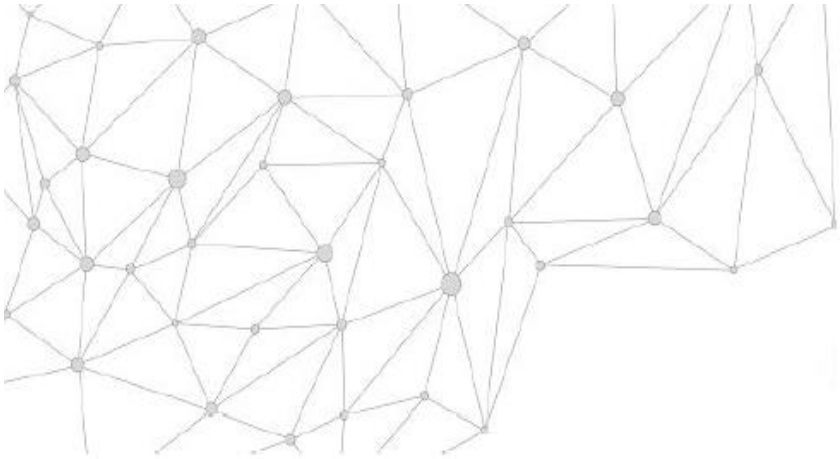


区块链中心

区块链
初学者指南

区块链
Web3
密码经济
代币
智能合约
分布式应用
去中心化组织
首次代币发行

区块链行业词典

区块链王座

2018 年 3 月 5 日

翻译：Stanley Diao，杨勇，陈骆虹，孙骁，陈昱霖，Jessica, 也佳, Jiaqi Yi

目录

区块链基础
区块链
去中介
智能合约
Web3-去中心化
重新设计数据结构
从“数据专制”到“数据民主”
Web3 技术栈
区块链种类
公有链
联盟链
私有链
区块链数据库
不同分类标准
密码经济
P2P 网络中的机器共识
经济共识准则
升级／改变共识
代币
代币种类
法律地位
智能合约
降低交易成本
智能合约特征
智能合约举例
智能合约种类
智能合约编程
Oracle
Oracle 种类
安全问题
去中心化软件（dApp）

dApps vs 智能合约
dApps 要求
dApp 开发流程
举例：Ethereum dApps
dApp 许可证
DAOs
去中心化组织
颠覆统治
Daos 的运用
Daos 作为众筹平台
法律要求
首次代币发行
众筹还是众投?
规则
首次代币发行种类
首次代币发行历史

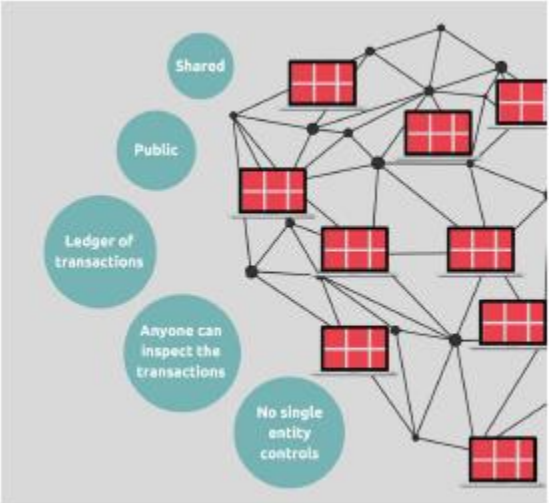
实用指南
如何开始一个区块链项目
如何寻找区块链开发者
如何购买比特币
比特币投资
如何参与首次代币发行

区块链基础知识

在第一部分中，我们将介绍区块链、智能合约和去中心化网络的基本原理。这一部分概述了区块链技如何运作和其为何将带来巨变。在第二部分中，我们将重点介绍一些实用的操作指导。

区块链

区块链作为比特币背后的技术，是下一代互联网，即去中心化网络Web3背后的驱动技术。区块链是一个解决亘古人与人之间互信的新方法，提供了所谓“去信任”的互信架构。它允许我们系统的输出，而不依赖于其中的参与者。

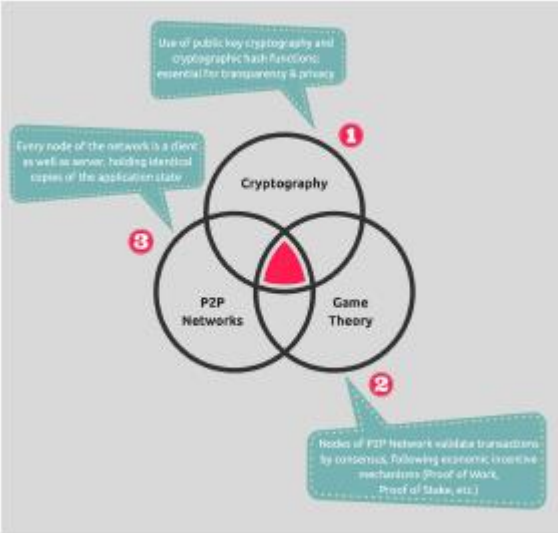


比特币：类似空中的数据表

来源：Blockchainhub.net

共享，公有，交易账本，每个人都可以查账，个体无控制权

区块链是一个共享的、可信的、公开的交易账本，每个人都可以检查但没有人可以控制。它是一个分布式数据库，将新的交易数据不断记录到列表中，并通过密码保护防止数据的篡改和修改。



三大技术的融合

来源：Blockchainhub.net

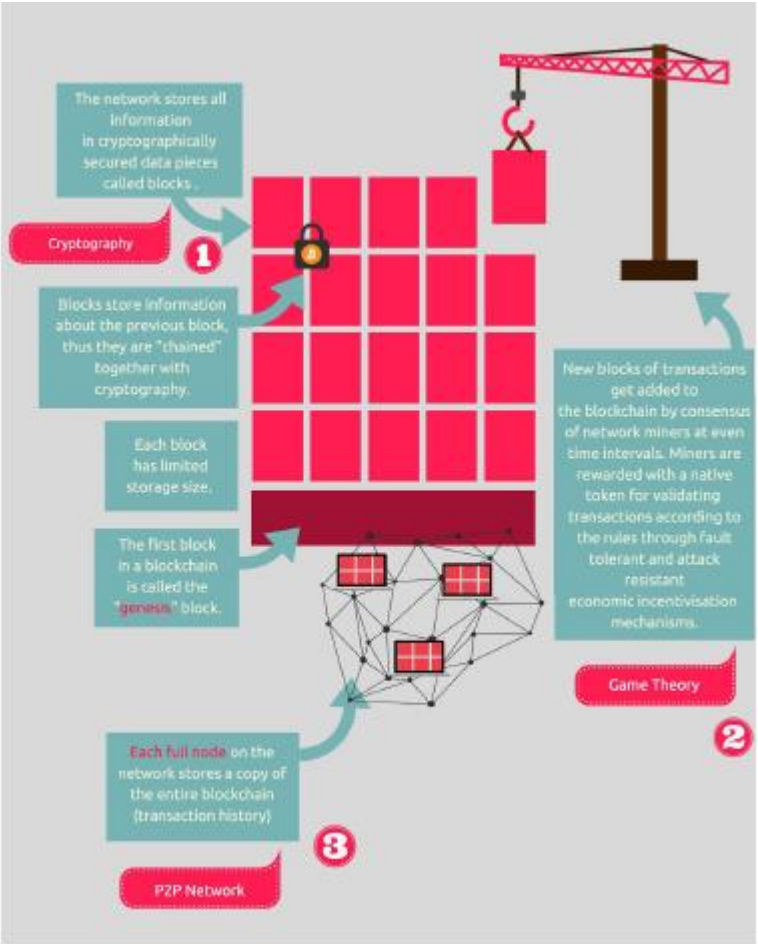
1.密码学：运用公钥密码学和散列编码：保证透明和隐私

2.点对点网络：每个节点网络都是一个用户，也是一个服务器，保有相同的交易副本

3.博弈论：点对点网络的节点通过共识验证交易，基于经济激励机制（工作量证明，权益证明等）

区块链协议可以在互联网，以及在所有运行该协议的计算机 P2P 网络上运行，所有的协议都保有相同的交易总账副本，这使得 P2P 的交易无需中间人，只需依赖于机器共识。区块链本身是一份文件——一份共享和公共的交易记录，记录了从创世块(第一个区块)到今天的所有交易。

分布式账本是使用链表或区块链构建的，其中每个区块包含在给定时间范围内一定数量通过网络验证的交易。区块链协议(共识层)的密码经济规范了网络中所有利益相关者的行为规则和激励机制。



为何称作区块链?

来源：Blockchainhub.net

密码学:

网络中保存了所有通过密码学加密的数据，称作数据块

数据块保有之前交易的信息，和密码一起构成了数据链

每个区块都有限制的贮存量

数据链中的第一个区块称为“创世块”

博弈论

新的交易在通过矿工的验证后将添加到区块链中，矿工将因验证交易获得代币的奖励，基于容错和抗攻击的经济激励机制。

点对点网络

网络上的每个节点都有整个区块链的副本（交易历史）

分布式账本是在计算机的点对点网络（P2P）上运行，分布式协议基于经济激励机制

（博弈论）与密码学，保证了 P2P 交易的安全验证，从而无需传统验证互信的第三方。

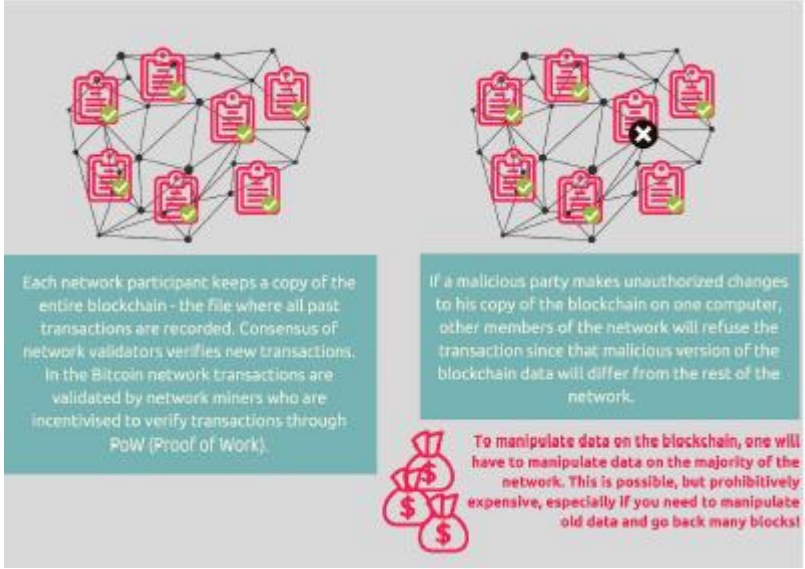
2008 年 10 月，分布式账本作为比特币提议的一部分首次被提出，目的是在没有银行的情况下创建点对点的货币。所有的网络交易信息都可以存储在区块链中:想象一下谷歌文档:每个人都有最新版本的文档且每个人都可以检查。如果需要改变文档的内容，用户之间需要达成共识。

相比于非中心化存储的谷歌文档，但网络的每个节点都保留了区块链的副本——分布式账本记录所有交易历史。

去中介

点对点网络的计算机通过协商一致 (多数投票) 的方式运行区块链协议来验证交易，而非通过一个单独的可信第三方通过服务器(单一投票)对交易进行验证。

因此区块链协议将预先定义的共识规则规范化，作为确定的治理法规，用于在 P2P 网络上验证交易,，管理和自动执行网络中所有参与者的交易。



为何区块链可以防止篡改?

来源：Blockchainhub.net

每个参与者都保有整个区块链的副本-包含所有过去交易历史的文档，通过网络共识验

证新的交易。在区块链网路中，矿工受到工作量证明（PoW）的激励会对交易进行验证。

如果有恶意组织想对某台电脑上的区块链副本进行未授权的篡改，网络中的其他成员会拒绝授权交易因为该副本不同于网络中的其他副本。
想要操纵区块链的数据，需要操纵区块链网络中大部分的数据。这不是没有可能，但是代价很高，特别是还需要追溯之前的区块和修改旧的数据。

一个运行比特币协议的点对点网络将检查用户在服务器上存储的数据，通过协商一致的方式验证交易，这有别于银行验证金融交易——比如把钱从 A 汇到 B。

比特币网络的共识规则规范了参与者的互动，并定义了：
❑在哪些条件下交易——从 A 到 B 汇钱——是有效的
❑从 A 到 B 汇钱的交易成本
❑基于博弈论原理中激励机制，通过加密代币验证交易
❑如何改变目前的共识准则的规则

智能合约

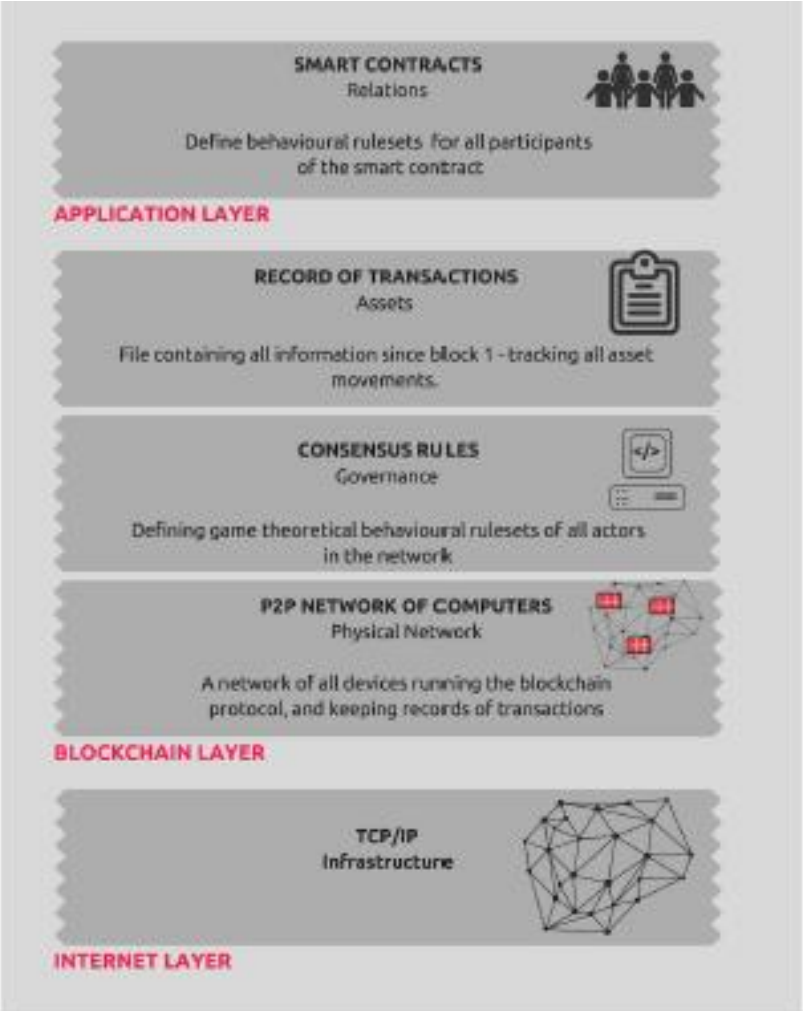
区块链最初是为 P2P 贷款而设计的，它很快就显示出了适用于互联网上任何一种 P2P 价值交易的潜力。因此，Ethereum 项目引入了将契约层与区块链层分离的想法，在这种情况下，在满足某些预设条件时，可以自动触发交易的智能合约。通过将智能契约层与区块链层分离，类似 Ethereum 的区块链相比比特币区块链而言，提供了更灵活的开发环境。

