第4章
关键区块链网络和技术

首先把区块链网络的概念分成两部分——区块链和网络，并分别对二者进行定义，以便更好地理解。区块链是一个公开的、被广泛复制的记录，记录了区块链上曾经发生的所有交易。这个记录通常被称为账本，就像一个商人用来记录销售和库存的东西。区块链的账本是自该区块链创建到现在所发生的事件和交易的记录。这个记录是不断增长的。当新的交易发生时，它们会被写入记录，并被复制、验证和打上时间戳。

例如，当你给你的朋友玛丽发送比特币时，该交易记录就会被录入比特币区块链。交易记录可以让网络知道，曾经分配给你的地址的比特币，现在已经分配给玛丽的比特币地址。

你的交易记录分布在一个计算机网络中，每个计算机都拥有比特币的完整交易记录。计算机的数量每时每刻都在变化，因为每台被称为节点的计算机都是独立运行的。比特币通常有 1 万个甚至更多的节点，但一个区块链网络只需要两个节点。

更新交易记录的计算机越多越好，这些计算机相互竞争以保持记录的更新。

一个简单的思路是，区块链网络的节点越多，网络越

安全，但这种安全是要付出高昂成本的。一方面，需要权衡参与的计算机数量，数量越多，安全地完成一次记录的时间就越长；另一方面，需要权衡每台计算机在网络中竞争的难度大小，难度越大，节点需消耗越多的电力来保证网络的安全，而这是要花钱的。

区块链网络没有中央服务器来协调和促成计算机之间的通信。它是一个点对点的网络，每个节点直接与其他节点进行通信。所有的计算机都在一个共享的规则集上运行，这套规则让它们知道如何更新交易并与其他节点协作。构成协作的一个重要部分是对记录的当前和过去状态达成共识。它们必须就交易的有效性达成一致。在上面的例子中，你给你的朋友玛丽发送了一些比特币，需要比特币网络上至少 51% 的计算机同意你的交易。网络上关于历史记录的一致意见就叫作共识。

每个节点都有一个完整的历史记录是至关重要的，这使它可以确定每一枚货币的所属都是准确的，并且没有发生欺诈行为。当一台新的计算机加入系统后，它首先要做的是从其中一个对等节点获取最新的副本。

然而，这并不是区块链网络神奇的地方。真正神奇的是当账本需要更新时，网络上所有节点的副本都必须同步更新，且多数节点对此交易达成共识才能记入账本，这类更新操作时刻都在发生。

除了记录你给朋友玛丽发送了一些比特币这样的交易，区块链网络的功能也在不断丰富。为了吸引不同的用户，每种区块链协议都做了修改和定制。有些网络提高了速度，减少了容纳的节点数量，因此用户可以更快地确认交易。有些网络则扩充了它们的功能，以支持简单的网站、游戏平台和智能合约等。这些区块链应用被称为去中心化应用（DApp）。

区块链可以存储和处理这些应用程序收集和生成的数据，其工作方式很像你最喜欢的手机应用程序背后的服务器。但有一点非常重要：区块链的设计旨在永久存储信息，以证明自己的历史。所以，DApp 产生的任何信息，想要储存在区块链上都需要付出较高的成本。

4.1 区块链网络的发展历程

区块链网络是多种技术演进的产物，这些技术已经存在了很长时间，有些已经有数千年。区块链网络创新的基础组件包括密码学、点对点网络、工作量证明和数字签名。

从古代美索不达米亚、希腊和埃及开始，密码学就已经成为人类社会的一部分，换句话说，它已经有 3000 多年的历史了。但是，随着时间的推移，具体的形式和方法在不断变化。大多数区块链网络中使用的公钥和私钥或非对称加密技术是在 20 世纪 60 年代发明的，并被广泛应用于互联网的其他领域。

同时，大卫·乔姆（David Chaum）在 1983 年发表的一篇学术论文中首次提出盲数字签名。大卫·乔姆因 1989 年创立了 Digicash 公司而闻名，这家公司推出了最早的电子现金。乔姆发现的双花问题反映在所有的区块链中，并且他于 2017 年创立了 Elixxir 区块链网络。

工作量证明（PoW）是点对点网络上的计算机如何就共享账本的状态形成共识的一个关键组成部分，最早在 1992 年发表的一篇题为《通过处理或打击垃圾邮件进行定价》的学术论文中出现。论文的作者是计算机科学家辛西娅·德沃克（Cynthia Dwork）和摩尼·纳欧尔（Moni Naor）。

后来在 1997 年，英国密码学家亚当·贝克（Adam Back）开发了哈希现金（Hashcash），这是一个工作量证明系统，有助于限制垃圾电子邮件。亚当·贝克目前是 Blockstream 的联合创始人，这家公司汇集了许多比特币的核心开发者，为区块链网络构建扩展解决方案。同时，点对点网络从互联网诞生初期就开始使用。互联网本身就是一个庞大的点对点网络。

2008 年 10 月 31 日，中本聪在密码朋克（Cypherpunk）邮件列表上发表了题为《比特币：一种点对点的电子现金系统》的白皮书。密码朋克是一个成立于 20 世纪 80 年代末的论坛，旨在倡导使用包括密码学在内的技术，通过推翻政府和大公司的“暴政”，建立更加开放和自由

的社会。密码朋克运动的一些积极参与者包括大卫·乔姆和维基解密创始人朱利安·阿桑奇（Julian Assange）。

在白皮书中，中本聪描述了第一个区块链网络的工作方式。2009 年 1 月 3 日，中本聪推出了第一个区块链网络——比特币。这是一项全新的服务，但构建它的技术模块已经使用了很长时间。现在有成千上万的区块链网络。有些看起来与比特币非常相似，如莱特币（Litecoin）和比特币现金（Bitcoin Cash），而另一些如 Ethereum、Hyperledger 和 EOS 则非常不同，它们承载了大量的 DApp。

区块链技术已经取得了长足的发展。在德勤的《2019 年全球区块链调查报告：区块链进入商业》一文中，对包括巴西、加拿大、中国、德国、以色列、卢森堡、新加坡、瑞士、阿联酋、英国和美国等 11 个国家的 1386 名高级管理人员进行了采访，其中 53% 的高管表示，区块链技术是他们公司 2019 年的重要优先事项。在这些公司中，有许多精心设计的试点项目已经显示出区块链的实用价值和产业化能力。

