存在假名)。它们也只支持一个单薄的理念,即整个系统级别的控制,因为它们向不特定对象开放参与网络。

这些都是未来企业使用区块链时需要考虑的重要因素。

尽管如此,在公链中,没有任何人、团体或组织可以控制区块链上的资料或者支持协议本身的一系列规则。任何成员均不得单方面修改区块链协议和其承载的信息。用户应该能够完全信任公链,并因此完全信任使用相同区块链的第三方。

简而言之,公链可信程度高,但运行速度慢,成本高。公链升级也相对困难,因为它们需要在大量参与者之间达成共识,其中许多参与者的利益可能存在差异(甚至是相悖的)。此外,他们

的可信地位可能会受到各种因素的破坏，例如恶意活动(例如所谓的矿工“抢先”);通过共谋行为(例如，当算力集中于少数参与者时);甚至是由于同时在多个司法管辖区记录和验证交易而产生的法律复杂性。

私有区块链

参与私有链网络需要受邀请，并且必须由网络启动器或由网络启动器放置的一组规则进行验证。建立私有区块链的企业通常会建立一个经过许可的网络。这就限制了谁可以参与网络，以及处理什么交易。参与者需要获得邀请或许可才能加入。访问控制机制可以是多种多样的:例如，现有的参与者可以决定未来的参与者，监管机构可以为参与者颁发许可证，或者由一个企业来做决定。一旦实体加入网络，它将以分布式方式在维护区块链方面发挥作用。

私有链可以(通过仔细的系统级 IT 设计)在交易吞吐量方面实现更大的可伸缩性。

简而言之，私有区块链提供了更好的隐私性、最大的吞吐量，而且运行成本可能更低，但它们缺乏从更广泛部署的公有区块链中获得的信任水平和网络效应。

许多企业都在尝试建立自己的区块链。许多这样的计划(以及相关的联盟)都面临着将这些私有区块链引入实际生产系统的困难。

其中的一些原因可能是:

1. 构建私有区块链系统需要专业的 IT、云和开发者，而只有很少的公司拥有这些要素
2. 使用一个开源模型来构建这些——目的是长期使用、增强和维护这些——是非常具有挑战性的(软件开发和维护通常不是这些业务的核心功能)
3. 上述两个因素可以显著增加此类系统的长期成本

因此，对于希望将区块链技术集成到业务流程中的公司，需要非常仔细地考虑(i)信任加互操作性(公有)需求与(ii)性能加隐私(私有)需求。

在处理公链和私链组合时，这是一个基本的悖论。

大多数企业 PoC 显然是在私有区块链网络中实现的。看起来，其中只有三分之一实际上部署在公共网络上(见图 26 了解银行业中的类似比较)。

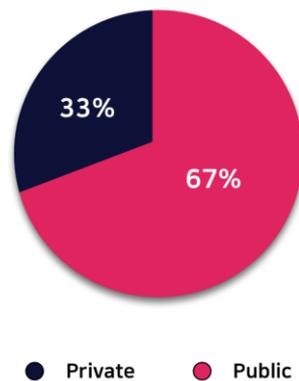


图 26. 在银行驱动 PoC 中使用的区块链类型²⁸

由于严格的安全性和适配性需求，大型公司通常在私有计算机体系结构(如私有内部云)中部署其 IT 系统。出于同样的原因，这些公司中的许多都在试验私有区块链，并选择不使用任何形式的公有区块链。

许多行业协会(如 R3 和 Hyperledger)可能只考虑一种类型的区块链架构，从而限制了它们潜在的长期价值和实用性。

事实上，区块链中的许多创新实际上都发生在公共协议领域。这一点可以从许多大型区块链项目(主要是加密货币驱动的)推动的新思想、项目和服务水平得到证明。这些项目中的大多数确实专注于 dApp 开发，但这也推动了运行它们的底层(主要是公有)区块链的某些创新。

我们相信，如果使用区块链的混合方法，就可以实现真正的变革性商业效益。这种方法将有助于最大化公有和私有区块链体系结构的优点(并减少缺点)。我们看到了在业务架构中获益——使用一个公链提供企业诚信、不变性和不可靠的网络环境,数据和价值(资产)交易——加上一个私链,有助于使监管的记录,隐私和配置和优化所需的企业级性能。

类似形式的混合方法今天已经在云计算中使用。企业将私有云(高度关注信息的)数据中心与低成本的安全公共云(用于商业应用的自动伸缩和性能吞吐量)结合起来。

²⁸ Nivedita Bhattacharjee. (2017). 区块链已经不仅仅是一个流行词，现在有了切实的证据。链接：<https://www.techinasia.com/bankers-like-blockchain>

附录-D: AERGO 团队和顾问

AERGO 是一个处于开发阶段的复杂而全面的项目。它的开发和成功部署将需要多学科融合——即区块链技术、云计算和开源技术。

AERGO 组建了一个真正互补的团队，在这些领域拥有一流的经验和成熟的专业知识。

AERGO 董事会



Phil Zamani

- Global VP Sales & Biz Dev. Internet Embedded Linux Appliances for Redhat Inc.
- Global Head of Big Data & Cloud Biz Models at Santander
- Senior VP of Cloud Biz Unit at Deutsche Telekom