这些智能合同是在区块链网络上运行的一段代码，其中数字资产由执行预设规则的代码控制。这些合同有协议的性质，但不应与法律合同相混淆。(更多关于区块链的法律问题的信息请访问我们的区块链法律页面)。

如果智能合同各方履行预先定义的规则，智能合同将自动执行交易。这些智能合同的目的是提供优于传统合同法的交易安全，降低协调和执行交易的成本。

智能合约可以用于简单的经济交易，比如从 A 向 B 汇款，也可以用于注册任何类型的

所有权和产权，比如土地注册和知识产权，或者管理共享经济的智能访问控制。此外，智能合约还可以用于更复杂的交易，比如管理一群拥有相同兴趣和目标的人。分散的自治组织 DAOs，是智能合约更复杂的一个例子。



智能合约技术栈：以太坊和类似的区块链

来源：受 Florian Glatz 的启发

智能合约（关系）- 所有参与者规定的条款

<u>应用层</u>

交易记录（资产）- 包括所有信息的文档，跟踪左右资产的变化

共识规则（治理）- 针对网络中所有参与者的理论化的行为规则

点对点计算机网络（实体网络）- 由所有运行区块链条约并且保有交易记录的设备组成

<u>区块链层</u>

互联网协议族（TCP／IP）构成的底层设计

<u>网络层</u>

有了区块链和智能合约，我们可以想象这样一个世界:合约被嵌入到数字代码中，并存储在透明的共享数据库中，保护它们不被删除、篡改和修改。

在这个世界上，每一个协议、每一个过程、任务和支付都会有一个数字记录和签名，可以被识别、验证、存储和共享。像律师、经纪人和银行家这样的中介机构和公共行政人员可能不再必要。个人、组织、机器和算法都可以以很小的摩擦和交易成本自由地进行交易。

区块链和智能合约:

❏从根本上减少交易成本(官僚)通过机器共识和自动执行的代码

❏避免了传统的委托代理问题,提供一个“去信任”的互信架构。这意味着人们将不必信任其他人和组织，只需信任开放源码和提供透明流程的代码

Web 3.0 – 去中心化

在 20 世纪 90 年代，互联网革新了我们对于信息的理解，10 年之后，互联网愈发成熟和易于编程。我们见证了所谓 Web 2.0 的兴起，它为我们带来了社交媒体和电子商务平台，革新了社交互动，融合了信息、商品和服务的生产者和消费者，让我们在全球范围内享受点对点的互动。

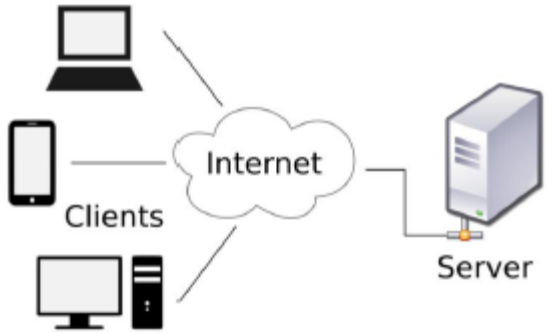
但是总有一个中间人- 如果 A 和 B 互不了解、互不信任，那么就会有一个作为平台作为双方的信任中介。这些平台成功创造了点对点经济和更加复杂的内容发现层，但是它们也规定了所有交易的规则并拥有我们全部的数据。

在这样的背景下，区块链驱动了下一代去中心化网络 Web3.0。它能让我们在无须中间人的情况下相信点对点交易，比特币就是第一个案例。比特币是一种无需银行和银行经理介入的点对点货币，其背后的科技将是我们享受无需 Uber 的共享汽车，无需 Airbnb 的共享公寓和无需 Facebook 和 Twitter 的社交媒体。

重新设计数据结构

我们首先拥有电脑，然后通过互联网协议连接了各个独立的电脑。在个人电脑问世的早期，我们将数据存放在软碟中，然后把文档复制到电脑上，这样别人也可以使用。

数据被存储在一个中心化的实体设备中，为了传输数据，我们创建副本。互联网加快了传输这些副本的速度并在很大程度上降低了交易的成本。

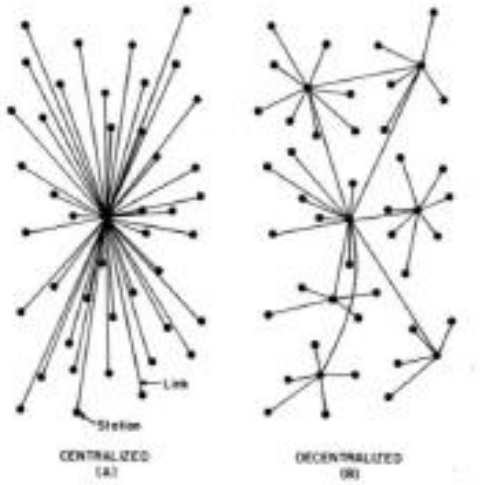


今日的互联网：一个从客户端--服务器的世界

来源：Client-Server Model , David Vignoni (2011)

30 年来，互联网的大规模普及，我们的数据架构主要还是基于客户端服务器。这意味着我们的数据集中存储在一台电脑上，并通过互联网使得另一台电脑能够检索到。即使我们生活在一个更加紧密相连的世界里，无论烤面包机还是冰箱都与互联网相连，数据仍然集中存储：在我们的设备上，u 盘里，甚至在云端。

这就引发了信任问题:我能信任那些存储我数据的人和机构吗？他们会保证我的数据不被破坏：不论内部还是外部，人为还是机器，故意还是意外吗？这样中心化的数据结构总有一个独特的故障点，好像我们从来没有发明过“互联”网。



中心化 vs 去中心化

改编自：On Distributed Communications; Introduction to distributed communications networks Paul Baran (1964)

从“数据专制”到“数据民主”

自上世纪 90 年代以来，P2P 数据架构就已经存在，它们以文件共享程序(如 BitTorrent 和 Tor browser)而声名鹊起。与密码学和博弈论的激励机制相结合，区块链将 P2P 架构提升到了一个新的高度。我们可以从集中式的数据结构，所有数据都存储在中央计算机上，转移到分散或完全分布式的数据架构。

数据君主制
服务器

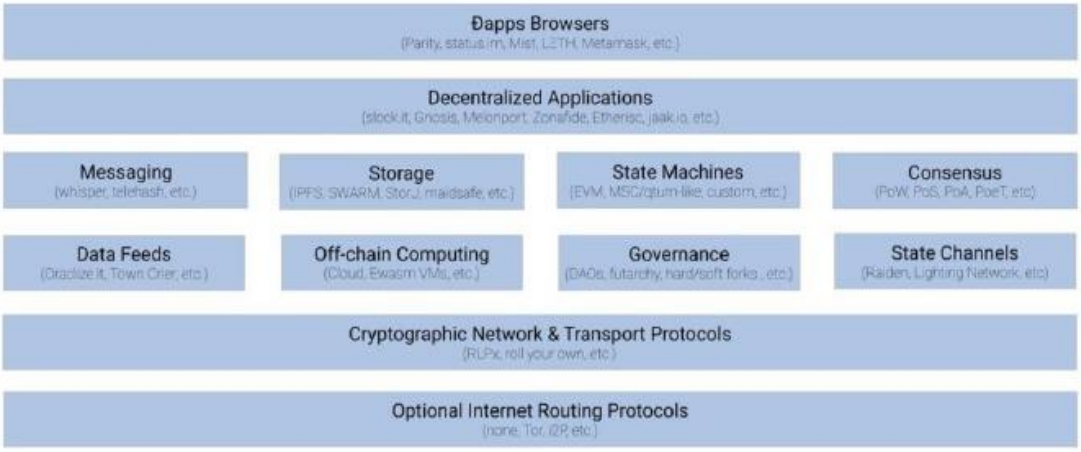
数据民主制
点对点网络

在 Web3 中，我们生活在一个连接的世界，并重新定义数据结构。需要注意的是，区块链只是这个去中心化网络中众多技术之一。虽然区块链是一种很好的 P2P 方式，可以记录谁在何时做了什么，但它并不适合存储大量的数据，原因有两点:(1)可拓展性:区块链速度太慢，(2)设计本身没有考虑隐私:永远不要将私人数据存储在区块链上。

Web3 技术栈

类似于构建一个标准的互联网或移动应用程序，创建一个 dApp（去中心化应用）需要这些准备:计算功能、文件存储功能、外部数据、货币化和支付功能。在过去的四年里，社区在生态系统建设方面取得了很大的进步。

虽然在 2014 年构建一个 dApp 不太可能，但在 2017 年构建一个基本的 dApp 是可行的，只需要最基本的计算和文件存储功能。Web3 生态系统经过多年已开发出一个开发人员可以构建的技术堆栈。这里列出了一些图示:

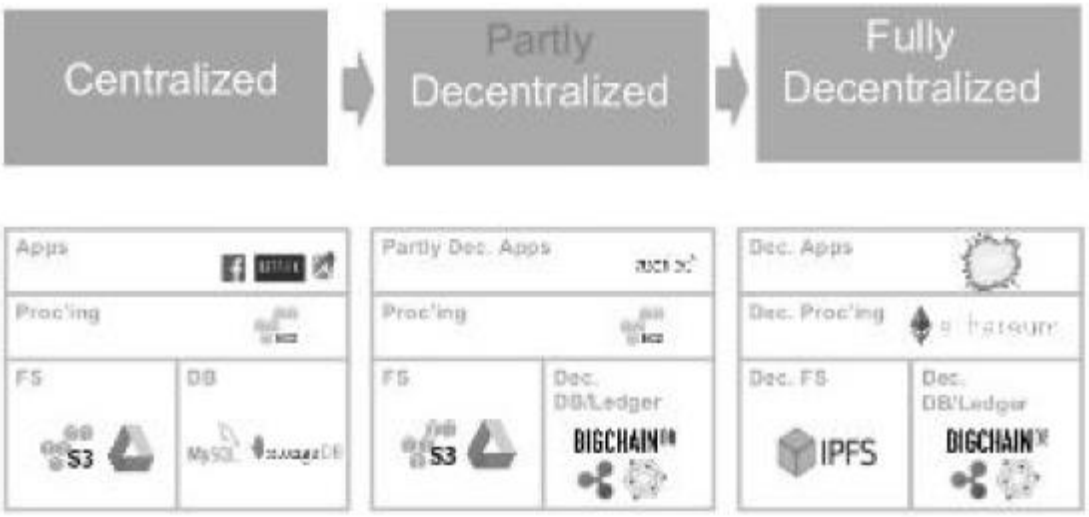


互联网 3.0 技术堆栈

来源：The Web 3.0 Abstracted Stack by Stephan Tual (2017)

从客户端--服务器互联网过渡到去中心化网络的过程是渐进的而不是激进的。随着去中心化网络堆栈逐渐成熟，从中心化到部分去中心化，再到完全去中心化。此外，很重要的一点是，虽然分散的体系结构更具有容错能力和抗攻击能力，但它们的速度也较慢。

虽然互联网的未来很可能是去中心化的，但这并不意味着我们将完全摆脱中心化的系统。中心化系统也有优势，并在特定的场景中可能更有优势。



去中心化云端

来源：Weaving the ILP Fabric into Bigchain DB , BigchainDB (2016)

引用和扩充阅读

ÐApps: What Web 3.0 Looks Like , Gavin Wood

Ethereum White Paper Bitcoin White Paper , Satoshi Nakamoto

The dApp Developer Stack: The Blockchain Industry Barometer , by Fred Ehrsam

Blockchain will usher in the era of decentralised computing , Bruce Pon, BigchainDB

Fat Protocols , Joel Monegro

The Shared Data Layer of The Blockchain Application Stack , Joel Monegro

Web 3.0 Revisited — Part One: “Across Chains and Across Protocols” , Stephane Tual

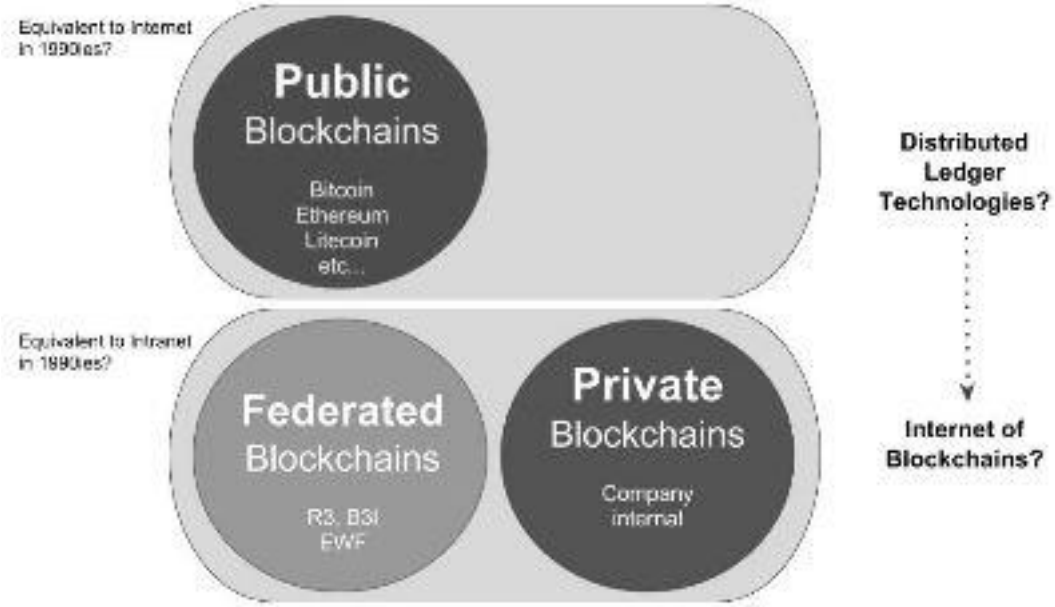
Blockchain Infrastructure Landscape: A First Principles Framing , Trent McConaghy

区块链种类

比特币白皮书于 2008 年由中本聪发布，第一个比特币于 2009 年被开采。由于比特币协议是开源的，任何人都可以使用协议、修改代码，并创造单独的点对点货币。所谓的山寨币便应运而生，它们试图超越比特币，成为更好、更快或更匿名的加密货币。很快代码的编写不仅运用于创建更好的加密货币，一些项目还试图将区块链技术拓展到点对点货币之外的领域。

比特币区块链实际上可以运用于任何一种价值交易或任何形式的协议，如 P2P 保险、P2P 能源交易、P2P 共享等。彩色币(coloredcoin)和万事达币（Mastercoin）试图通过比特币区块链协议解决这个问题。Ethereum 项目决定创建自己的区块链，以太币的属性与比特币非常不同，它将智能契约层与核心的区块链协议分离，成立了一种全新的方式来创建在线市场和交易，即智能合约。

像银行这样的私人机构意识到，他们可以运用区块链的核心思想，即分布式帐本技术(DLT)，创建一个许可区块链(私有化协作)，验证器是联盟中的成员或是相同组织的独立法人。然而，是否应将区块链一词用于许可的私人分布式账本仍然颇具争议，这也解释了为何分布式账本作为一个更通用的术语被更广泛地运用。