4.2 区块链网络的主要挑战

困扰区块链行业的一个关键问题是成千上万的项目缺乏所需的技术和开发人才。鉴于该技术相对较新和其分布式所带来的独特挑战，寻找优秀的人才一直很难。由于该领域内优秀的开发者不多，许多项目没有足够的人才来实现他们的宏伟构想，同时许多项目还面临着安全风险和糟糕的设计和执行。

区块链技术的主要用例之一是数字身份和价值转移。银行和消费者身份是高度监管的领域。监管限制了支付和身份认证软件开发方面的创新，这既是好事也是坏事。

区块链正在做一些以前无法想象或没有实现的事情，这项技术可能会像过去 30 年的互联网一样重塑社会。然而，一些政府的反应是严厉的，以保护现状不受破坏。一些国家已经禁止加密货币在其境内流通。这些国家包括中国、俄罗斯、越南和玻利维亚。其他一些国家则让区块链网

络上的资产难以交易。

区块链网络正在努力解决的另一个问题是它们与其他区块链的交互性。大多数区块链开发的开源性质意味着它们没有组织协调或标准。现在许多大学正在努力创建术语标准和开发最佳实践。

互联网之所以成功，是因为早期就存在的不同利益相关者之间的合作。像互联网名称与数字地址分配机构（ICANN）和互联网工程任务组（IETF）这样的机构，就是为了帮助不同的项目进行有效的合作和衔接而成立的。得益于此，当你发送一封邮件时，相应协议［互联网消息访问协议（IMAP）］可以让它跨越不同的平台到达收件人手中。目前区块链网络缺乏类似的可工作接口协议。

4.3 深入比特币

比特币是第一个区块链网络。它有助于促进价值在互联网上以比特币的形式流动和存储。每个比特币都是一个自我认证的数据包，每个数字单位都记录在一个名为比特币区块链的共享账本上。必须指出的是，首字母 B 大写的比特币是用来指区块链网络，而首字母 b 小写的比特币则是指其平台的通证。

比特币是一种加密货币，因为它的价值是通过加密技术来保证的。比特币的数量有一个上限，为 2100 万枚。新比特币通过作为对保障网络安全和处理交易的节点的奖励进入流通领域。这些节点被称为矿工。

新比特币产生的速度在协议中已定义。大约每隔 10 分钟，新的比特币就会释放给网络上的一个矿工，被称为区块奖励。作为奖励的比特币数量每隔几年就会减少一半。在写这本书的时候，每 10 分钟释放的数量是 12.5 个比特币。当达到 2100 万时，也就是 2140 年的某一天，将不再有新的比特币出现。

比特币网络从每笔交易中抽取少量费用。最初，发送者是自愿给费用的。那些提供费用的人的交易确认速度更快，但最后，即使是那些没有提供费用的交易，也会被网络批准并添加到分布式账本上。然而，随

着挖矿奖励的缩水，为了让交易得到处理，交易费变得很有必要。

矿工获得比特币作为维护共享账本的奖励，然后出售给其他人。要接收、存储或发送比特币，你需要有一个钱包。钱包是你安装在桌面或手机上的应用程序。但这里的问题是，基于网络的钱包往往不太安全。更安全的选择是硬件钱包，它是一种专门为保护加密货币安全而设计的设备。

比特币全球推广面临的最大挑战

公有链面临的最大挑战之一是其加密货币的价格波动性。这种波动性会影响到愿意运营独立节点和保障网络安全交易的人数。如果节点运营商不能从他们的工作中获利，他们将转向其他活动。不能够吸引和留住足够多的全节点的区块链很容易受到攻击和腐败[1]的影响。

虚假的负面新闻也是采用区块链的一大障碍。尽管美国反洗钱团队表示，“美元仍然是最好的洗钱方式”，但加密货币在很大程度上与“丝绸之路”（一个黑暗的在线市场）和资助不法活动等非法活动有关。讽刺的是，加密货币为任何货币的交易都提供了最好的视线，虽然一些功能可能看起来是匿名的，但很大程度上是可以从网络中挖出身份的。

换句话说，匿名的前提就是错的。从早期开始，比特币和其他区块链就被主流媒体负面报道。主流媒体将其描述为犯罪分子和其他不良分子的工具，他们希望在执法部门面前隐藏自己的金融活动。因此，受错误信息影响的监管机构试图让加密货币难以获取，并将一些用户关进监狱。

另一类负面媒体则不断宣扬加密货币的失败和死亡。这类媒体煽动了加密货币市场内部的恐慌情绪，并引发了大规模的抛售。虽然很难衡量其程度，但很多觉得比特币令人兴奋甚至有用的人，在开始探索比特币的潜力之前，就已经忽视它了。一个名为“比特币讣告”的网页[2]一直在追踪主流媒体宣布比特币死亡或即将死亡的次数。据该网页显示，

[1] Blockchains that can attract and retain enough full nodes are vulnerable to attacks and corruption. 原文描述有问题，显然是不容易被攻击。

[2] https://99bitcoins.com/bitcoin-obituaries

2010 年至 2019 年期间，媒体宣布比特币死亡的次数接近 400 次。

随着人们对区块链技术的运作方式有了更多的了解，主流媒体开始提供更多的有利报道。但比特币仍然是一个禁忌的话题，经常与犯罪活动联系在一起。一些人承认区块链技术的有用性，但对加密货币仍存有负面的印象。

然而，媒体并不完全是加密货币被负面报道的罪魁祸首。大量利用比特币以某种方式窃取公众利益的骗局给加密货币带来了不好的名声，同时该领域内的黑客也给它增加了负面声誉。2019 年 5 月初，总部位于中国香港的交易所 Bitfinex 被曝出为了掩盖 8.5 亿美元的损失，利用其稳定币 Tether（一种与美元挂钩的通证）的账户秘密弥补了这一缺口。更普遍的是，仅在 2018 年，不良行为者就从投资者手中偷走了价值 17 亿美元的加密货币。

公有链，尤其是比特币，面临的另一个关键问题是可扩展性。当比特币网络在 2009 年 1 月推出时，它可以每秒处理和确认大约 7 笔交易。在早期，这已经足够了，不存在任何问题。然而，随着越来越多的人开始使用比特币，1MB 的区块容量在新用户数量下显得捉襟见肘，很快 mempools（一个节点存放所有待处理交易的区域）就被备份了好几天。近乎即时的交易时间停滞不前，使用比特币的平均交易成本在 2017 年飙升至每笔超过 50 美元。

随着隔离见证（SegWit）和闪电网络（Lightning Network）等扩展解决方案的使用，情况有所改善。然而，展望未来，这个问题还没有完全得到解决。信用卡公司 Visa 每秒可以处理超过 65000 笔交易。如果比特币网络要作为一种全球交易手段进行竞争，它必须处理几乎同样多的交易。