Hun Young Park

- Expertise in Machine Learning solution development
- 12 years of experience in Relational DBMS and distributed solutions
- KAIST, Computer Science. MS



Roderik van der Graaf

- Founder of Lemniscap, an investment and advisory firm in the blockchain space
- 7 years of PE/VC at Caldera Pacific and KCP Capital
- 13 years of equity derivatives trading at Deutsche Bank, HSBC, Rabobank, Bear Stearns, LIM Advisors and All Options
- Queen Mary, Univ. of London, Information Technology. MSc

委员会负责人



Won Kim

Technology Committee Head

- 9 years of experience in Relational DBMS
- 6 years of research & development of distributed systems
- Boston Univ. Computer Science



Jane Lee

Finance Committee Head

- 7 years of experience in Strategy Consulting at Accenture
- Expertise in digital transformation, and technology commercialization
- Cornell Univ. Hotel Administration



Alison Shim

Ecosystem Committee Head

- 5 years of experience in Strategy Consulting at Accenture
- Expertise in go-to-market, and business development
- New York Univ. Economics and Communication studies

技术团队



Yun Woo Park

- 7 years of experience in relational DBMS
- Principal software researcher in database R&D
- Korea Univ. Computer Engineering



Sung Jae Woo

- 11 years of experience in Relational DBMS buffer cache and IO subsystem development
- Expertise in Computational Physics
- Korea Univ. Physics. PhD



Pierre-Alain Ouvrard

- Python, Solidity developer
- Offchain scaling and plasma researcher
- INSA Lyon. Electrical Engineering



Kyung Tae Lee

- 12 years of experience in Relational DBMS and Query engine development
- Expertise in Graph database
- Kangwon Univ. Computer and Communication Engineering



Bernardino Ramos

- 19 years of experience on software development
- Expertise on SQLite database replication
- Creator of Binn, LiteReplica and LiteSync

+25 more

Blocko Team

商业团队



Mason Park

- 7 years of experience in Advertising and Marketing
- Innovator and expertise in branding, marketing strategy & execution
- Univ. of Wisconsin-Madison, Biochemistry



Han Kim

- 5 years of experience in Public Relations development
- Excellence in cryptocurrency dynamics and ecosystem
- HUFS, Social Science



Seona Kim

- 3 years of experience in IT Consulting & Cloud management service
- Strategy project manager and researcher for blockchain market
- HUFS, English-Korea Interpretation & Translation



Camron MirafTAB

- 4 years of experience in innovation strategy and venture capital
- 3 years of experience in blockchain research and due diligence of blockchain businesses
- Newcastle Univ. International Economics and Finance MSc

AERGO 顾问



Eddie Allyn

Eddie Allyn is a technology entrepreneur and expert in security and secure communications. He spent thirty five years leading special projects for the UK Government, in the Ministry of Defence and the Foreign and Commonwealth Office. From 2011-2016 he was Chair and CEO of HMGCC, an agency of the FCO, involved in the design, manufacture and integration of secure communications and cyber systems for the UK Government. He is now an Exec and Non-Executive Director to innovative tech start-ups in the security and cyber security fields, and an Adviser to SANS Institute. Eddie knows how to get the best out of innovative technology and engineering teams to deliver ground-breaking security solutions.



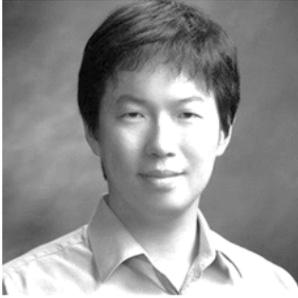
Djamel Souici

Djamel Souici is a legal expert on open source technology, Licensing and business models. He is also a leading advisor and practitioner in Data Privacy and Regulation (such as GDPR). Djamel, a member of the German Legal Barr Association, has spent the past 19 years as General and Legal Counsel for a number of innovative software firms, leading their representations in respect of open source, data privacy and compliance. He has also developed a number of strategic partnerships with many Fortune 100 firms in diverse sectors such as Telecoms, Financial Services, Government, Automotive, Manufacturing, Petrochemicals, Logistics, Retail and Healthcare. Djamel is also a renowned negotiator and expert in international mergers and acquisitions.



Vincent Zhou

Vincent is the founding partner of FBG Capital. He has extensive experience in digital assets trading and investment. His professional experience has seen him work at leading technology companies including the likes IBM and Oracle. With an aptitude towards distributed ledger technology, Vincent has become an early investor in a broad spectrum of blockchain companies and projects. His successes in the blockchain arena has led him to being considered as one of the most well-connected and visionary crypto hedge fund managers in Asia.