比特币种类

来源：Blockchainhub.net

私有链对于解决传统金融机构内部的效率、安全和欺诈问题颇具价值。但价值的累积并不意味它将彻底改变金融体系。而公有链更有可能用软件取代传统金融机构的多数职能，从根本上重塑金融体系的运作方式。

公有链

公有链是基于工作证明(PoW)共识算法的区块链协议，它是开源的，任何人都可以参加并无需验证。(1)任何人都可以下载该代码并开始在本地设备上运行公共节点，验证网络中的交易，从而参与共识过程——确定将哪些区块将被添加到链中以及当前区块链的状态。(2)世界上任何一个人都可以通过网络发送交易，并在通过验证后，被添加到区块链中。(3)任何人都可以读取公共区块上的交易，交易是透明和匿名的。

例如：比特币，以太坊，门罗币（Monero），达世币（Dash），莱特币（Litecoin），狗币（Dodgecoin ）等等。

作用：(1)拥有通过非中介化颠覆当前商业模式的潜力。(2)没有基础设施成本:不需要维护服务器或系统管理员，可以从根本上降低创建和运行去中心化程序(dApps)的成本。

联盟链

联盟链在一个组内运作。与公有链相反，他们不允许任何人进入互联网参与验证交易的过程。联盟链的速度更快(更高的可拓展性)，并保障了的交易隐私。联盟链大多用于银行业，共识过程由预先选定的节点集控制;例如，可以想象一个由 15 个金融机构组成的联盟，每个金融机构都有一个节点，其中 10 个必须在区块上签名才能使交易生效。阅读区块链的权利可能是公开的，也可以仅限于参与者。

例如:R3(银行)，EWF(能源)，B3i(保险)，Corda

作用:(1)降低交易成本和数据冗余，替代原来的系统，简化文档处理，消除半人工的合规机制。(2) 在这种意义上，它可以被看作是 1990 年代的 SAP:降低成本，但并非颠覆性。

注:有些人认为这样的系统并非区块链。此外，区块链还处于早期阶段，目前这项技术将被如何应用仍是未知。许多人认为,私有链和联盟链的命运将和 1990 年代的内联网类似，当私人企业建造自己的私人局域网或广域网,而非使用公共网络, 尤其是伴随着 Web2 SAAS 的出现，这些服务或多或少都将过时。

私有链

私有链的编写权限被集中到一个中央组织，读取权限可以是公共的，也可以限制在任意范围内。示例应用程序包括数据库管理、审计等，这些都是单个公司内部的，在很多情况下，公共可读性可能根本并无必要；而在其他情况下，共审计能力是需要的。私有链利用区块链技术，建立可以在内部验证交易的群组和参与者。相比于由博弈论激励机制保护的公共区块链，私有链更类似于一个中央集权的系统，并有安全漏洞的风险。然而，私有链也有自身的应用，特别是涉及到数据隐私和其他监管问题时，私有链更具可拓展性并易于验证合规。总之，私有链有一定的安全优势，也有一些安全漏洞(如上所述)。

例如:MONAX,Multichain

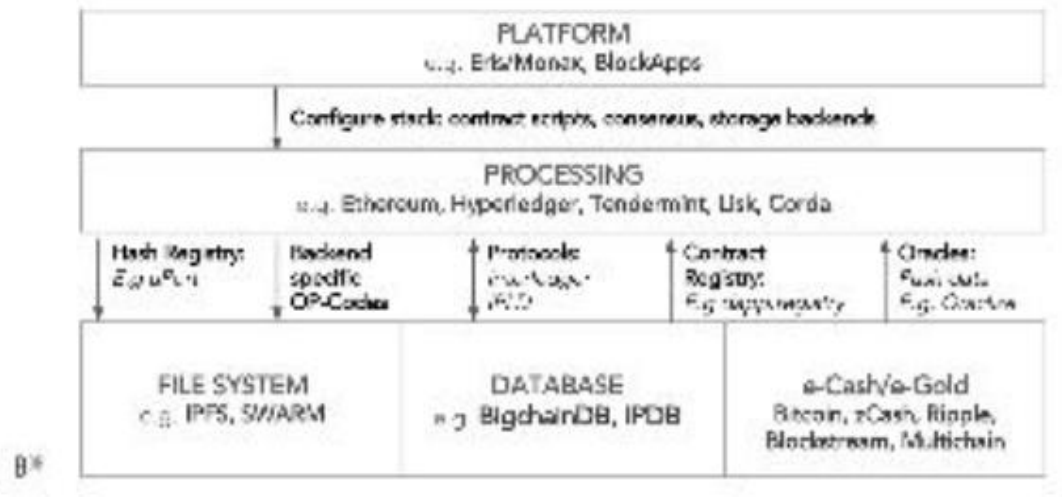
作用:(1)降低交易成本和数据冗余，替代原来的系统，简化文档处理，消除半人工的合规机制。(2) 在这种意义上，它可以被看作是 1990 年代的 SAP:降低成本，但并非颠覆性。

注:有些人认为这样的系统并非区块链。此外，区块链还处于早期阶段，目前这项技术将被如何应用仍是未知。许多人认为,私有链和联盟链的命运将和 1990 年代的内联网类似，当私人企业建造自己的私人局域网或广域网,而非使用公共网络, 尤其是伴随着 Web2 SAAS 的出现，这些服务或多或少都将过时。

区块链数据库：案例-巨链数据库（BigchainDB）

最先进的区块链目前也存在可拓展性的问题，这意味着网络只能每秒只能处理少量交易，这使得它们无法适用于具有高交易量的大型应用程序。比特币和以太币每秒只能处理少于十几笔交易，但单是 Visa 就需要在高峰时段每秒完成高达十万笔的交易。巨链数据库将分布式数据库的可扩展性能力与区块链的不可变元素结合在一起，以解决数据库限制的问题。

有些人会质疑将巨链数据库称为区块链，但它是分布式计算技术栈中的一项重要技术，解决了可扩展性的重要问题。我们正在重新设计 Web3 的数据结构,从中央集权计算转变为分布式计算和分布式网络。在这样的背景下，巨链数据库是Web3 技术栈中的一个重要元素(见下图)。



分散堆栈的互操作性

来源： n.d., BigchainDB (2016)

不同分类标准

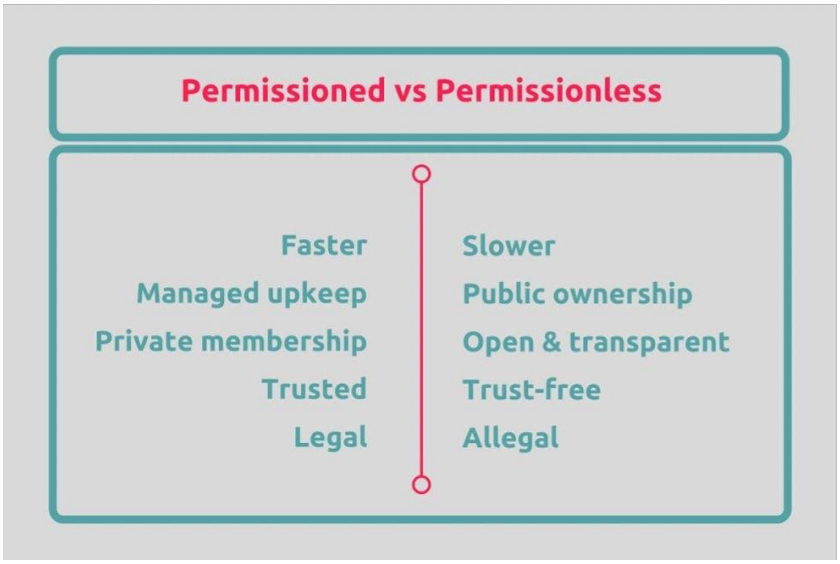
许多人试图对区块链进行分类，但对于如何准确区分不同类型的区块链，并没有达成共识，下图列出了不同的分类方案。

	公有链	私有链
权限	读取和编写权限开放	读取和编写权限需经许可
速度	慢	快
安全	工作证明、权益证明、其他共识方法	事先批准的参与者
身份	匿名，笔名	身份可知
资产	原始资产	任何资产

公有链 vs 私有链

来源： Chris Skinner's Blog

区分区块链的一种方式是按照公有和私有，或需要许可和无需许可。有时这些术语是同义的，但它们其实指的是不同的东西。



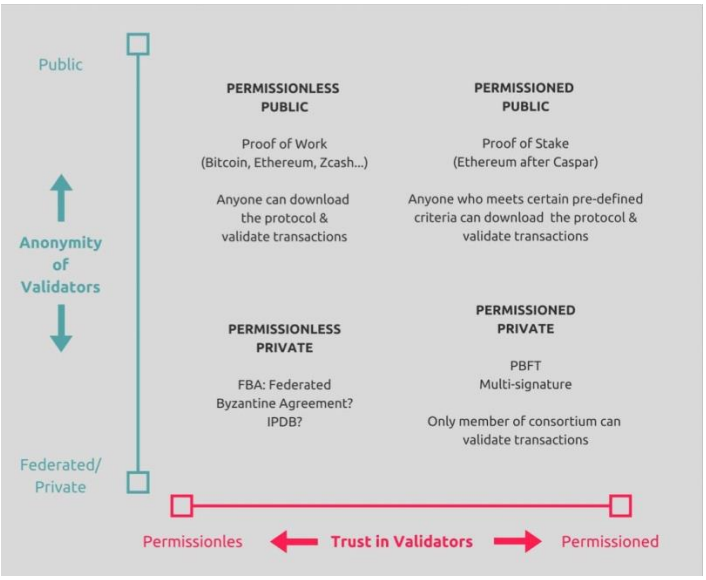
许可 vs 未经许可

快	慢
管理维护	公共所有
私有	开源和透明
可信	无须信任
合法	无法约束

来源：Gavin Wood (2016)

比特币区块链是颠覆性的，因为它是公开和无需许可的。世界上任何一个人都可以下载开源代码，并通过一个名为挖矿的概念，开始验证交易，并获得比特币的奖励。

比特币网络的所有利益相关者并不认识和信任彼此，但却通过点对点网络的共识，在协议和自动执行的经济激励框架中相互协调。因此，区块链协议中的智能合约为所有网络参与者提供了一个协调框架，无需传统的法律合同。在私有和许可的区块链中，所有参与验证交易的网络参与者身份都是可知的。信任框架由双边或多边法律协议提供，而非代码。



无需许可的公有链 工作证明 （比特币、以太币，Zcash…） 任何人可以下载合约并验证交易	**许可的公有链** 权益证明 （Caspar 后的以太币） 任何符合事先约定条件的人可以下载合约并验证交易
无需许可的私有链 联邦拜占庭协议 星际数据库	**许可的私有链** 实用拜占庭容错算法 多人签名 只有联盟成员可以验证交易

我需要哪种区块链呢?

改编自 Pavel Kravchenko (2016)

	公有链	联盟链	私有链
参与者	无需验证 -匿名 -可能是恶意的	需要验证 -可识别 -可信	需要验证 -可识别 -可信
共识机制	工作证明、权益证明等 -大能耗 -结果最终性无法保证 -51%攻击	投票或多边共识机制 -更轻 -更快 -更少能耗 -结果最终性可以保证	投票或多边共识机制 -更轻 -更快 -更少能耗 -结果最终性可以保证
交易验证频率	长 比特币：10 分钟及以上	短 100 微秒	短 100 微秒
USP	颠覆性 颠覆性表现在去中介化；尚不清楚商业模式应用	节约成本 可以减少大量交易成本；类似于 1990 年代的 SAP；减少数据冗余，更多交易频率，更加透明化	节约成本 可以减少大量交易成本；类似于 1990 年代的 SAP；减少数据冗余，更多交易频率，更加透明化

改编自：Slideshare

引用和扩充阅读

On Public and Private Blockchains , Vitalik Buterin (2015)

Vitalik Buterin: On Public and Private Blockchains , Coindesk

Ok, I need a blockchain, but which one? , Pavel Kravchenko

IBM blockchain explained , Diego Alberto Tamayo

Blockchains What & Why , Gavin Wood

密码经济

密码经济学是指在对抗环境中对经济行为的研究。潜在的挑战是，在分散的 P2P 系统中，不把控制权交给任何中央集权方，人们就会假定有不守规则的参与者试图破坏系统。密码经济方法结合了密码学和经济学，建立了强大的分布式 P2P 网络，尽管对手试图破坏它们，但这种网络仍能持续发展。这些系统背后的密码学是使得网络中的P2P通信安全的原因，而经济学会激励所有参与者对网络做出贡献，这样它就会随着时间的推移不断发展。

在比特币出现之前，人们普遍认为不可能在 P2P 网络节点中实现容错和攻击一致性(Byzantine General’s Problem)。中本聪为 P2P 网络引入了经济激励措施，并在 2008 年发布的比特币白皮书中解决了这一问题。虽然基于密码学的分散 P2P 系统并不是什么新鲜事，但在比特币之前，这些 P2P 系统缺乏的是经济激励层以协调众多参与者。中本聪引入的一项工作证明(POW)机制将区块链带入了一个新的经济协调博弈领域，现在被称为密码经济学。

P2P 网络中的机器共识

分布式计算的一个基本问题是，如何在错误和潜在风险共存的情况下，实现整个系统的可靠性。这通常要求参与者在计算过程中对某些数据值达成一致。协商一致需要在多个网络参与者之间达成一个单一数据值的协议。某些过程可能出错，因此共识协议必须是容错并能抵抗攻击和串通的

❑ 容错

分散的系统不太可能失败，因为它们依赖于许多独立的部分。

❑ 抗攻击

破坏分散的系统的代价更大，因为它们缺乏敏感的中心点，后者的攻击成本比整改系统的经济代价低得多。

❑ 防止串通

在分散的系统中，参与者很难串通一气，以牺牲其他参与者的利益为代价行事，而企业和政府的领导方式却能让他们自己受益，但却不会伤害到那些配合的公民、顾客、员工和公众。

经济共识原则

在一个密码经济体制中，经济激励被设计成容错、抵抗攻击和串通的。这些经济刺激围绕着加密代币，代币被认为是最小公约数，在一个众多利益相关者的网络中协调利益。比特币就是将利益相关者的利益与经济激励联系在一起的例子。

当中本聪将比特币的代币规则与激励机制捆绑在一起时，其他的区块链也尝试了其他的共识机制。如下列出的就是一些共识机制。需要注意的是，密码经济学领域是一个全新的领域，随着时间的推移，我们很可能会看到更多的共识机制。

工作量证明(PoW):比特币区块链使用电力来保证系统的安全。它创造了一个经济系统，人们必须承担成本——提供工作证明才能参与。参与者为了得到回报——比特币。如果参与者花钱，按规矩办事，就会得到钱；如果作弊就会赔钱。共识机制使作弊得不偿失，而这种简单的博弈理论是比特币共识算法的核心。目前，比特币协议大部分都是该协议的软件分支，通常是对工作证明算法进行微小的改动。一些人认为，比特币目前的共识机制更多的是一种委托的工作证明，而不是中本聪设计的纯粹工作证明，因为大多数的矿商已经形成了以采矿池为形式的寡头。