在维护和改进核心软件的开源社区内，扩展比特币已经变成了一个非常有争议的话题。在 2017 年达到了高潮，当时社区分成了对立的两派。事实上，它的争议之大，以至于被形容为一场内战。一方推动区块大小增加至 1MB 以上，另一方则争取保持大小不变。他们希望减少每笔交

易的数据量，被称为隔离见证。隔离见证是一种链外扩容解决方案，它利用一个辅助层，在闪电网络上处理交易。

由于比特币不是一家具有决策或治理结构的公司，因此很难就如何利用现有方案进行扩展达成一致意见。2017 年 8 月 1 日，比特币网络分裂成比特币和比特币现金。那些不希望增加区块大小的人留在了比特币（BTC），而那些喜欢更大区块的人则站在比特币现金（BCH）的背后。即使比特币网络目前可以处理它所收到的交易数量，但如果要与传统支付网络竞争，它仍然需要改进。如果它不能扩大规模，那么可能永远不会被大规模地应用。

主要的比特币贡献者

比特币是一个由用户社区运营的项目。比特币区块链的第一个核心开发者是中本聪，在项目启动后的几个月内，仅有他独立运作。随后，加文・安德尔森（Gavin Andresen）等人也加入了他的行列。当中本聪在 2010 年离开该项目时，他任命安德尔森为继任的核心维护者。

到 2019 年 5 月，Bitcoin.org 上列出了超过 350 名比特币核心贡献者。他们中的大多数都为项目贡献了一些代码。然而，碰巧的是，根据他们所贡献的提交数量，前三名比特币核心开发人员在三大实体的资助下，全职从事比特币项目。

任何具有编码技能和伟大想法的人都可以为项目做出贡献，并帮助比特币变得更好。要做到这一点，就必须写一份比特币改进提案（BIP），并将其发布给社区进行审核。然后，他们应该主导编写必要的代码来实现改变。如果社区的大多数人认为这是一个有用的改变，那么它就会被添加到下一个版本的比特币核心软件中。根据 Github 上的提交情况，以下是三位顶级的比特币核心开发者。

弗拉基米尔・范德兰（Wladimir J. van der Laan）是 Github 上比特币项目提交次数最多的人，超过 6000 次。他在 2014 年 4 月接替安德尔森成为首席开发者。他的职责是合并社区已经同意的核心软件的补丁和其他改动。他由麻省理工学院媒体实验室（MIT Media Lab）

下的项目——数字货币计划（DCI）资助。麻省理工学院媒体实验室是麻省理工学院的一个研究实验室，2016 年数字货币计划宣布为此设立 90 万美元的比特币开发者基金。

马可·法尔克（Marco Falke）作为比特币核心开发的主要质量保证和软件测试人员，发挥了重要作用。他在 Github 上的项目提交次数位居第二，超过 1700 次（2019 年）。马可开始是以比特币志愿者的身份工作，此后转到纽约 Chaincode 实验室工作，继续从事比特币项目。

到 2019 年，彼得·乌耶尔（Pieter Wuille）已经为 Github 上的比特币项目贡献了超过 1600 次提交。2011 年，在发现比特币一年后，他开始作为一名志愿核心开发者工作。他已经成为资源最丰富的贡献者之一。他的一些贡献包括隔离见证，这是一个扩展解决方案，它可以修改进入比特币区块的每笔交易的数据，以此为更多的交易创造空间。彼得还被认为实现了分层确定性钱包，它可以自动生成新的公钥地址，使比特币用户更容易避免过度使用他们的公钥和泄露他们的隐私。

4.4 超级账本

Hyperledger 是一个支持若干区块链倡议的项目，包括 Hyperledger Fabric。从 Linux 基金会拆分出 Hyperledger 帮助区块链技术引入标准，以满足企业和政府的独特需求。其核心重点是促进企业级和开源 “分布式账本”框架和代码库的发展。

分布式账本技术（DLT）被归入区块链技术范畴，但有三点根本性的区别值得注意。这三点分别是：

1. 没有加密货币——没有加密货币意味着交易必须由有激励的节点来处理，因为这些节点与维护其网络和处理的交易有利益关系。

2. 节点是已知的——分布式账本是由相互了解并选择合作的节点运行的。网络是私有的，要操作一个节点必须获得明确的许可。

3. 开发是有指导性的——由 Hyperledger 基金会领导，开发是有指导性的。与比特币不同的是，比特币的开发贡献是自愿的，而非经过组

织指导的。

Hyperledger 的网络是私有的，但是是开源的，所以你可以应用到自己的 DLT。它属于私有区块链的范畴，被称为许可区块链。要加入一个私有或许可的区块链网络，一个实体必须获得管理员的许可。这与公有链网络相反，你不需要任何人的许可就可以加入，因为公有链网络没有管理员。Hyperledger 直接管理其开发和维护。

Hyperledger 是由 Linux 基金会于 2015 年 12 月推出的一个联盟项目。基金会与多家顶级科技公司和金融机构合作启动了该项目。创始成员包括 IBM、英特尔、思科、富士通、日立、摩根大通和富国银行等重量级企业。此后，更多的成员加入了该联盟，目前有近 300 名成员。

Fabric 是第一个在 Hyperledger 上实现的区块链。它已经成为开发许多商业解决方案的框架，并且在区块链生态系统中是独一无二的，因为它允许开发人员使用 Fabric 的部分功能，而无须承诺使用完整的区块链功能。Fabric 是一个许可的区块链，并没有利用加密货币。它可以作为一个量身定制的即插即用的区块链私下运行，是完全中心化的。它砍掉了大部分区块链用于防止串通的安全功能，这并不总是一件坏事。它取决于你的开发目标。

Fabric 上的所有参与者都是已知的，与典型的公有链相比，所有参与者默认都是匿名的。它的工作原理与大多数区块链一样，它保存着一个数字“事件”的账本。这些事件被结构化为交易，并在不同的参与者之间共享。交易是在没有货币的情况下执行的，这又与公有链形成了鲜明的对比，公有链使用其原生货币来支付网络运行费用。挖矿节点被激励去保护网络安全，并因此获得加密货币的奖励。在 Fabric 上，每个节点都由个人运行，他们有动力保护记录和历史，因为这是他们自己的需求，而不是因为他们将获得区块奖励。

即使没有典型的区块链基础设施，在 Fabric 上，所有的交易都是安全、私有和保密的。它只允许通过所有参与者节点的共识进行更新，从而保持其完整性。这意味着，当记录被输入后，它们永远不能被更改。