Joon-Hong Jake Kim

Jake Kim has a deep understanding of capital markets, strategic business development, as well as hands-on experience in system engineering and back-end computing. He is currently a venture capital and cryptocurrency fund manager based in Seoul where he specializes in corporate venturing, M&A, company building and (selective) Angel investments. He is a seasoned startup investor, adviser and entrepreneur with over 20 years of combined experience in capital markets, consultancy and large-scale back-end and middleware systems development. Jake currently manages Innobase, the corporate venture capital arm of Kolon group. He holds an MBA in Strategy and Corporate Governance from IE Business School.



Sinhae Lee

Sinhae Lee is a Partner at GBIC, leading blockchain investments and accelerating robust projects. Prior to joining GBIC, she has been deeply involved in the FinTech/blockchain industry in Silicon Valley. She led business development and operations at a payment start-up, Coin, which was acquired by FitBit in 2016 and later worked at NerdWallet, a FinTech start-up in San Francisco. She started her career as a management consultant at McKinsey & Company. She brings her Silicon Valley and consulting experience to the blockchain/crypto industry. Sinhae holds an MBA from Stanford University and a B.A. in Business from Korea University.



Pierre F. Suhrcke

Pierre Suhrcke is a leading Fintech expert and investor in Europe, having been active in this sector since 1999. Pierre spent more than 17 years in various senior executive management positions in Investment Banking at Deutsche Bank in London and Frankfurt (Equities, Risk Management and Head of Capital Venture Partners). Pierre is currently a Venture Partner at Tempocap, a European technology investment firm, and a board member of Acorus Capital, a Hong Kong based Private Equity firm. He is an angel investor, mentor and advisor to companies - having worked with and sat on the board of - over 20 successful private companies (US & Europe). He is frequently invited as an expert fintech panel member at leading conferences.



Riad Hartani

Riad is a seasoned technology specialist and strategist with over 20 years contributing to the development of Internet, Mobile and AI technologies. He co-founded and led multiple high-tech startups (Caspian, Anagran, Wichorus and more) with some seeing very successful exits. He has advised over 10 leading technology corporations, numerous private equity houses and several governments and regulators. He also co-founded Xona Partners, a boutique technology and investment advisory firm and ivalley.co, a Fintech co-creation studio. Riad holds a Ph.D in Artificial Intelligence. He is frequently invited as a lecturer, speaker and panelist at leading industry fora and academic institutions

附录-E: 专业术语

分支：在修改控制的前提下复制对象(如源代码文件或目录树)，以便修改可以沿着两个分支并行进行。

并发控制：数据库管理系统的概念，用于解决与同时访问或更改数据(可能发生在多用户系统中的)的冲突。

内容分发网络：由代理服务器及其数据中心组成的地理分布式网络。目标是相对于最终用户在空间上分布服务，以提供高可用性和高性能

去中心化应用程序(dApp)：dApp 的后端软件代码运行在分散式对等网络上。与此相比，典型的应用程序的后端代码运行在集中的服务器上。

拒绝服务攻击(DDoS)：一种网络攻击，作恶者试图通过暂时或无限期中断连接到 Internet 的主机的服务，使计算机或网络资源对其目标用户不可用。

硬分叉：对协议的根本更改，使以前无效的块/交易有效(反之亦然)。

JIT 编译：一种执行计算机代码的方法，包括在程序执行期间(在运行时)而不是在执行之前进行编译。

LLVM：编译器基础设施项目，它是用于开发编译器前端和后端的模块化、可重用的编译器和工具链技术的集合。

合并：合并文件或文件夹的各种版本和/或更改。

微服务：一种软件开发技术——面向服务体系结构(SOA)体系结构风格的变体，将应用程序构造为松散耦合服务的集合。

编译：自动化或系统部署控制理论要素的效果。

并行性：一种计算方法，其中许多计算或进程的执行是同时进行的。

私有链：与公有链相比，区块链网络具有有限的开放性和去中心化性，新节点加入网络需要特定规则下的授权。

权益证明(PoS)：一个人可以根据他或她持有的代币数量来挖掘或验证大宗交易的概念。

工作量证明(PoW)：一种经济措施，通过要求服务请求者完成一些工作(通常意味着计算机处理时间)来阻止拒绝服务攻击和其他服务滥用，如网络上的垃圾邮件。

公有链：一个完全开放和去中心化的区块链网络，任何参与者都可以按照公有链协议加入网络。

序列化：将数据结构或对象状态转换成一种格式的过程，这种格式可以存储(例如，在文件或

内存缓冲区中)或传输(例如，跨网络连接链接)，然后重构(可能在不同的计算机环境中)

无服务器计算：云计算执行模型，其中云提供商动态管理机器资源的分配。

智能合约：一种计算机协议，旨在以数字方式促进、验证或强制执行合同的谈判或履行。

预言机：外部代理程序或程序，用于查找和验证真实世界发生的事件，并将此信息提交给区块链供智能合约本身使用。它们提供外部数据并“触发”智能合约。实际上，智能预言是第三方的“数据输入”。他们以安全和可信的方式提供这些信息。

软件存储库：可以在计算机上检索和安装软件包的存储位置。