历史:工作证明是一种经济措施，它通过要求参与者付出某些工作量(通常指计算机处理时间)来阻止对服务攻击和其他服务的滥用，比如网络上的垃圾邮件。这一概念最早可能是由 Cynthia Dwork 和 Moni Naor 在 1993 年的期刊上提出。“工作证明”一词最早是在 1999 年由 Markus Jakobsson 和 Ari Juels 提出的。这些方案的一个关键特性是它们的不对称:工作对于请求方而言，需要付出适度的努力(但可行)，但对服务提供者而言，则很容易检查。这个概念也被称为 CPU 成本函数、客户端谜题、计算谜题或 CPU 价格函数。

权益证明(PoS):这是一种替代方法，通过这种方法，加密货币区块链网络的目标是实现分布式协商一致。当工作证明方法要求用户重复运行散列算法或其他客户端难题时，为了验证电子交易，权益证明要求用户证明其拥有一定数量的货币 (他们在货币中的权益)。Peercoin 是首个使用权益证明的加密货币。其他案例包括 BitShares, Nxt, BlackCoin, NuShares/NuBits 和 Qora。以太坊计划从工作证明过渡到权益证明。Decred 将工作证明

与权益证明混合，并结合两者的元素，试图获得两个系统的好处，并创建一个更完美的共识概念。对于工作证明，挖掘一个区块的概率取决于挖掘人员所做的工作(例如，CPU/GPU 周期用于检查散列)。在比特币的例子中，有证据表明，比特币是一名矿工持有的比特币数量——持有 1%比特币的人可以获得 1%的“股权证明”。用户必须证明他们拥有一定数量的加密货币来生成一个块，而不是牺牲掉一个块的能量。赌注越高，就越有可能产生一个区块。理论上，这会阻止用户创建分支，因为这会使他们的股份贬值。权益证明听起来是个好主意，但讽刺的是仍存在“缺乏利害关系”（nothing at stake）的问题。因为开采比特币代价昂贵，所以把精力浪费在一个不会赚到钱的分叉上是不明智的，但是有了权益证明，参与者就可以自由挖矿。

委托权益证明:委托权益证明使用信誉系统和实时投票来达成共识。具体而言，就是建立一个受信的小组，所有成员都有资格创建区块，并阻止不受信任的各方参与。受委托人负责创建区块，但无法更改交易细节。但是这可以防止特定的交易被包含在下一个区块中。信任在这里至关重要，值得注意的是，如果下一个区块中没有交易——或是未能创建区块——将意味着之后的一个区块将是它的两倍大小。在某种程度上，这可以防止在指定的时间段内出于恶意而阻止交易或创建区块。这些行为只是稍微延迟了交易，但从长远来看似乎不可能阻止创建。任何出于恶意行事的人都会最终暴露。具有委托权益证明能力的社区成员可以投票决定将其作为一名受委托人废除。在委托权益证明规则下作弊不仅是不可能的，而且也不符合任何人最佳利益的。在整个网络中，受委托人的数量或多或少，需要记住的是这个数量是可以改变的。

锁定（燃烧）证明:“这是一个分布式共识并替代工作证明和权益证明的方法。它还可以从另一个加密货币中引导到另一个加密货币。他们的想法是，矿商应该拿出证据，证明他们锁定（燃烧）了一些货币——也就是说，把它们送到一个可核实的无法使用的地址。从个人的角度来看，这很昂贵，就像工作证明一样;但它除了消耗基础资产以外，没有消耗其他资源。到目前为止，所有的证据都是通过锁定（燃烧）证明的加密货币来证明的，因此稀缺的最终来源仍然是被开采的燃料”(Bitcoin Wiki)

权威证明：权威证明是在私有链上的一个共识机制，它给一个客户(或特定数量的客户)一个特定的私钥，来检查所有的区块。

升级/改变共识规则

区块链协议是一种强大的工具，可以在去中心化的分布式网络中自动执行预定义的共识规则。网络成员知道透明和开源的规则集，可以随时选择进出。只要协议不被修改，区块链协议就是强大的治理工具。

随着时间的推移和环境的变化，可能需要对系统进行升级。这些升级需要网络中所有利益相关者的多数共识。虽然协议可以通过硬分叉或软分叉进行升级，但是这些分叉可能会引起很大的争议，就像我们在 Bitcoin 总量和以太坊硬分叉的辩论中看到的那样 。

举例:在比特币网络中，开发人员对比特币提出的改进建议以及 Github,Bitcointalk,Reddit,邮件中的讨论等。这个层面的讨论是至关重要的,以确保平稳过渡到共识，可实施的改进建议将在测试网上进行测试。在成功测试后，开发人员将这些更改应用到比特币软件中。谁在协商一致过程中有发言权?(1)软件开发人员(实现);(2)矿商(矿业区块运行共识);(3)交易所(验证交易的节点);(4)钱包公司(在节点上创建交易);(5)商户(商户处理也通过节点)。

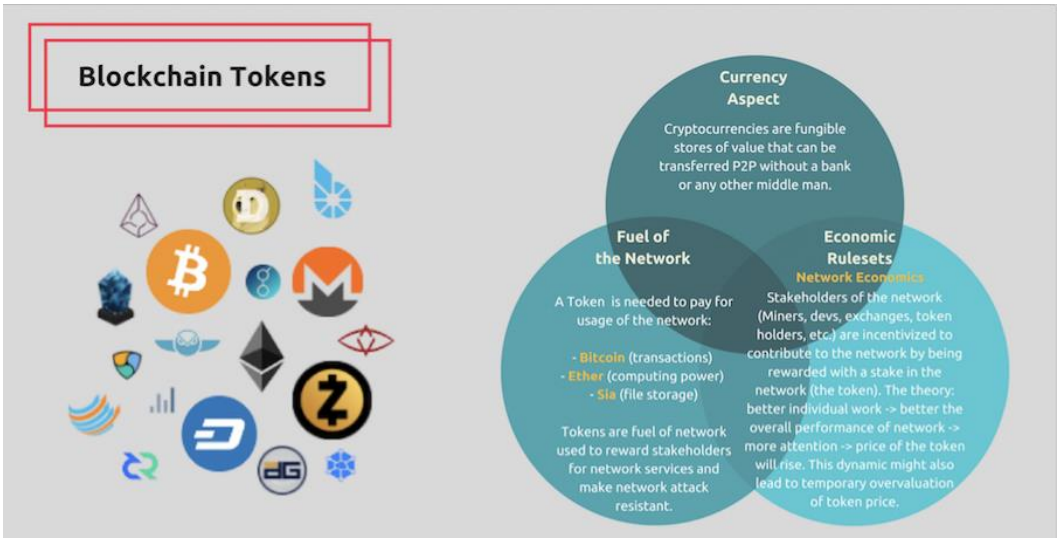
引用和扩充阅读

- Cryptoeconomics 101 , Nick Tomaino
- The meaning of Decentraization , Vitalik Buterin
- Understanding Crypto-Economic Security through Game Theory , Delegated Proof of Stake , Bitshares
- Fat Protocols, Joel Menegro
- Tokens, Tokens and More Tokens, Nick Tomaino
- Crypto Tokens and the Coming Age of Protocol Innovation, Albert Wenger
- Crypto Tokens: A Breakthrough in Open Network Design , podcast with Vitalik Buterin, podcast with Olaf Carlson-Wee
- Regulatory discussions , Coincenter
- A gentle Introduction to Digital Tokens

代币

像比特币或以太币这样的最先进的、公开的、无需验证的区块链，鼓励原来不认识或不信任彼此的不同群体围绕着一个特定的区块链进行交易活动。比特币网络的代币也被称为比特币，它基于密码学的经济激励机制，这样的机制可以判定哪些交易是有效的，并创建新的区块。

基于密码学代币，“分布式互联网部落”应运而生。与传统的公司拥有多层管理结构(官僚式协调)不同,区块链颠覆了自上而下的治理结构，成立了去中心化的自治组织(DAOs),将人们聚集起来的不是一个法律实体和正式合同,而是加密代币(激励)和完全透明的软件规则。



区块链代币

来源：Blockchainhub.net

货币：加密货币是客户还的价值储存工具，并能无银行和中间商的情况下进行点对点的交易

网络：使用网络需要支付代币

1. 比特币（交易）
2. 以太币（编程能力）
3. Sia（文件存储）

所有者提供网络服务并使网络更加安全，获得代币奖励。

经济准则：网络经济学

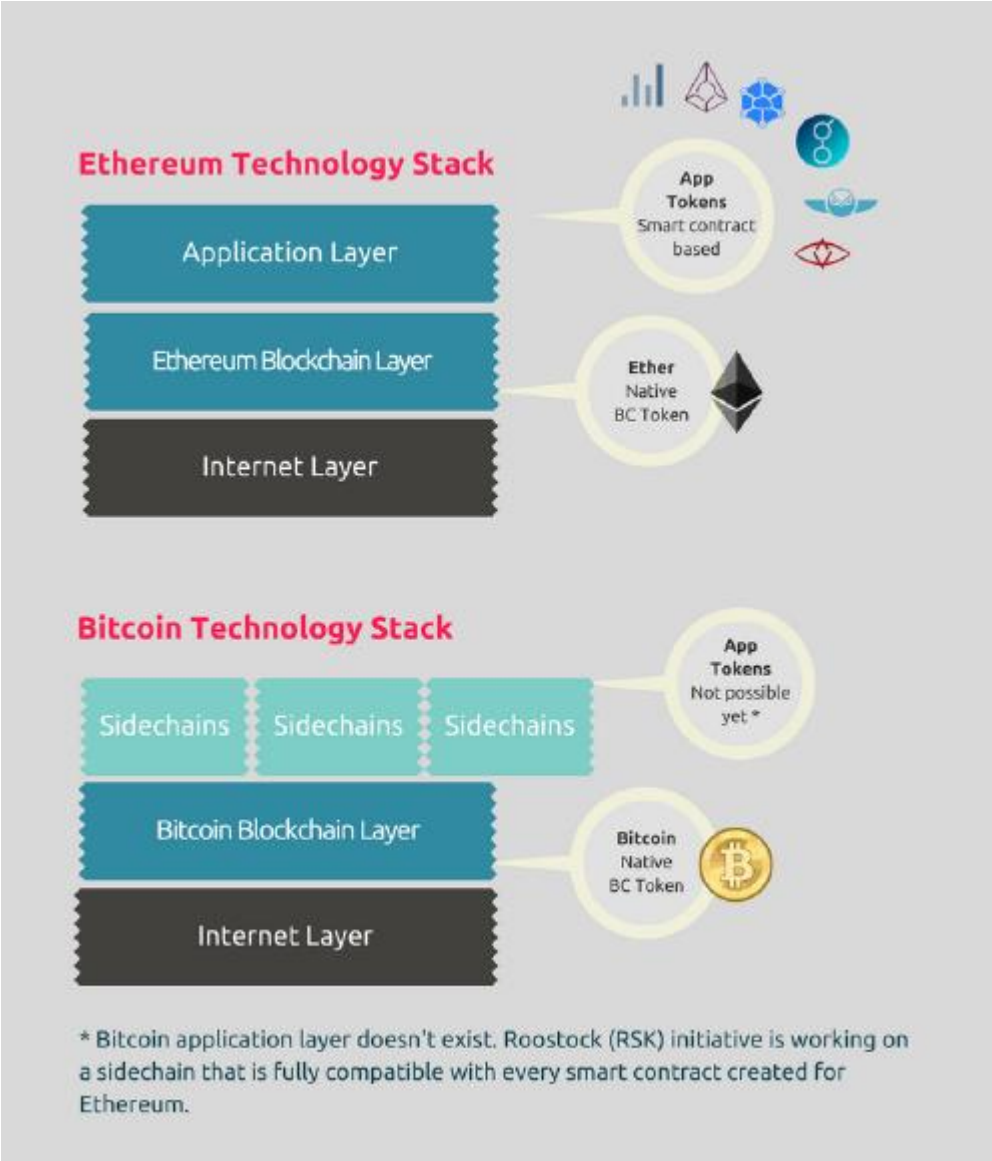
网络中的参与者（矿工，开发者，交易者，拥有者等）由于获得奖励而参与网络活动。理论：更好的个人工作-> 更好的整体表现-> 更强吸引力-> 代币价格上涨。这样的机制

也可能导致货币价格暂时被高估。

比特币网络可以被视为第一个真正的去中心化组织，在无银行和银行经理的条件下为资金流通提供了渠道。自 2009 年第一个区块创建以来，比特币网络保持着抗攻击和容错能力，没有一个中央实体能完全控制比特币。从理论上讲，只有全球范围的停电才能关闭比特币。

然而，随着以太坊的出现，代币在技术堆栈层面上升，现在可以在应用层上开发去中心化代币。在以太坊区块链上的智能契约可以创建带有复杂功能的代币。今天，代币的概念仍对大多数与区块链技术发展息息相关的社会经济创新颇为重要。

只有许可的账本(类似比特币或以太坊这样的公共区块链)，需要某种激励机制来保证区块的验证者按照预先定义的规则去执行任务。在需要验证的(联盟／私有链)分布式总帐系统中,验证者和区块创造者可能出于不同的原因完成他们的工作：如果他们存在这样的义务。在需要验证的环境中，验证者只能是联盟中的成员，并且验证是手动和集中控制的。因此，许可的账本不需要一个代币，另一点值得注意的是，区块链这个术语在这样的账本中是存在争议的。



代币的等级

来源： Blockchainhub.net

代币种类

可以用不同的方法来区分代币，下面概述了其中的一些。由于代币经济学是一门新的学科，我们仍然处于探索不同角色和代币种类的早期阶段。对于每一个新的区块链和每一个新的应用程序层，我们将通过尝试并从错误中学习哪些是有效的，哪些无效。

❑用户代币: 用户代币是需要使用服务时使用的代币。比特币和以太币是用户代币最好例子——代币所有权不会给你在网络中的任何专业权利，但它能让你访问服务(对于比特币和以太币，就是比特币支付网络和以太网虚拟机)。稀有的代币和有用的服务可以为代币持有人和企业家创造巨大的价值。

❑工作代币:工作代币给予用户权利来参加去中心化组织的工作 (无论是区块链还是智能合约)并且靠工作赚取收入。这项工作可以是类似自动计算机(例如 Augur)，也可以是作为抵押债务系统(例如 Maker)的后盾，或者是确保网络安全(例如以太坊中的权益证明)。

这两种类型的代币不是互斥的，而且一些代币可以同时使用:用户代币和工作代币。一个具有两者特征的代币就是以太币，当以太坊从工作证明过渡到权益证明的时候。另一种区分代币的方法是:

❑内在、本地或内置的代币:类似比特币,以太币等作为:(a)区块验证激励(矿工奖励);(b)预防交易垃圾。这背后的逻辑是如果所有的交易都会被支付，那么它就限制了滥发交易信息的能力。

❑应用代币:有了以太坊，代币现在可以很容易地通过以太坊区块链智能合约发布在应用程序层上，这也就是所谓的复杂去中心化应用代币或复杂 DAO 代币。

❑资产证明代币: 资产证明代币是由一方发行的用于后期兑现的代币。它们是相当于实物资产的数字资产。它们对标的资产(如黄金)有索取权，持有者需要向特定的发行人(金匠)提出索求。交易时，代币在人们之间传递并被记录在区块链中。如需索取标的物，你需要把代币发给发行方，而发行方会向你发送标的资产。