Fabric 是为那些需要和想要一个可扩展的解决方案，并且不想违反合规要求的企业设计的。所有参与者必须通过会员服务注册身份才能进入系统。然而，你可以在 Fabric 上拥有匿名性，因为它可以为你的交易颁发衍生证书，这些证书与拥有证书的参与者是无法关联起来的，而且每笔交易的内容都会被加密，以确保只有特定的参与者才能理解这些数据。

Hyperledger Composer [1] 是一个易用的工具，允许你创建 Fabric 应用。这些应用不具有可扩展性，但可以轻松地用作概念验证（PoC）。它最大的好处是你能够使用 JavaScript 构建你的区块链网络，因为 JavaScript 是世界上最流行的开发语言之一。仅仅这个特性就会大大减少你对专业区块链开发人员的需求。

Composer 将减少开发时间和成本，让你更快地投入生产。Composer 的另一个好处是它利用了 LoopBacks。LoopBacks 将数字数据回传到你现有的业务系统，从而使你的操作保持同步。你仍然需要一个优秀的开发团队来做这件事，但他们可以很容易地模拟你的业务逻辑并建立系统。

4.5 EOS 的委托权益证明（DPoS）

EOS 是为适应智能合约和去中心化应用而建立的区块链平台。EOS 是在 Ethereum 之后成立的，它致力于解决困扰前两波区块链技术的许多限制性因素，即工作证明的高成本和拥有数千个独立全节点处理交易的速度缓慢问题。

虽然 EOS 的许多先行开发者都专注于创建去中心化系统以及低成本地保存每个人都可以访问的永久记录，但 EOS 更以用户为中心。EOS 的开发团队 Block.one 的信念是，区块链技术必须能够支持数以千万计的日活跃用户。他们认为，使用区块链来保护你的应用不应该是昂贵的。他们想要避免的第三方因素是去中心化开发的陷阱。许多区块

[1] 译者注：从 2019 年 8 月 29 日，该项目就已经被标记为弃用。详情见 https://github.com/hyperledger/composer/。

链在每次软件升级或每次出现需要修复的缺陷时，都会发生高度政治化的冲突。比特币和 Ethereum 都曾因为内斗频繁而停滞发展。

EOS 团队创建了一个新的区块链，它具备以下特性：

- 能支持数百万活跃用户；
- 可以免费使用；
- 具有快速升级和错误恢复能力；
- 具有低延迟性。

这些核心信念极大地塑造了 EOS 的结构。EOS 的主要特点是其共识架构。它使用了委托权益证明（DPoS）。委托权益证明是利益证明的一种变体，一直以来都引起激烈的争论。一些开发者认为委托权益证明在安全性上对可扩展性和降低成本有一个合理的权衡，而另一些开发者则认为，基于一个可以被所有人查阅的永久记录，区块链技术应该尽可能安全和不可改变，以保护系统的本质。

在 EOS 的委托权益证明共识架构中，货币持有者投票选出负责验证交易的代表，他们可以通过工作赚取交易费。当选的第三方区块生产者为整个网络创建新的区块并验证交易。EOS 将执行这一动作的节点数量集中到 21 个。这样做，可以提高网络的速度。EOS 区块链的安全性和完整性是有问题的，这不仅是因为生产区块的节点数量有限，而且因为并不是所有的节点都需要持有 EOS 区块链的完整历史记录，少数不良行为者可能会串通并支持相互投票。

在委托权益证明下，不诚实的区块生产者会被通证持有人清除。EOS 加密货币持有者通过投票来完成这项工作，他们的权力与他们持有的总通证的百分比成正比。区块生产节点不需要自己押注通证，这是与其他股权证明共识架构的区别，后者要求区块生产节点押注自己的加密货币，以此来抑制欺诈行为。在大多数权益证明的系统中，如果区块生产者处理的交易不符合该区块链的规则，就会失去他们的押注资产。加密货币的持有者不会因为投票而直接获得补偿，但出于对其加密货币价值和完整性的维护，他们会被激励拒绝不良行为者。

EOS 加密货币用于促进智能合约和 DApp 的发展。EOS 的通证经济体系与其他智能合约协议有很大的不同。EOS 加密货币的持有者有权按其持有的加密货币总量比例使用网络的计算和存储能力。用户不需要支付费用来执行他们的智能合约。他们只需要持有足够的与完成他们的智能合约所需的处理和存储量成比例的 EOS 加密货币。

EOS 始于 2017 年的一份白皮书，由一家位于开曼岛的密码公司 Block.one 发布。该团队筹集了大约 700 万个以太币。他们筹集的资金估值达到了创纪录的 40 亿美元。Block.one 团队举行了一个运行时间最长的首次代币发行活动，具有讽刺意味的是，他们以 Ethereum 作为筹集资金的手段。

EOS 团队的创始成员包括布兰登·布鲁默（Brendan Blumer）和丹尼尔·拉里默（Daniel Larimer）。布兰登和丹尼尔都在区块链领域活跃了多年。布兰登创立了中国香港最大的数字地产机构 okay.com。丹尼尔联合创办了多家区块链公司，包括去中心化交易所 BitShares 和社交媒体网络 Steemit。

EOS 自首次代币发行以来已经取得了长足的进步，现在已经跻身世界十大区块链协议之列，是市值最大的协议之一。它做了一些品牌重塑，现在被称为 EOSIO。这次更名对应的是 Block.one 团队发布的新软件。

EOS 获得如此多投资者关注的主要原因之一是，它解决了开发一个强大的 DApp 生态系统的许多问题。虽然 Ethereum 是一种替代方案（许多人会认为是竞争对手），但 EOS 以不同的方式实现了去中心化应用的开发和托管，允许更多的可扩展性、更快的速度和更大的灵活性。人们不需要花费 EOS 币来构建和运行 DApp，只需要持有这些通证就可以。

EOS.io 是一个区块链协议，是一个智能合约操作系统，它以其用户设计而闻名，因为它模拟了计算机的实际属性。投资者认为 EOS 将改变企业的互动方式，其中一种方式是提供去中心化的企业解决方案，可以显著提高生产力。EOS 通证的所有者可以通过区块链对各种问题

进行投票，并参与“链上治理”。这使得在做出诸如冻结、特定应用的缺陷修复等关键决策时，可以更加灵活。EOS 还把自己打造成对去中心化应用开发者极为友好的平台。

4.6 Ripple

Ripple 是最令人印象深刻的全球价值转移和交易网络之一。Ripple 成立的理念是，资金应该像信息一样自由、便捷地流动，它的成本低，安全性高，是全球价值交易和交换的快捷方式。它的基础设施正在作为新的现代银行和交易的框架来实施。