代币可以代表资产	代币可以被用作
❑屋顶太阳能的一个小时	❑所有权的代表
❑货币如美元、欧元、卢比,或英镑	❑凭证
❑众筹承诺的产品	❑软件许可证
❑未来下载你最喜欢的艺术家的歌曲	❑股票证书
❑保险政策	❑访问租车或其他车辆

❑ 奥运门票	❑ 门票,访问权限 ❑ 会员,订阅 ❑ 奖励计划 ❑ 金融工具 ❑ 系统中的投票权

法律地位

区块链代币体现了区块链技术的全部潜力，为了让区块链充分发挥其在数字领域的潜力，即重新定义所有权，这项技术需要被认可为一个能够创造客观事物的系统。作为一种新的发明，它应该有它自己的监管框架来反映区块链技术的独特的功能和限制。

引用和扩充阅读

Crypto Economics , BlockchainHub

A Blockchain Token Taxonomy, Florian Glatz

Thoughts on Tokens, Balaji S. Srinivasan

ICOs and VCs here , Fred Wilson

Fat Protocols, Joel Menegro

Cryptoeconomics 101 , Nick Tomaino

Tokens, Tokens and More Tokens, Nick Tomaino

Crypto Tokens and the Coming Age of Protocol Innovation, Albert Wenger

Crypto Tokens: A Breakthrough in Open Network Design , podcast with Vitalik Buterin, podcast with Olaf Carlson-Wee

Regulatory discussions, Coincenter

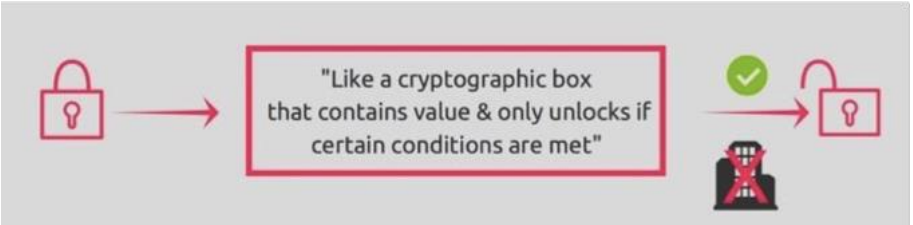
A gentle Introduction to Digital Tokens , Bitasonblocks

Tokens on Ethereum, Consensys

智能合约

智能合约是一种运行在区块链之上的计算机代码，它包含一组规则，其中智能契约的

双方同意进行交易。如果预先定义的规则得到满足，协议将自动执行。智能合约促进、验证和执行协议和交易，体现了最简洁的去中心化和自动化。这种机制涉及数字资产和两个及以上的交易方,在当事人完成存款执行智能合同后，资产将基于公式和数据计算自动在交易方之间分配，分配的结构在缔结合约时并不可知。



“好似一个密码箱，里面存储了价值并且只有在满足特定条件下才能打开。”

来源：Blockchainhub.net

智能合约这个词其实不是那么贴切，因为智能合约既不智能，也不同于法律合同:

❑智能合同的智能程度取决于编码者在编码时考虑到的所有情况

❑智能合同在一定条件下可以变成法律合同,但这不应与法院的法律合同或具有法律效力的执法合同相混淆。然而，随着技术变得更加成熟和广泛应用， 我们很可能会看到未来几年看到法律合同和智能合同的组合。

降低交易成本

你会和你素未谋面的人签订合同吗?你愿意借钱给埃塞俄比亚的农民吗?你会成为一个在战区的少数民族报纸的投资者吗?你会不会为了在网上购买5美元的合同而去写一份具有法律约束力的合同呢?对于大多数人来说，答案是否定的，因为这些例子的交易成本超过了转移的价值。

智能合约这个术语延续了区块链，并于1996年由Nick Szabo首次提出。其目的是为了提供优于传统合同法的安全性，并减少与合同相关的其他交易成本。可强制执行的代码——无论是在协议级别上还是在应用程序级别上——构成了标准化交易的规则，从而降低了交易成本:

❑达成共识

❑创造协议

❑执行协议

一份智能合约可以使人们、机构和他们拥有的资产形式化。智能合同的交易规则(协议)定义了各方需同意的条件——界定了权利和义务。它通常是预先定义的，并且通过简单的选择来达成协议。这个交易规则集以数字形式，以机器可读的代码形式进行了形式化。这些权利和义务在智能合同中得以确立，一旦双方达成协议并满足协议的条件(执行)，计算机网络将自动执行。

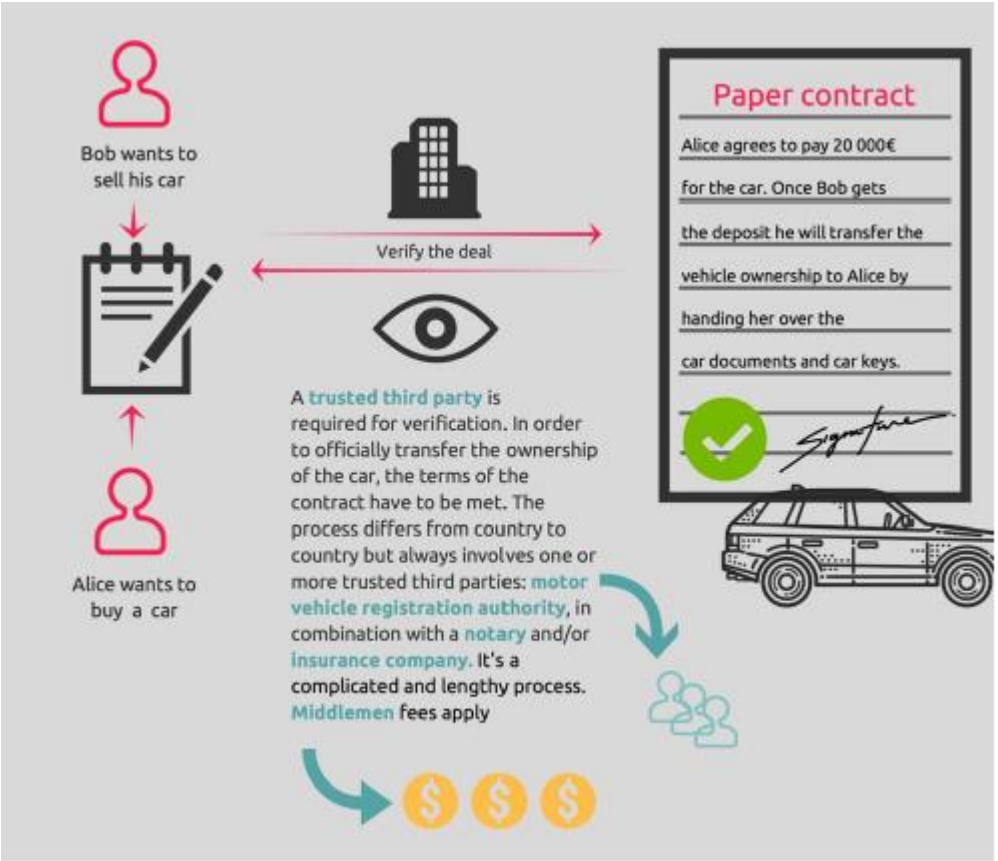
虽然智能合约的概念并不新鲜，区块链技术似乎是智能合同实现的催化剂。智能合同最原始的形式是自动售货机。交易的规则被编程，你选择一个产品，按一个与那个产品相关的数字，投入硬币，机器像智能合约一样，检查你是否投入足够的钱。如果是，机器会给你相应的产品，如果你投入太多的钱，它也会退回找零。如果你没有投入足够的钱，或者机器没钱了，你就会找回你的零钱。自动贩卖机减少了交易成本，供应商变得过时，而且自动贩卖机还扩展了服务，提供24/7全天候的服务，不止是有限的开放时间。

智能合约是	智能合约可以
❑自动验证的 ❑自动执行的 ❑防止干预的	❑将法律操作自动化 ❑保证更安全 ❑减少对第三方的依赖 ❑降低交易成本

智能合同能够实时跟踪性能，并能节省大量成本。服从和控制同时发生 。为了获得外部信息，一份智能合同需要信息输入，它通过外部信息来满足智能合同的需求，从而触发交易。

智能合约举例

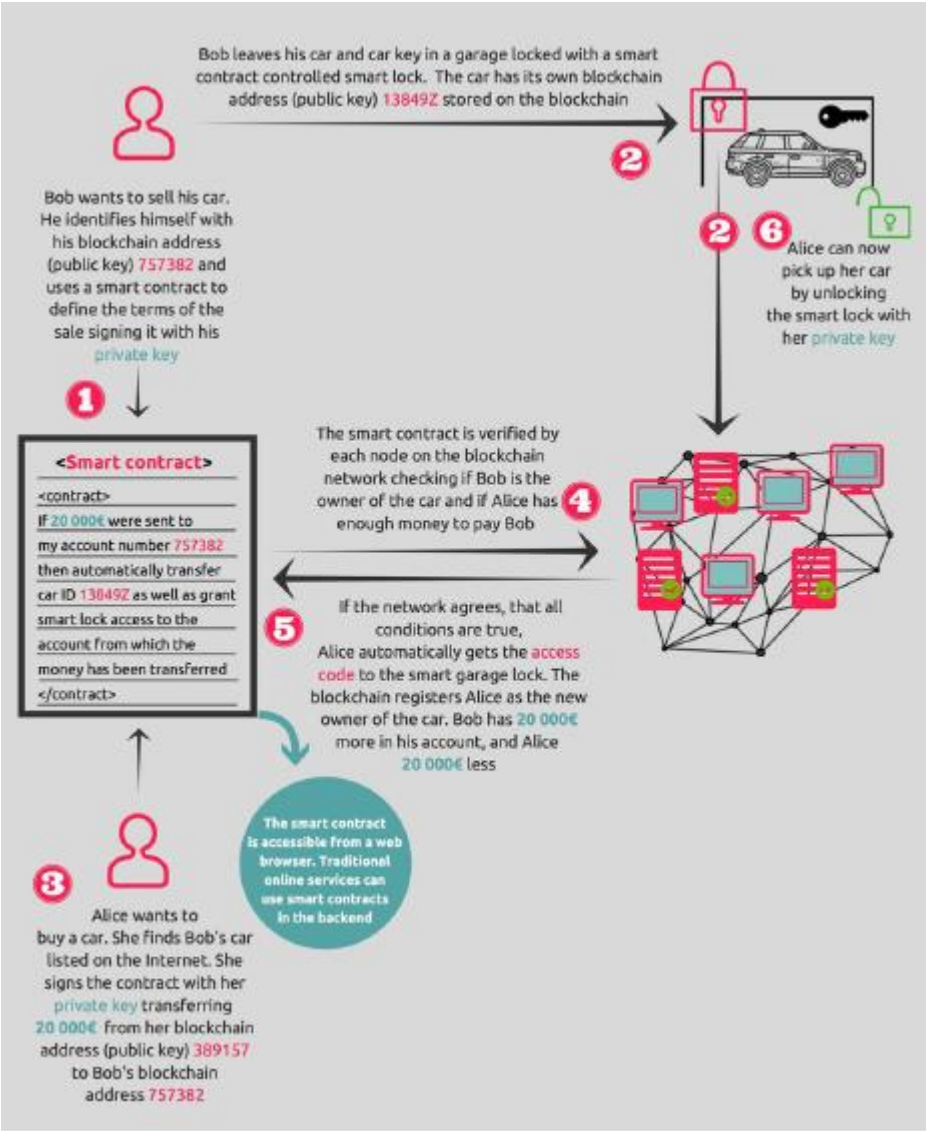
如果A和B不知道并且互不信任，他们通常需要一个可信的第三方作为中介来验证交易并执行。有了智能合同和区块链，你就不再需要那些中介来清算或结算你的交易。以购买和销售汽车为例：如果Alice想从Bob那里购买一辆汽车，需要受信任的第三方来验证和验证交易。这个过程取决于不同国家，但至少包括一个，通常更多的第三方:机动车登记管理局，与公证处、保险公司。这是一个复杂而漫长的过程，对于这些中间人来说，也可收取相当可观的费用。



目前买车的过程

来源： Blockchainhub.net

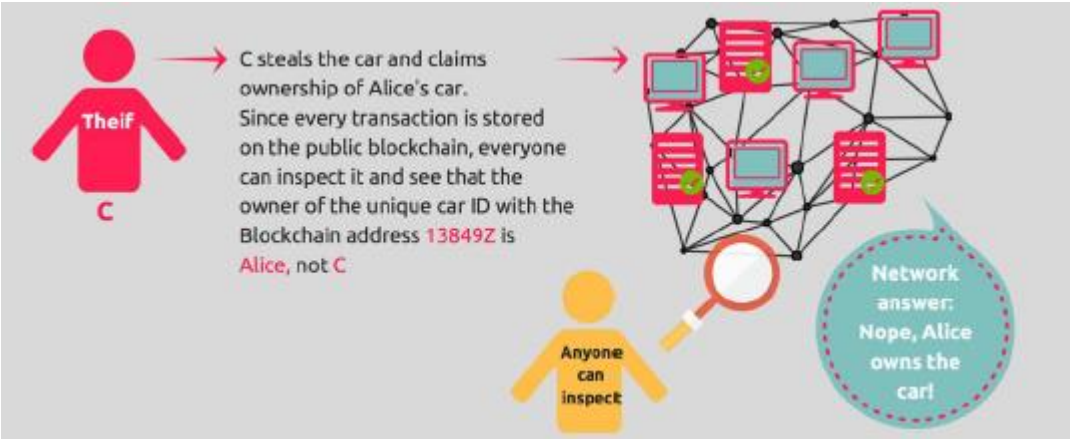
一旦所有相关部门和公司都参与区块链，一个智能合约可以用来定义销售产品的所有规则。如果Alice想用区块链上的智能合约从Bob那里购买汽车，那么区块链网络中的每个节点都将验证该交易，看看Bob是否为汽车的所有者，Alice是否有足够的钱支付Bob。



通过区块链买车的过程

来源：Blockchainhub.net

如果网络验证这两个条件都复核，Alice就会自动获得获取车库智能锁的访问代码，区块链也会将Alice登记为汽车的新主人。Bob 在他的账户上有多于€20000,爱丽丝少于€20000。这个过程不需要中间人。在区块链，谁拥有什么是透明的，以匿名或假名的形式呈现。这意味着运行区块链协议的每一台计算机都可以检查某一个人是否是这辆车的合法主人。偷车不会像今天这样容易，特别是一旦我们有了在区块链上验证的智能密码，未来就可以解锁我们的车辆。作为汽车的拥有者，你可以授权其他人驾驶它(展示个人的公钥)。在这种情况下，只有在区块链上使用智能密码才能发动汽车。



我们可以信任区块链

来源：Blockchainhub.net

智能合约种类

区块链和智能合同可能为许多行业带来变革。比如可以应用于银行、保险、能源、电子政府、电信、音乐和电影工业、艺术界、通行、教育等领域。智能合约的应用从简单到复杂都包含。

简单应用的例子包括像归属(艺术注册)、政府和半政府注册(土地名称，出生证明，出生证明，学校和大学学位)。另一方面，去中心化的自治组织是最复杂的一种契约形式。2016年的DAO就是这样一个复杂智能合约的例子。

鉴于区块链仍然是一个新技术,有些行业采用智能合约会稍晚,特别是受到政府严密监管或是需要网络效应的领域——例如供应链的技术采用和标准化等等。一般来说,可以先在较小的、不太复杂的实验项目上积累经验，更好地理解技术后，在稍后的阶段转移到更复杂的用例上。

智能合约编程

Solidity是一种智能的契约编程语言。它的语法与JavaScript类似，它的设计目的是为Ethereum虚拟机编写代码，为投票、众筹、盲目拍卖、多签名钱包等创建契约。

Official Solidity Documentation, Ethereum Foundation
Solidity Tutorial , using Visual Studio
Solidity Code Snippets, useful for Đapp development
Accessing Contracts & Transactions : Interacting with smart contracts
Integrated development platform (IDE) browser based with integrated compiler and solidity runtime environment without server-side components
Ethereum Solidity Gitter chat channel Remix : IDE that allows developers to build and deploy contracts and decentralized applications on top of the Ethereum blockchain
The Hitchhiker’s Guide to Smart Contracts in Ethereum , Manuel Aráoz, Medium
Truffle : The most popular Ethereum development framework, Github

引用和扩充阅读

Nick Szabo, Smart Contracts
Check out our Smart Contract Infographic
Internet of Agreements: Building the Hyperconnected Future on Blockchains - why smart contracts could change the way people do business: by Hexayurt.Capital in collaboration with ConsenSys
Smart Contracts , Florian Glatz OpenLaw , Consensys

Oracles

在区块链和智能合约应用中，Oracle是一种代理软件，它能够接收并验证来自现实世界的信息，并将这些信息提交给智能合约使用的区块链。

有的智能合约包含一定的数值，只有在某些事先定义好的条件得到满足的情况下才能解锁该数值。当数值达到某一个临界点，智能合约就会改变其状态并以程序的形式执行预定义的算法，进而自动触发区块链上的事件。Oracle的主要任务是以安全可信的方式将这些数值提供给智能合约。

区块链不能访问区块链网络之外的数据。Oracle是第三方提供的数据服务，被设计用于区块链上的智能合约，它提供外部数据并在预定义的条件满足时触发智能合约执行。这些预定义的条件可能基于任何数据：天气温度、支付成功、价格波动等。

Oracle是多重签名合约的一部分。例如：原始受托人签订合约，约定在特定条件下未来会释放相应的资金。在任何资金释放之前，Oracle都必须签署智能合约。

Oracle种类

基于使用类型不同，有多种不同的Oracle，可以分为如下几类：软件Oracle、硬件Oracle、共识Oracle、内向Oracle和外向Oracle。

❑ 软件 Oracle

软件Oracle能够处理网上的信息。例如温度、商品的价格、火车或飞机的延迟时间等等。这些数据来源于网络，如公司网站。软件Oracle从各种数据源提取这些信息并把信息推送给智能合约。

❑ 硬件 Oracle

硬件 Oracle 需要直接从现实世界传入的信息。例如：当一辆车穿过障碍，运动传感器能够检测到这辆车，并把这一数据发送给智能合约。另一个使用场景是供应链产业中

的射频识别。硬件 Oracle 最大的挑战是如何在不牺牲数据安全的条件下保证数据传输。针对数据安全风险，Oraclize 提出了一个两步解决方案，通过提供传感器读数的加密证据和防篡改机制，保证入侵者无法操纵设备。

❑ 内向 Oracle

内向 Oracle 能够把外界的数据提供给智能合约。例如：当美元(USD)到达指定价格，自动触发买单。

❑ 外向 Oracle

外向 Oracle 使得智能合约能够向外界发送数据。例如：与区块链相连接的智能锁，在接收到向自身区块链地址的支付时自动开锁。

❑基于共识的 Oracle

预测市场（例如 Augur 和 Gnosis）高度依赖 Oracle 来确认未来事件结果。使用单一数据源风险高且不可靠。为了防止有人操纵市场，预测市场通常会开发一个 Oracle 的打分系统。为了进一步确保安全性，通常会使用 3-5 个 Oracle，这些 Oracle 数据共同决定了事件的结果。

安全问题

Oracle是第三方服务，它并非区块链共识机制的一部分。Oracle的主要难题在于如何让人们相信这些数据源是可靠的。不管是网站还是传感器，信息源必须是可信的。不同的可信计算技术可以用来解决这些问题。例如Oraclize 利用基于TLSNotary的证明机制来给亚马逊提供支持。另一个公司Town Crier则专注于利用英特尔的软件防护拓展Software Guard Extensions (SGX) 。从智能合约的角度看，可信任的数据源对于用户来说是至关重要的，毕竟一旦出错无法回滚重来。

引用和扩充阅读

Hardware Oracles: bridging the Real World to the Blockchain
Understanding oracles
A visit to the oracle
Smart Contract Oracles
Can oracles send data to smart contracts on multiple blockchains?
How can an Ethereum contract get data from a website?
Why Many Smart Contract Use Cases Are Simply Impossible?
1,749,693 blocks later , Oracalize

SchellingCoin: A Minimal-Trust Universal Data Feed, Vitalike Buterin
Town Crier: An Authenticated Data Feed for Smart Contracts: Scientific paper

去中心化软件（dApp）

去中心化应用（dApps）

去中心化应用（dApps）是在计算机的P2P网络上运行的应用，而非单一一台计算机。dApps自P2P网络出现以来就已经存在。 它们实质上是一种软件程序，设计这类程序的目的在于它们在互联网上可以不受任何单一实体控制。

❑ 去中心化的应用不一定需要在区块链网络上运行.较为常见的dApp, 诸如：BitTorrent，Popcorn Time，BitMessage，Tor都是在P2P网络上运行的，而不是在区块链上运行。

❑ 与简单的智能合约相反，按比特币的传统意义上说，它将钱从A发送到B，dApp在市场的各方面拥有无限数量的参与者。

去中心化应用VS 智能合约

dApps是一个“启用区块链”的网站，智能合约可以让它连接到区块链。 了解这个最简单的方法是了解传统网站如何运作。

❑传统网站的运作

传统网站是使用HTML，CSS和JavaScript来呈现页面。 它还需要利用API从数据库中获取细节。 当您进入Facebook时，该页面将调用一个API来获取您的个人信息并将其显示在页面上。

❑去中心化应用

而去中心化应用类似于传统的Web应用。 前端使用完全相同的技术来渲染页面。 显著的区别在于，您有一个智能合约连接到区块链而不是连接到数据库的API。

与传统的中心化应用（后端代码在集中式服务器上运行）不同的是，dApp的后端代码运行在分布在P2P网络上。 去中心化的应用从后端到前端都由软件包组成。 智能合约只是dApp的一部分：

●前端（你看到的）

●后端（后台逻辑）

另一方面，智能合约只包含后端，通常只包含整个dApp中的一小部分。 这意味着，如果您想在智能合约系统上创建去中心化应用，则必须合并多个智能合约，并依靠第三方系统作为前端。

dApp可以以任何语言（就像应用）编写前端代码和用户界面，可以调用其后端。 此外，其前端可以托管在Swarm或IPFS等分散存储上。

dApps要求

对于在区块链中被视为dApp的应用，它必须符合以下标准：

❑应用必须是完全开源的

它必须自主运作，并且没有实体控制其大部分令牌。 应用可能会根据改进意见和市场反馈来调整其协议，但用户的共识必须决定所有更改。

❑应用的数据和操作记录

应用的数据和操作记录必须密码存储在公共的，去中心化的区块链中，以避免任何因中心化产生的故障点。

❑应用必须使用的加密令牌

（比特币或其他系统令牌）是登入应用所必须的，（矿工/农民）价值贡献都应该使用相应的令牌给予奖励。

❑应用必须生成令牌

根据作为价值证明的标准密码算法，每个节点可作为应用的贡献点（比特币的获得是使用工作证明算法）。

dApps开发流程

❑ 白皮书和原型

白皮书的发布是阐述了dApp细节和其功能，白皮书可以概述dApp 开发者的想法，并且阐述了工作原型。

❑ 令牌的发行

初始币发行规则的设立。

❑ ICO – 初始币上市发行

dApp所有权益的扩散。

❑ 实施和启动

投资基金投钱构建dApp，并且进行部署

案例：以太坊

以太坊计划为建立去中心化应用创建了以太坊合约。 以太坊为开发人员提供了一个终极抽象的基础层：内置嵌入了图灵完整编程语言的区块链，使得任何人能够创建智能合约和去中心化应用，并且创建自己的所有权，设立他们自有定义的所有权规则，交

易格式和状态转换函数。域名币的主题框架自需要两行代码就可以实现。 总的来说，在以太坊之上有三种应用。

❑金融应用：为用户提供更有效的管理方式，并使用他们的资金签订智能合约。
❑半融资应用：涉及到金融，但所做的事情也有很大程度上是非金融属性。
❑管理应用：如在线投票和去中心化治理，并非在金融领域的应用。

- 31 –

举例：Ethereum dApps:

❑**令牌系统**：区块链令牌系统有许多应用，从代表资产（如美元或黄金）的子货币到公司股票，代表智能财产的单个令牌，安全不可伪造的优惠券，甚至与传统价值无关的令牌系统，用作激励的积分系统。

❑**金融衍生工具和稳定价值货币**：例如，一个非常理想的应用是智能合约，通过使用来自例如纳斯达克的数据，对冲以太币相对于美元的波动。

❑**身份和信誉系统**：一份声明土地所有者名称的合同可以添加到以太坊网络中，但不能修改或删除。 任何人都可以注册一个有一定价值的名字，那么注册就会永远持续下去。

❑**去中心化文件存储**：类似 Dropbox 的 dApp，其中智能合约将所需数据分成块，对每个块进行加密以保护隐私，并从中构建 Merkle 树，然后将整个数据分布到 P2P 网络中。 然而私人数据不会存储在区块链上

❑**去中心化自治组织（DAOs）**：拥有一定数量的成员或股东的虚拟实体（可能拥有多数的 67%）有权使用该实体的资金并修改其代码。 成员们将共同决定组织如何分配资源。

dApp许可证

在开放源代码许可下运行允许dApps在不受版权或专利限制的情况下开源。 另外，通过完全开放源代码，分布式应用可以在开源软件的合法模式下运行。 例如，比特币使用MIT开源软件许可证。

引用和扩充阅读

以太坊白皮书适合入门者
以太坊黄皮书适合区块链技术规格
挑选一种语言：坚持一个拥有最广泛文献资料的语言
选择一个框架和测试 rpc：Solidity 框架出发，并使用 Ethersim 作为测试 rpc
看看示例项目：例如。 在 Github 上的 Consensys
dApps 的基本术语
ConsenSys dApps 教程
以太坊 dApps 为初学者
以太坊阅读清单适合潜在的 dApp 开发人员查看
全栈“Hello World”投票以太坊 dApp 教程
在以太坊开发的所有 dApp 的列表

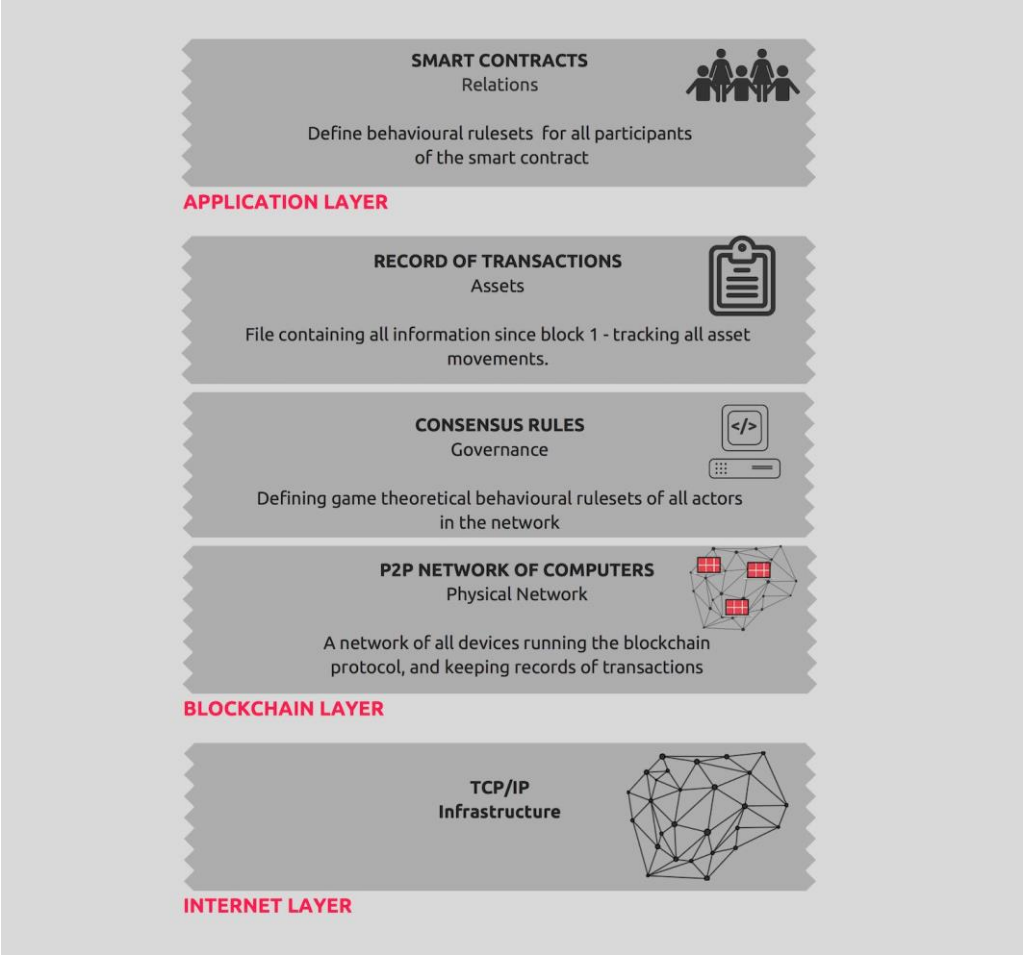
DAOs

DAO (Decentralized Autonomous Organization, 去中心化自治组织) 可以被看做智能合约最复杂的一种形式，其中去去中心化组织的细则被一套复杂的代币管理条约嵌入了智能合约的代码中。

历史上，比特币网络被认为是第一个真正的分布式自制机构（autonomous corporation），它仅仅

通过一个人人都可以随意采纳的分布式共识协议（distributed consensus protocol）进行协调。如

今，DAOs 提升了技术栈（technology stack），从而通过软件实现了完全虚拟化。在一个比特币式的分布式自治机构中，会使用一系列复杂的技术和人机系统创造出能良好运行的自制基础设施。



以太坊及相似区块链的技术栈

在现今的演进阶段，一个 DAO 将实现为一个智能合约 —— 一段代码 —— 在越来越不

透明的，例如以太坊和其他类似区块链这样的分布式网络和共识技术上执行。

去中心化组织 Decentralized Organizations (DO)

去中心化组织这个概念来自于传统的组织，并将它去中心化。传统组织由不同的等级架构组成，一部分人通过法律系统来对这个组织架构进行管理，他们需要亲自互动。与之不同的是，去中心化组织中，这部分人之间的互动是通过被代码指定，并在区块链中执行的协议来完成。