不管你信不信，Ripple 出现得比比特币更早。该项目经历了多次迭代，但最初的实现是由加拿大开发者瑞安·富格（Ryan Fugger）在 2004 年设计的。瑞安设计的第一次迭代是一个去中心化的货币系统，允许个人和社区建立自己的货币。

Ripple 已经发展成为一个全球金融结算解决方案，使银行和消费者能够进行价值交换。与比特币类似，Ripple 协议通过允许用户直接和即时交易，降低了结算的总成本。它建立在一个分布式的开源互联网协议上，利用共识账本，并拥有一种名为 ripple（XRP）的原生货币。与公有链不同，不是每个人都可以参与进来，Ripple 上验证交易的节点受到严格控制。XRP 是一次性创建的，并不是通过挖矿区块创建的。

Ripple 的分布式金融技术使用户能够在其网络上进行实时国际支付。利用 Ripple，全球市场可以满足快速、低成本、按需综合支付服务的需求。

Ripple 特别擅长跨境支付和交换两种不同价值的东西。它建立了一个由金融机构、做市商和消费者组成的全球网络，现在他们可以在世界上任何地方即时交易任何类型的价值。

由于 Ripple 对银行业造成了破坏，它不得不与监管机构打了几场仗。金融犯罪执法网络（FinCEN）对 Ripple 违反保密法的行为罚款 70 万美元。罚款的原因是向著名的比特币投资者罗杰·弗埃尔（Roger Ver）出

售 XRP，并且没有提交可疑活动报告，因为罗杰曾因在 eBay 上出售烟花而被判重罪。

关于 Ripple 最恰当的描述是作为一个交换网络和一个具有区块链后台的交易平台。大多数区块链在不知道其他用户身份的情况下运行，而 Ripple 则可以控制谁可以访问他们的区块链。在 Ripple 网络上有两种主要的交互方式。一种方式是该系统的金融用户通过发行、接受和交易资产来参与，以促进支付；另一种方式是作为节点运营商参与。Ripple 只允许少数节点存在，而且运营商的身份都是已知的。节点会跟踪交易，并与网络中的其他节点就这些交易的有效性和顺序达成共识。

与比特币不同的是，比特币不需要用户认识或信任网络上的其他个人，而 Ripple 的整个基础设施则要求各方在一定程度上相互认识和信任。一个金融参与者必须信任它所持有的资产的发行人，一个节点运营商必须信任它的验证者名单中的其他节点不会串通起来阻止有效交易的确认。这就是信任和一致的合作激励。

XRP 是 Ripple 网络的加密货币，它有一个其他加密货币不具备的附加功能。它可以用于促进两个价值相异的事物之间的交易，这些事物的交易量很低，在 Ripple 网络上没有可信路径。在节点、网络和金融参与者之间，Ripple 构建了优化全球现代支付流程和交换的基础设施。

Ripple 一直在通过软件取代一些中央银行的功能。它作为一个中立的交易协议，允许银行和支付网络拥有一个共享的账本，以确保能够在 5 秒钟内完成交易。它给用户之间提供了连续的连接，而且它对整个网络的交易流有持续的监控。

这项技术令银行非常兴奋，因为它使银行能够从中介机构和票据交换所转向一个更快、更便宜、风险更低的系统。通过消除对纸张和中介的需求，银行大大加快了跨境支付的进程。

Ripple 的主要特点：

- 实时支付；
- 全面地交易追踪 ；

- 近乎即时地对账；
- 具有转换几乎所有类型的货币、商品或通证的能力。

要知道，Ripple 与比特币在结构和网络运行方式上有很大的不同。Ripple 找到了最有效的交换途径，将交易结构化为债权，并将瑞波币用作在 Ripple 网络上交易的不同价值类型之间的交换中介。

一个主要的区别是，Ripple 是关于信任的，而在大多数情况下，其他区块链是关于去信任系统的。在比特币中，任何两方都可以互相发送比特币通证，然后网络会验证该交易中没有人作弊。比特币平衡每一个交易区块的方式之一，就是检查确保所有涉及的通证只被花掉一次。

另一个重要的区别来自信任，就是 Ripple 不使用工作量证明共识。Ripple 团队已经消除了大多数区块链为保证自身安全所需要的大量电力负担，这样一来，他们使用的电力就大大减少了。去掉这些传统的功能，Ripple 变得更快。

不是一般的区块链

很容易看出，Ripple 的工作方式与其他区块链有很大不同。其中最值得注意的差异是网络如何去中心化和达成共识。

Ripple 中去中心化的本质是微妙的。一个节点可以把它想要的任何其他节点放入它的验证者列表中，以监听这些节点想要确认的交易。唯一的要求是，验证者列表中的每个节点之间有足够的重叠，以使网络不会意外地得出多个不同的共识。

Ripple 现在的管理方式是让每个节点都维护自己的验证者列表，包括 Ripple 的节点，这样可以确保有足够的重叠。随着节点网络的发展，它的名单将包括越来越多的验证者，而这些验证者来自全球知名的值得信赖的独立机构。随着时间的推移，Ripple 的共识过程将变得越来越去中心化。

重要的是要记住，Ripple 是为更快、更便宜地转移资金而生的。这是一个监管非常严格的经济领域。Ripple 明确表示，它仅仅是能够让你执行这些任务的软件。如何使用它完全取决于你是否理解和遵守法规。

Ripple 和其他通过加密货币工作的区块链一样，存在许多潜在的危险。我在下面列出了一些 Ripple 特有的危险。然而，在加密货币世界工作时，最好总是使用常识，并遵循本书中描述的所有其他安全的最佳实践。它确实是充满机遇和风险的“新大陆”。

使用 Ripple 可能存在的危险

如前所述，Ripple 的诞生是为了比其他网络更便宜、更快地在全球范围内转移价值，Ripple 的结构适用于市场集群。这些市场由受信任的节点一起确认交易。这些群组之间有时会有微小的价格差异，而这些价格差异会吸引不道德的交易。

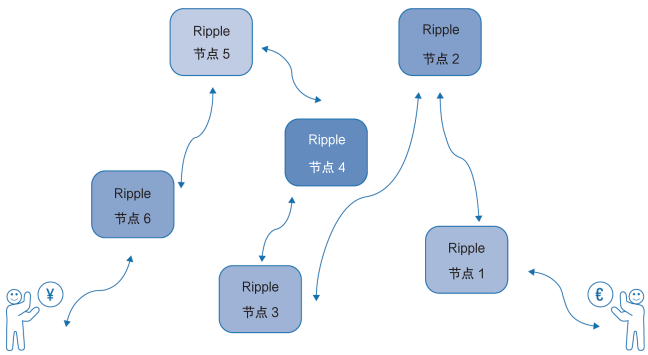

图 23 Ripple——在 Ripple 网络上交换两个有价值的东西

特别是因为 Ripple 网络有很多货币和多个市场，聪明的程序员可以操纵交易的顺序，所以容易出现套利。在 Ripple 上比较有名的两种形式是优势套利交易配售和大额交易前置运行。优势套利交易配售是在账本关闭之前，利用多个市场之间的价格差异进行交易。这种情况每 5 秒就会发生一次，所以交易者利用套利机器人来操控市场。这些机器人会利用市场之间微小的不平衡配对交易的组合，并将其交易推到账本内的最佳位置。然后，交易者通过获取这些市场的价格差来获利。

此外，Ripple 共识中的结构和延迟使网络面临着一种新型的大额交易前置运行的问题。之所以能够做到这一点，是因为网络中的每个节点

都会向其他受信任的节点广播交易。在这段时间里，机器人将监控所有交易，以寻找跳到大额交易之前的机会。

机器人会买下最初的报价以实现大额购买，然后将其加价卖给原所有者。同时，它还会在账本中重新设置来完成交易。这种行为的最终结果是，原始所有者将在交易中获得的价值变少了。

Ripple 致力于清除其网络中的漏洞，并公开向程序员提供通过修复漏洞和缺陷来赚钱。上述两个缺陷极有可能很快被修复。

4.7 挖掘 Ethereum 的内涵

Ethereum 是世界上最先进和最容易使用的区块链之一。它为开发者提供了工具，可以构建他们所能想象的任何东西。Ethereum 最强大的用途之一是其智能合约，特别是符合 ERC-20 规则集的智能合约。ERC-20 智能合约在 Ethereum 上允许成千上万的新区块链项目通过首次代币发行获得资金。

Ethereum 是区块链创新的行业领导者。作为一个全球可访问的共享网络，它在不断探索其可能性。Ethereum 是一个完全公开的分布式的区块链，它允许世界上任何一个人，当然没有受到他们的政府限制，在任何级别上参与开发和使用。了解这项技术是非常必要的，因为它在智能合约、去中心化组织和通证发行方面处于领先地位。

Ethereum 简史

Ethereum 从 2013 年开始，它主要是来自俄罗斯的维塔利克・布特林（Vitalik Buterin）撰写的白皮书，当时他只有 19 岁。维塔利克当时在比特币社区担任写手和程序员，希望扩展区块链技术的功能。维塔利克认识到，区块链的应用远远不止是在没有中央权威机构的情况下转移价值的能力。

当时的比特币区块链社区正激烈地争论着第一波去中心化应用浪潮中大量低价值交易所导致的网络“拥塞”。这些应用创造了大量小额交易，且每笔交易都需要通过比特币区块链实现安全保障，这使矿工的负荷不断

增加，因为他们需要保存完整的交易记录。矿工们不喜欢这种做法，因为这是对他们的存储征税。一些比特币用户也不喜欢这种做法，因为它增加了他们确认比特币交易的时间和成本。

然而，维塔利克和许多其他开发者认为，去中心化应用将是革命性的。要在比特币上实现这一点，需要进行大规模的代码修改，但其政治色彩太浓，无法改变。维塔利克在比特币上的项目是“彩色币”，他与佩雷尔曼（Or Perelman）等人试图在比特币内建立脚本。然而，交易规模限制了这个项目。

维塔利克和其他一些开发者一起决定：他们需要建立一个新的区块链，主要为应用而设计。维塔利克和他的开发者以及业务团队在 2014 年初成立了 Ethereum 基金会。首次代币发行中他们筹集了 1800 万美元的资金。首次代币发行是否违法引起许多人热议，因为它们是一种未经许可的证券发行，但投资者相信他们对通证的投资会增值。美国证券交易委员会（SEC）批准了 Ethereum 的首次代币发行，但一再强调所有其他希望从公众那里筹集资金的创业者必须注册。

在为 Ethereum 筹集资金后，基金会聘请了一个庞大的开发团队来构建它。他们遣散了大部分的业务团队，被遣散的这群人继续组建了另一家名为 ConsenSys 的公司，在 Ethereum 上构建应用程序。

Ethereum 区块链网络的第一个版本叫作 Frontier，于 2015 年 7 月上线。这是一个简陋的软件版本，很难用来构建应用。Homestead 是 Ethereum 的一个更加人性化的版本，于 2016 年推出。它允许任何有一点编程技能的人利用应用程序模板。正是 Homestead 的发布，促进了更广泛的社区建立和应用发展，提高了区块链技术的知名度。在其发布一年后，区块链领域新的基金会和公司爆炸性增长，这些公司都建立在 Ethereum 上，特别是 ERC-20 智能合约，允许他们通过首次代币发行来筹集资金。

随着 Ethereum 的不断扩张和去中心化的运营和发展，Ethereum 又经历了一次转型。该基金会的思维方式与大多数组织的运作方式不同。

他们认为，要想成功培育一个充满活力的去中心化生态系统，必须刻意运用减法哲学。减法的理念是抵制自我或组织内部成长和积累价值的自然倾向。反过来，一个组织要促进组织外部和整个生态系统的价值创造。

Ethereum Serenity 是目前（2019 年）Ethereum 正在进行的开发的名称。它将包括一系列计划中的升级，使 Ethereum 能够降低复杂性，即使在很大一部分节点离线的情况下也能继续运行。它还允许 Ethereum 在有资源时升级到量子安全代码。Ethereum Serenity 正在努力增加去中心化，允许典型的消费者笔记本电脑处理和验证交易。这些升级已经开始，并将在几年内逐步推出。

其中第一个是 ETH 1.x 计划，该计划专注于提高 Ethereum 的短期可扩展性和可持续性，以缓解向 ETH 2.0 的过渡。这种升级的一个重要部分可能是 ZK-rollup。它是一个零知识证明，以使 Ethereum 能够实现每秒数百笔交易。零知识证明是一种密码学方法，通过这种方法，一方可以向另一方证明他们知道某件事情，而不传达除了价值之外的任何东西。