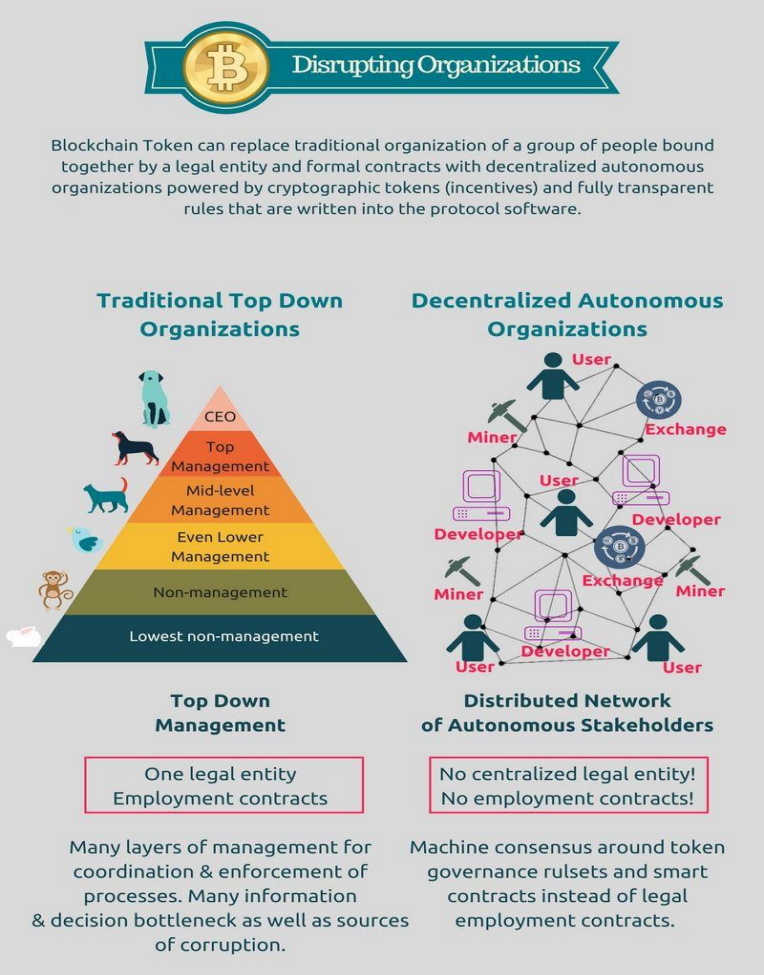
去中心化组织可能会也可能不会使用法律制度来保护它的物理性质，但这种用法是次要的。比如说，可以把股东拥有的公司整个移植到区块链上；以区块链为基础的一份长期运行的合约酱保留每个人持股的记录，同时区块链上的投票让股东们能选举董事会和员工。

智能财产系统（smart property systems）也可以被直接集成到区块链中，可能允许DO来控制车辆、保险箱和建筑物。**DAOs 是 DOs 的圣杯**：它是一个自主存在、生活在互联网上的实体，但也很大程度上依靠雇佣个体来执行某些依靠自动机制无法完成的任务。

颠覆统治

管理 (governance) 是一种建立并维持规则、规范和行为的方式，来指导人们的互动。当一个有关于创造、强化或再造社会规范的问题出现时，“管理”规范了参与者之间的决策过程。管理形式的程度，对内取决于特定组织内部的规则，对外取决于它的商业伙伴。因此，“管理”可能有多种形式，由不同的动机驱动，也带来不同的结果。

“管理”涵盖了管理中的所有过程，无论是由政府、市场还是网络、家庭、部落 ——正式或非正式——通过法律、规范、权利或者语言来实现。区块链可以打破任何形式的传统管理结构，挑战我们目前对管理的看法。



区块链代币打破传统组织结构

传统来看，我们社会的大部分组织都采用自上而下的指挥和控制方式，而区块链保证了更大程度上的去中心化和自发协调的功能，以应对传统僵化的组织结构的两个主要问题：1.委托代理困境；2.协调交易成本。

智能合约在信用缺失的信用环境里——DAOs是最复杂的一种智能合约形式——解决了一个关于管理的一个历史性困境，即在政治学和经济学中被称作“委托人—代理”的问题。这种困境的出现，主要是因为代理人——通常是一个人或一个机构——能代表，或影响委托人的决定。这种情况下会出现道德风险的问题，因为做出行为的人和承担风险的人不是同一个，行为的人会倾向于风险更大的行为，而这其中往往还暗含着信息不对称的情况。如果行为人比风险承担人对这个交易的信息了解更多，他们会出于自己的利益考量去做事——而这往往和委托人的利益相悖。

区块链和智能合约降低了交易成本和官僚级别，并且带来了一种全新的可能性，用去中心化的方式去分配利益、管理团队，和现今的管理方式完全不同。

DAOs 的运用

去中心化自治组织 (DAOs) 通过在被称为智能合约的计算机程序运行。它是一个互联网上自主存在的组织，但也严重依赖于个体去完成一些自动化不能完成的任务。

- 交易代币：DAO 的组织结构中需要一种内部有价值的财产，能够被用来作为奖励机制。这笔资金直接来自于组织的简历。DAO 不具有层级结构，也没有高层和管理层。

- 自治：一旦 DAO 组织被组建起来，它便独立于创造者，而且不会受到外部力量的影响。 DAO 是开源的，因此透明且不可腐败。一个 DAO 的交易记录和程序规则保留在区块链上。这种方式消除了需要在金融交易中需要一个双边接受的可信第三方。

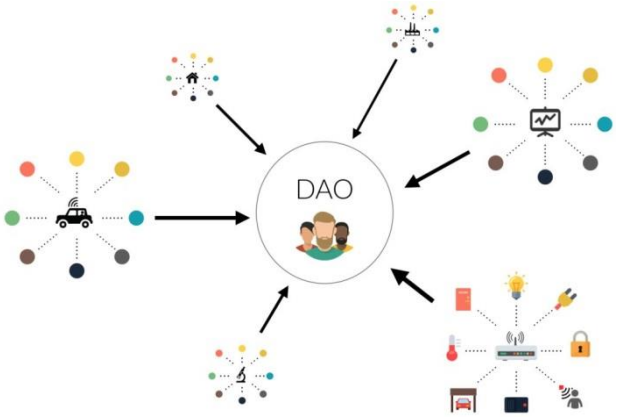
- 共识：为了从 DAO 中提出或转移资金，大多数利益相关者（数量可由 DAO 的代码指定）必须统一这个决定。这就导致，即使代码中发现有错误，在没经过投票决定之前是不能对它进行修补的，这可能导致已知的安全漏洞被利用。

- 承包商：DAO 不能构建产品，编写代码或开发硬件。它需要一个承包商来实现目标。承包商通过代币持有人的投票指定。

- 提议：提议是 DAO 中作出决定的主要方式。为了避开大量的建议在网络上拥堵，DAO 可以要求一笔定金，以防止网络被恶意信息侵占。

- 投票：提议方案提交后，就进行投票。DAOs 允许每个人和世界上任何人进行交换经济，比如投资、融资、借款、贷款，而不需要一个中间人，只需要相信代码。

所有使用公共区块链的加密货币都是 DAO (Bitcoin，Ethereum，Dash，Digix 等). 现代 DAO 是区块链上的复杂智能合约。DAO 就是一个 DAO 在以太坊区块链上的例子。

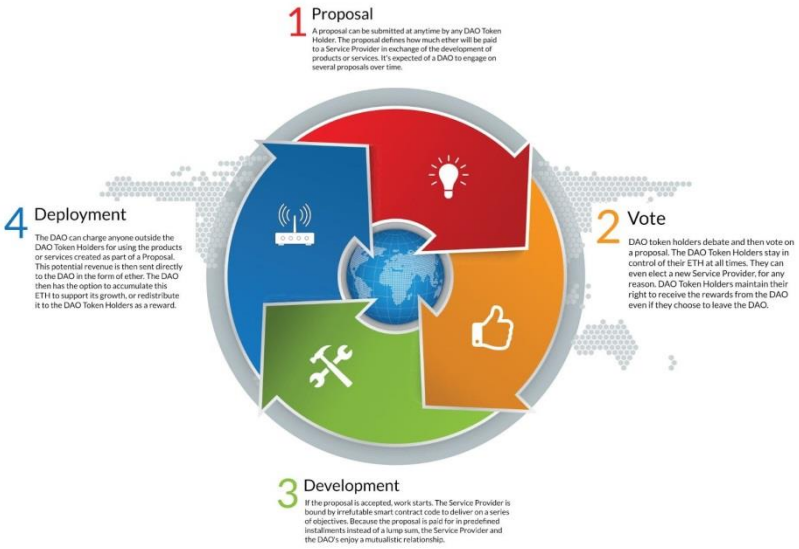


去中心化自治组织

DAOs 作为众筹平台

由于智能合约运行在诸如以太坊这样的公共区块链网络之上，智能合约可以被设计成程序用于收集和管理任意数量的实际经济价值，这个过程被称为 ICO。DAO 就是这样一个 ICO 的例子。其目标是成为一个分散的自治投资基金，这个基金不需要基金经理。TheDAO（当时最大的 ICO）最终收集了价值相当于 1 亿 5 千万美元的加密货币。愿意投资 DAO 的每个人都能保证按比例获得这个公司未来收入的一部分份额。此外，这些份额可以在加密货币交易所上与任何其他资产进行交易，交易对可能是法定货币和加密货币。

尽管 DAO 实验以引人注目和极具争议的操作手法和随后从以太坊的硬分叉草草收尾，但这种基于区块链代币发行作为基金未来所有权份额的众筹模型已深入人心， 这进一步引发了全球的创业者们对 ICO 的狂热。



TheDAO 的投票过程

越来越多的创业公司开始用一种能让用户和投资者分享未来收益的方式去寻求风险资本，并将这些资金用于支持独立产品、服务或协议的开发。投资者和创始人之间不必使用复杂、不确定、且严格管制的法律合同关系，而是完全依靠 DAO 型智能合约来管理他们之间的关系。

但是，规避法律体系和合法性，并不是大多数初创公司的主要兴趣。相反，由于它很低的进入壁垒，以及未开发的市场潜力，激励了创业者们走上了 ICO 众筹。这是一种新型的共享经济，服务的使用者同时是其所有者，让这些初创企业有了冒险进入合法灰色地带的道德余地。

法律要求

想要用 DAO 来运行的创业公司需要一个法律框架，帮助他们不仅仅在区块链网络的封闭环境中开展业务，还要和传统金融工具和知识产权的物理世界产生互动。为了实现这个目标，需要克服两个主要的障碍。

首先，初创公司在出售加密币的时候，需要知道在不同的辖区和法规中，哪种形式代表了未来利润的股份。不言而喻，当代的证券监管系统有被应用的潜质。其次，初创公司需要一个可行的合法合同框架，可以让 DAO 被嵌入上述的物理世界、知识产权和传统金融工具的机构框架中。

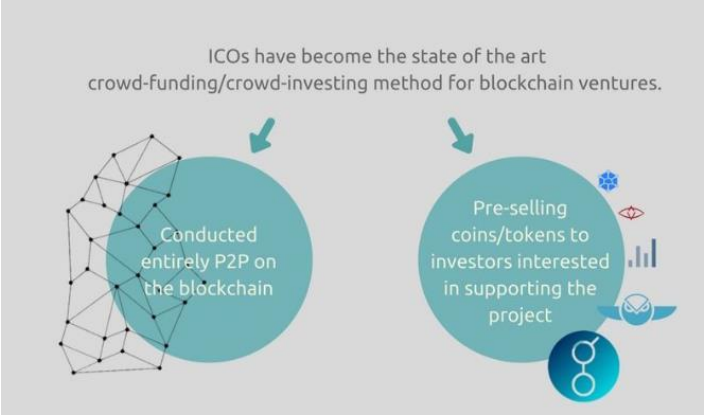
这两个问题都是很难解决的，因为这是一个从前只在科幻小说中出现过的领域，而我们需要在这个前所未有的领域中用法律的眼光去看很多问题，这是非常艰难的。不过，我们可以在一定程度上得出一个勉强合意的解决方案。这需要依靠一个对复杂的合规问题有丰富经验的团队，并且熟悉国际私人法、金融法、贸易法、公司法及税法。

引用和扩充阅读

DAOs, DACs, DAs and More: An Incomplete Terminology Guide, by Vitalik Buterin
On Risks, Rewards and The Evolution Of DAOs, by Maciej Olpinski
Explaining DAOs to a non-technical person in 10 points, by Maciej Olpinski
How to Evaluate an ICO, by Shermin Voshmgir
Resisting the ICO gold rush, Greg McMullen
On Tokens and Crowsales, Coindesk
Disrupting Organizations with Blockchain & Smart Contracts Journal For Strategic Change, Shermin Voshmgir

首次代币发行

ICO 是完全通过区块链进行众筹或集体投资的方式。一开始，ICO 的主要目的是通过向感兴趣的投资者提前售卖数字货币/代币，来为项目筹集资金。在 ICO 之前，创业者通过白皮书展现项目的商业模式和技术特点。他们提出了项目的时间线和财务预算（如何使用资金，推广，R&D 等等），以及数字货币的分配方案（自己持有多少代币，发行多少数字货币等等）。在众筹的路演中，投资者使用比特币和以太币等较为成熟的数字货币购买代币。



首次代币发行

来源： Blockchainhub.net

传统的众筹投资一般被认为是对众筹产品的捐赠和预先购买，与之不同的是，ICO 同时给予那些投资者高价转售代币的可能性。同时，只要代币代表了在项目中的权益，ICO 就与 IPO（首次公开募股）相似。

众筹还是众投?