Ethereum 在其“减法”理念上的另一项努力是对 Ethereum 学术与研究合作组织和 ETHGlobal 的支持。他们在世界各地举办黑客松和研讨会，与斯坦福大学和麻省理工学院共同努力，支持数学家、计算机科学家和经济学家的研究。

数千人的合作和努力使 Ethereum 成为有史以来最复杂的区块链之一。它有几种自己的图灵完备的编程语言。图灵完备意味着一种编程语言可以用来创建你能想象的任何类型的软件。

新的图灵完备编程语言的强大功能允许开发人员创建任何他们想要的应用程序，并且仅受限于 Ethereum 网络的经济性和速度。ETH2.0 的实现将颠覆 Ethereum 现有的成本和速度限制。新的编程语言与 JavaScript 和 Python 等流行的编程语言非常相似。

Ethereum 生态系统是目前构建去中心化应用的最佳场所。所有其他区块链都限制了节点的数量，以降低成本和提高速度。Ethereum 社

区致力于创建令人印象深刻的文档和比许多其他区块链更友好的界面。要记住，Ethereum 仍在不断发展中，它可能是一个不稳定的环境，这一点非常重要。许多人可能更喜欢 Ethereum 的私有版本，以此控制去中心化的开发。

即使 Ethereum 是最知名的加密货币之一，许多人认为它甚至有可能在某些时候超越比特币，但事实上，在有关 Ethereum 的合作伙伴关系和规模化应用方面，仍然存在许多挑战。

首先，最重要的是，虽然 Ethereum 可能在许多领域为当前的解决方案提供一个更透明的替代方案，但有些人仍对它质疑。那就是 Ethereum 可能太慢了。当人们考虑到 Ethereum 每秒只能处理 20 笔左右的交易时——当 Visa 等信用卡巨头每秒可以处理数千笔交易时，很难想象它能彻底改变金融行业。有一些人想知道，如果 Ethereum 可能无法像当前的传统系统那样高效地处理交易，那么它如何能够成为革命性的技术。

Ethereum 是最知名的加密货币之一，因此，它面临着来自美国证券交易委员会（SEC）的监管问题。然而，美国证券交易委员会的一位高级官员威廉·辛曼（William Hinman）最近表示，Ethereum 很可能不会因为违反证券规定而被起诉，但目前还没有做出具体决定。美国证券交易委员会主席杰伊·克莱顿（Jay Clayton）似乎同意辛曼的说法，但这并不意味着 Ethereum 一定会摆脱传统的证券监督。

另一个主要问题是 Ethereum 在大规模应用时如何扩展。虽然 Ethereum 目前还不能作为“世界计算机”存在，但有很多人认为，充满活力的开发者社区已经预见到了这个问题，而且各种可扩展性解决方案正在酝酿之中。有的解决方案既关注如何扩展 Ethereum 本身，也关注如何将交易转移到第二层，以提高整体效率。

4.8 Waves——一个俄罗斯区块链平台

Waves 平台是最容易使用的区块链之一。它有一个直观的钱包，内

置去中心化的点对点交易所、投票系统、消息和聊天功能，以及去中心化的域名系统。许多区块链具备其中的一两个功能，但 Waves 平台具备所有这些功能。它可以让你开始使用和创建你最前沿的去中心化应用（DApp），只需简单下载和打开。许多人认为，在构建对公共和私有部门都有利的区块链基础设施时，Waves 将成为不可或缺的一部分。

该项目由俄罗斯物理学家萨恰·伊凡诺夫（Sacha Ivanov）于 2016 年创立，已经有了实质性的增长。Waves 当时筹集了约 3 万 BTC，约 1800 万美元，以创建该平台。此后，萨恰已经构建了很大的社区，并声称在 25 个国家拥有 30 万活跃用户。Waves 在俄罗斯拥有一支由 100 名开发人员组成的专业团队，他们正在不断改进平台。

基于 Nxt Proof-of-Stake 协议，Waves 平台是一个完全公开的区块链，它是去中心化的、透明的、可审计的。它不同于其他使用智能合约基础设施的区块链，比如 Ethereum，或者是比特币区块链的分叉链。其中一个关键的区别是，Waves 允许你创建彩色币。当你创建一个彩色币时，你是将信息与地址相关联，而不是创建你为该特定目的而编写的智能合约。彩色币可以用来代表任何你可能想要在区块链上交易的东西，如股票、债券、商品和房地产等。你可以在 Waves 上几分钟内创建自己的彩色币。

必须记住，你可以创建通证和彩色币，但这并不意味着分发它们是合法的，特别是如果它们是一种金融工具或代表一种投资。在创建可能作为金融工具的东西之前，一定要咨询你的法律顾问。

Waves 通过利用现有账户的余额来 “锻造” 区块以确保其网络的安全。该平台不需要节点 “挖掘” 新的区块来赚取加密货币，而是对验证区块的加密货币持有者进行奖励。验证节点被称为 “铁匠”，并获得交易费用而不是区块奖励。权益证明（PoS）算法之所以流行，是因为它的操作成本更低，甚至可以在 Raspberry Pi 这样的小型设备上运行。

了解区块链的共识系统之间的差异是至关重要的。你可能还记得，

这些都是管理区块链的一套运作规则。具体来说，许多工作量证明区块链很容易受到 51% 的攻击，其中大部分的算力是由少数人产生的，然后他们可以破坏区块链的历史账本中的记录。权益证明系统，比如 Waves，也有其问题。少数个人有可能积累大部分 Waves 加密货币并接管网络。当你在评估一个区块链时，总是要考虑你的业务所需的成本、速度和安全性。

Waves 的定位很好，它是一个重要的平台，可以实现快速、便捷的资产通证化。2017 年的首次代币发行热潮给很多人留下了关于通证化的坏印象，因为其中有很多欺诈行为。Waves 正在努力改变公众对加密货币市场的看法，通过其 BetterTokens 项目培养对加密领域的信任，提高通证的透明度。他们正在为通证化资产的公司制定尽职调查标准。

Waves 团队正在改善投资者保护和监管合规性。他们的部分工作包括建立一个专家委员会，负责评估通证发行商的项目。那些有资格的人会在 Waves 去中心化交易所（DEX）上得到认可。

Waves 去中心化交易所

Waves 去中心化交易所允许你在钱包的安全保障下交易资产。因为 Waves 钱包支持几种不同类型的加密货币，你可以在 Waves DEX 上交易所有的货币，而不仅仅是 Waves 加密货币和 Waves 彩色币。

Waves DEX 解决了一个阻碍去中心化交易所广泛使用的问题。他们通过将订单簿匹配器中心化来创建实时交易。这使得他们可以更容易地连接买家和卖家。Waves DEX 是中心化和去中心化交易所技术的混合体。它的中心化匹配引擎对传入的订单进行配对，并通常在几毫秒内执行你的交易。相比其他完全集成在区块链内的 DEX，这是它的优势。完全去中心化的交易所依赖于其区块链的区块时间速度，交易成本要高得多。即便如此，流动性可能仍然是一个问题，因为 DEX 没有完整的市场生态系统，如帮助保持价格稳定的做市商。

在 Waves DEX 上，通过创建、签署并向 Waves 匹配器发送有限的订单请求来表明购买或出售资产的意愿。买入订单是指以等于或大于规

定的价格购买一定数量的通证。当你创建一个新的订单时，它会被发送到去中心化交易所。然后检查你的订单是否准确，以及你签名的有效性。它由你的钱包的公钥验证。

Waves DEX 上的订单是成对链接的，并由 Waves 节点进行检查。然后，匹配器会创建一个交易所交易；它将在 Waves 区块链上签署并记录交易。你不必执行一个完整的订单，因为匹配器可以配对部分订单。验证节点不会向这些未完成的订单收取完整的订单费用。交易在 Waves 区块链上发布后，你的资产才会被转移。如果匹配器因某种原因失败，你的交易将被取消，所有未完成的订单将在 30 天后自动取消。

Waves 已经进行了一些高调的合作，包括与全球最大的专业金融服务公司之一的德勤会计师事务所的合作。合作的意义在于为机构客户提供首次代币发行方案和定制化的区块链解决方案。

Waves 区块链如果要实现其雄心壮志，确实有很多挑战需要克服。有人担心它过于以俄罗斯为中心，无法在全球范围内发挥其潜力。俄罗斯经济可能是孤立的，这不是什么秘密；其政治一直很激烈。由于 Waves 完全与俄罗斯紧密相连，其许多战略伙伴关系涉及俄罗斯公司而非全球公司，因此它可能无法在其他国家获得吸引力。

4.9 小结

当前已经有数百种区块链和数千个区块链项目，而且这个数字还在与日俱增。本章只介绍了目前最激动人心、最有前途、最受欢迎的计划中的一小部分。

其他在未来值得你关注的举措包括脸书新兴的 Libra 计划[1]。Libra 将是一个建立在已经验证过的工作基础上的私有链。它将包含一种通证，提供完整的编程语言，允许创建 DApp。也许最重要的是，脸书的所有现有客户都有可能加入到 Libra 生态系统中。

未来的经济商业模式和行业正在诞生，这要归功于用于创建区块链

[1] 2020 年 12 月份，已经更名为 Diem。

的几种旧技术的融合。最明显的用例是身份、通证化、跨境支付和去中心化应用。这些创新都激发出了各自的新兴行业。而在下一代的区块链技术中，极有可能出现更多的创新和突破性的变化。

4.10 本章小测验

1. 区块链技术的四个主要用例是什么？

A. 区块链技术的四个主要用例：存储、数字身份、价值转移和去中心化应用。

B. 区块链技术的四个主要用例：通证化、数字身份、价值存储和中心化应用。

C. 区块链技术的四个主要用例：通证化、数字身份、价值转移和去中心化应用。

D. 区块链技术的四个主要用例：游戏、欺诈、首次代币发行和应用。

2. 在一些国家交易比特币是否违法？

A. 是

B. 否

3. 第一个区块链网络是什么？

A. 第一个网络是 Ripple。

B. 第一个网络是 Ethereum。

C. 第一个网络是 Waves。

D. 第一个网络是比特币。

4. 比特币有没有进行首次发币？

A. 有

B. 无

5. 使用比特币和发送交易是免费的吗？

A. 是

B. 否

6. Hyperledger 是一种公有链吗？

A. 是

B. 否

7. Hyperledger 挖矿的加密货币名称是什么?

A. Hyperledger 挖矿的是 Hyper。

B. Hyperledger 挖矿的是 HXP。

C. Hyperledger 不使用加密货币。

D. Hyperledger 从比特币、Ethereum 和 Ripple 中挖矿加密货币。

8. EOS 支持哪种类型的共识架构?

A. EOS 的共识架构是委托授权证明（DPoA）。

B. EOS 的共识架构是委托工作量证明（DPoW）。

C. EOS 的共识架构是权益证明（PoS）。

D. EOS 的共识架构是委托权益证明（DPoS）。

9. EOS 有多少个验证节点?

A. EOS 有 11 个专用节点。

B. EOS 有 21 个专用节点。

C. EOS 有 31 个专用节点。

D. EOS 有 51 个专用节点。

10. 在 Ripple 网络上可以挖掘 XRP 吗?

A. 能

B. 不能

11. 什么是 ERC-20？

A. ERC-20 是 Ethereum 网络的通证标准，允许开发者创建可与多个钱包和交易所互通的通证。

B. ERC-20 是 Ethereum 网络的共识算法。

C. ERC-20 是 Ethereum 网络的原生货币。

D. ERC-20 是监督 Ethereum 网络安全产品的监管机构。

12. Ethereum 引入了区块链技术的哪项重大创新?

A. Ethereum 是第一个做首次代币发行，允许成千上万的人使用 ERC-20 通证筹集资金。

B. Ethereum 是第一个区块链。

C. Ethereum 拥有多种图灵完备的编程语言。这一创新允许开发人员在区块链内创建他们想要的任何应用程序。

D. Ethereum 使用多算法方法来挖掘比特币。这一创新让开发者可以更快地保障更多区块的安全。

13. Waves 平台使用哪种类型的共识算法和网络结构来保证自身安全?

A. Waves 是 10% 权益证明（PoS）和 90% 工作量证明（PoW）的公有链。Waves 通过利用现有账户的余额来确保网络的安全，以“锻造”块。

B. Waves 是 100% 权益证明（PoS）的公有链。Waves 通过利用现有账户的余额来“锻造”区块，从而保证网络的安全。

C. Waves 通过利用现有账户的余额来“挖矿”来保证网络的安全。

D. Waves 是一个私有链。Waves 通过有专门的审计节点来保证网络的安全。

14. 什么是 DEX？

A. DEX 是一个去中心化的交易所，它允许你从一个中心化的交易所交易资产。

B. DEX 是一个聊天平台，允许你与其他通证持有者进行资产交易和交谈。

C. DEX 是一个分布式交易所，允许你从钱包的安全性中交易资产。

D. DEX 是一个去中心化的交易所，允许你从你的钱包的安全性中交易资产。