根据白皮书的不同，代币可以有完全不同的属性。ICO 经常被比作区块链上的众筹或集资投资。大多数 ICO 是两者混合的，难以被归于某一类。与众筹经常被认为是对产品的捐赠不同，ICO 给与投资者获取投资收益的可能性。ICO 可以被视作捐赠、投资和风险资产的混合体。

投资者通过投资支持某个初创想法获得代币。如果初创想法成功了，代币将会升值，但通常代币不代表在项目中的权益。如果代币代表了在项目中的权益，此时 ICO 就和 IPO 相似。大部分在 2016 年和 2017 年的 ICO 项目并没有给投资者在项目中的股份。这些投资者纯粹希望通过投资收益获利。

2016 年的 TheDAO 项目是与 IPO 最为相似的 ICO 项目，只是投资者并不希望获取投资收益。每个代币拥有者在项目中拥有与自己所持代币数量成正比的投票权。

请注意，根据白皮书的不同，代币可能有非常不同的特性、价值主张和法律性质！

Web2 vs Web3

来源： Blockchainhub.net

规则

直到最近，ICO 的设置方式完全根据区块链项目背后的团队进行。目前，ICO 仍然缺少政府监管和行业标准，这些都不利于未接受区块链教育的投资者。

大多数情况下，投资者购买一个新的代币并不能获得在公司中的股权，而是希望在项目成功后高价转售代币。批评者认为，目前人们投资 ICO 项目的动机主要出于害怕错过涨幅，而不是理性投资，这给那些真正理解交易系统的人许多优势。

大部分国家缺乏对区块链监管的事实使得创业者和投资者面临较大风险。但这种情况证迅速改变，监管者迅速制定规则或者开始研究规范 ICO。SEC 声明将监管去中心化组织和中国韩国禁止 ICO 的行为，可能会给 ICO 生态系统带来不一样的趋势。

首次代币发行种类

由于缺少监管，开发者有充分的自由来运行 ICO。因此 ICO 有许多方式。几乎每一个 ICO 都与众不同，覆盖所有的 ICO 情况是几乎不可能的。但是，ICO 期间代币的价格通常会经历几个阶段。大体上说有四种不同的定价机制：

1. 售价增长模式

售卖的代币价格在 ICO 的不同阶段中逐步上升，其中每个阶段的价格固定。这让那些早期承担更大风险的投资者获得最优价格。投资者通过将比特币或以太币送至指定地址获取新代币。

2.售价下降模式

售卖代币的另一个方式是荷兰式拍卖，Gnosis 团队是第一个使用这种方式的团队。售价从最开始的最高价慢慢回落，直至 ICO 阶段结束。

3.售价固定模式

代币售价（汇率）在发行阶段是固定的，投资者能以相同价格尽可能多的购买代币。这个机制对大额投资者较有吸引力，因为他们大额的购买不会造成市场价的波动。在代币发行阶段结束并经历一段静止期后，代币上交易所按照市价交易。

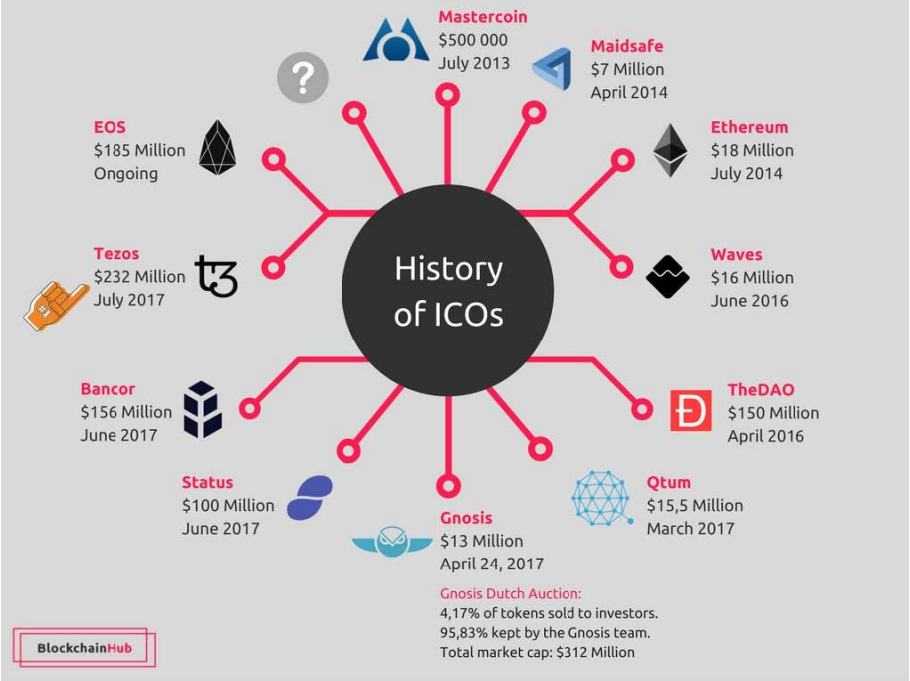
4.售价不固定模式

开发者可以选择不以固定的售价发行代币，而是让投资者投资他的创业公司，最终通过投资者在创业公司中投资的比例发行相应比例的代币。在 EOS 发行中，投资金额除以代币发行数额得出了发行价。在这种情况下，如果只有一个投资者，他将有 100%的代币。

目前大部分代币发行都有时间限制，但有些创世团队（比如 Tau-Chain）没有给他们的代币发行设定时间期限和截止时间。所以当你在投资之前，请先确认流通代币数量和定价机制。

首次代币发行历史

最早的 ICO 要追溯到万事达币（在交易所用比特币换取万事达币），这是完全以 P2P 形式运行的项目并且激励了许多利用比特币区块链来进行 P2P 众筹的项目。



来源： Blockchainhub.net

2014 年的以太坊项目也以比特币区块链为基础，在一个月里成功募集了 1800 万美元价值的比特币，打破了当时的 ICO 记录。以太坊区块链成为了简化发行代币的平台，促成了 2016 和 2017 年许多创纪录的 ICO 发行。

ICO 仍然是个比较新的概念，在众筹世界中仍然占比较小。全球 2015 年众筹规模为 340 亿美元，ICO 只占了不到 1%，共筹集 2400 万美元。2016 年最大的 ICO 项目是 "The DAO",共筹集 1500 万美元。

ICO 资料

Coindesk's ICO Tracker ICO Transparency Monitor CyberFund

Icoalert

Smith and Crown

加密数字货币基金

Iconomi Melonport

Prism

引用和扩充阅读

How to Evaluate an ICO - Part1 by Shermin Voshmgir

How to Evaluate Initial Coin Offerings by William Mougayar

Cryptoassets: Evaluation & Due Diligence framework

10 Steps for Evaluating Digital Asset Crowdsales, Tokenmarket

Investment Guide To 'Crypto' Coin Offerings Rating Blockchain Startups, Forbes WeTrust: Lending Circles Going Blockchain, Daniel Zakrisson, WeTrust

ICOs, Token Sales, Crowdfundings, Smith & Crown

What is an initial coin offering?, Blockgeeks

What is an Initial Coin Offering (ICO)?, Ben Dickson

Initial Coin Offering, Investopedia

实用指南

在第一部分中，我们介绍了区块链的基本原理，以了解区块链如何以及为什么区块链是一个游戏规则改变者。在这一部分中，我们将重点讨论一些实用的与区块链新手相关的指南。

想开展区块链项目-我从哪里开始?

实现区块链或其他分布式账本技术的方法有很多。各种各样的参与者出现了，包括软件服务提供商，他们提供的软件能力比区块链协议本身更高。每种方法都有其优点和挑战。

	怎么做	案例
IT服务	建立在需求上	ConsenSys
区块链优先	用特殊区块链提供的工具开发	Ethereum,Bitcoin
开发平台	为IT专业人员提供的工具	ERIS,Tendermint, Hyperledger
垂直解决方案	针对特定行业	Axoni,Chain,R3, itBit, Clearmatics
特殊应用程序界面	DIY建立区块	Blockstack,Factom, Open Assets, Tierion

区块链实施方案（来源：Coindesk.com）

区块链作为服务(BaaS)

建立一个测试和研究区块链的环境需要一个有多个系统的生态系统来开发研究和测试。云计算行业的大公司如亚马逊(AWS)、微软(Azure)、IBM(BlueMix)已经觉察到了在云服务中提供区块链服务的潜在好处，并开始为客户提供某种程度的BaaS。用户将受益于免除配置和设置工作区块链的麻烦，硬件投资也不需要。微软已经与双方达成了合作协议，在微软Azure上提供以太网区块链作为服务(EBaaS)。IBM(BueMix)已与Hyperledger合作，为其客户提供BaaS。亚马逊宣布，他们将与数字货币集团合作推出这项服务。开发者将拥有一个基于云的区块链开发者环境，这将允许快速开发智能合同。

例如: Accenture, ConsenSys, Cognizant, Deloitte, IBM, PricewaterhouseCoopers (PWC),

Ernst & Young.

区块链优先

在这种情况下，用户直接使用给定的区块链工具和堆栈。装配是必需的，目前而言许多技术仍在发展。然而，直接使用区块链提供了创新机会，例如构建去中心化的应用程序。企业家们创建了端到端的、点对点的应用程序，比如OpenBazaar(关于比特币)，或者Ujo Music(Ethereum上)。

例子:比特币、Ethereum等。

开发平台

这里，你不需要从区块链开始。相反，可以从开发方法的方向入手，然后构建一个应用程序，支持在云中服务的区块链基础设施。这里的目标是快速开发，关注的是区块链可编程性。

一些选择:BlockApps, Blockstream, Monax。

例子: Parity, Hyperledger, Tendermint.

垂直解决方案

在过去的一年里，我们经历了最快速的蜕变，主要是金融服务方面。这些解决方案是针对特定于行业的，并基于私有区块链或分类帐基础设施。需要注意的是，其中一些不是完整的区块链。相反，它们是分布式的账本，是区块链功能的子集。有些甚至还没有包含一个共识元素，它将实现从分布式的分类技术中降低到另一个层次。

例子:Axoni, Chain, Clearmatics, Digital Asset Holdings, itBit, R3。

接口

这种方法将区块链作为一种资产、所有权或身份验证的基础设施，并且在构建应用程序时，将重点放在证明、所有权、所有权注册或其他具有内置信任组件的特定服务上。

例如:Blockstack, Factom, Open Assets, Tierion。

如何找到区块链开发人员?

在区块链领域，人才短缺已经成为许多公司关注的问题。虽然这种类型的短缺在每种技术的早期阶段都是典型的，但在这种情况下有一些不同:许多在加密社区经验丰富的开发人员在早期也投资了加密货币，而且通常不需要你的资金。此外，他们中的许多人可能更喜欢自己创业，通过ICO筹集资金，而不是为别人打工。

更具体一些

在你列出工作机会之前，你需要了解你正在寻找的是什么。你需要或想要构建什么?声称你在寻找一个区块链开发人员就好像在说，你在寻找一个互联网开发者。

❑ 你想建立一个新的区块链吗?

然后您需要一个区块链全栈开发人员。

❑ 你想构建一个应用程序运行在一个区块链吗?

然后你需要dapp开发人员，他们了解固体(Ethereum)、侧链(Bitcoin)等。

❑ 理解blockchain面临法律挑战

这将影响你的基础设施决策。根据你想建立的服务类型，可能会面临更多或更少的法律挑战，因为一些行业受到了严格的监管。如果你的公司是在一个高度监管的行业，你可能会想考虑建立一个许可的区块链。这也可能影响你的发展决定或限制/增强你能吸引的人才。

在您雇佣一个区块链全栈开发人员之前，请考虑使用已经存在的区块链基础设施，如Ethereum。区块链的全部意义在于分包基础设施。应用程序变得更薄、更简单、更便宜。从头开始构建整个区块链非常耗时。除非你想发明一种新的区块链，如果你不是上帝，这是不可能的，因为你甚至不知道如何构建它，最好是在现有的区块链之上构建。在这种情况下，你需要对你想要构建的区块链类型有一定的想法:无需准入还是需

要准入、公开的或私有的。

去哪里寻找?

传统的求职网站，比如LinkedIn，可能不是区块链人才的最佳选择。建议开始查看相关的加密社区。

❑Reddit

需要注意的是，许多加密货币社区的人都很重视他们的隐私，在传统的社交媒体上并不是很活跃。然而，他们中的许多人在Reddit上都很活跃。看看Reddit上的相关群——这是许多开发者讨论他们感兴趣的话题和创新的地方。如果能与他们感兴趣的领域产生共鸣，你可能会幸运地找到需要的人。

❑Gitter

考虑在Gitter上推广你的项目，也许人们会来找你。Gitter是开发人员首选的聊天应用程序。

❑Slack/Discord

每个crypto项目都有自己的Slack/Discord通道。一些社区的频道有超过5000人。

❑Ethlance

给予自由职业者在区块链的帮助下提供在线服务的机会。为了访问应用程序并查看清单，需要安装一个dApp浏览器，例如MetaMask。

❑Bitcoin Talk forum

Bitcointalk论坛是一个宣布新的加密项目的地方，这也是第一个比特币论坛，它还有一个很大的社区。

❑Meetups

许多开发人员参加本地区块链聚会。参加当地的区块链聚会，和那里的人交谈。

❑Start up Contents & Hackathons

组织竞赛，以吸引区块链开发人员的注意，或者参加像Ethereum Devcon这样的会议。

建立内部的经验

区块链开发人员的缺乏可能会让他们很难从外部寻找和资助优秀人才，所以最好的办法就是培养内部人才。这需要一段时间，但从长远来看对你最有利。多接触外界有助于培训你现有的员工。

了解区块链和去中心化网络的文化

早期的区块链开发者仍然是比特币社区的一部分，他们倾向于强烈的自由主义。个人自由是最有力的主张之一。传统的招聘方法可能行不通(例如:，LinkedIn，求职网站的公告等等)。要求固定的工作时间表可能也不太吸引人。区块链不仅是存储价值的工具，而且还围绕着一个新的去中心化世界秩序创造了一个经济体系。如果你的文化与这种新思维不匹配，或者你不承认区块链是一种全新的经济方式并且商业逻辑正在改变，在吸引优秀人才时就可能遇到问题。

如何购买比特币

免责声明!交易加密货币涉及高风险(价格波动)、低可用性(对非开发人员而言，缺乏用户体验)和不良参与者(小心欺诈!)不建议没有经验的投资者投资大笔资金。投资金额不要超过你愿意承受的损失。而具备经验的高技能人应该抓住这样的机会。投机市场可能导致资金的全部损失!

哪里可以买到比特币和其他加密货币?

你可以在不同的地方购买比特币和其他加密货币。你可以选择:

❑Cryptocurrency交流(在线)

❑比特币自动取款机(你把钱里面可以加载您的比特币钱包)

❑比特币券卡(例如： Austrian Post Office, House of Nakamoto，Azteco London)

❑亲自从持有者处购买

为了购买比特币，你可以使用标准的支付方式，包括银行转账、信用卡、现金或Paypal。他们都有自己的优点和缺点，与其他方法相比，银行转账要慢一些;信用卡有很高的交易费用，paypal有交易限制，现金没有达到最好的汇率。下文将向您简要介绍如何购买加密货币和可能的支付方法。

加密货币交易所

开始购买货币的最好方式是在大型的加密货币交换网站创建一个钱包。为了创建一个帐户，每个用户需要提供一个正式的身份证。在交易所，您可以购买大多数流行的货币，并将它们放在同一个钱包中。这很方便，而且会节省你很多时间。钱包的类型被称为在线钱包，人们依靠交易所来保证他们的资金安全。在你购买了你的第一个比特币或其他加密货币之后，你应该考虑将这些资金转移到一个更安全的钱包里，这个钱包只能由你自己控制。购买加密货币有不同的方式。为了简单起见，让我们关注比特币。

❑Coinbase是最受欢迎的比特币在美国在线交易所。它在许多欧洲国家也有业务，并提供一流的用户体验和可用性。应该指出的是，Coinbase是为数不多的保证其平台上所有资金的交易所之一。在发生安全漏洞时，保险单会覆盖损失。该公司还提供移动应用。你可以通过银行电汇或信用卡购买比特币。

❑Anycoindirect是一家欧洲加密货币的交易所。它没有提供专门的在线钱包。客户使用他们的银行账户向供应商汇款。在收到钱后，用户可以将比特币的金额转移到他们提供的地址。

❑Cex允许购买比特币信用卡或银行转账。该交易所拥有全球范围的覆盖范围，并为交易平台提供了融资融券交易的能力。

❑Shapeshift是一个不同类型的交易所。该平台针对的是持有不同加密货币组合的用户。这个交易所的初衷是交换不同货币，而不需要注册一个账户。它提供了高度的隐私。如果你已经拥有比特币，这是一个购买其他加密货币的好地方。

❑LocalBitcoins提供点对点比特币交换。买卖双方同意贸易条件。该交易所连接了想要交易比特币的当地人。付款方式是由卖家决定的，你可以用Paypal购买货币，通过银行，甚至是现金。该平台提供高度的隐私。

❑Kraken 是基于美国的加密货币交易所和交易平台，在欧洲也有业务。它提供比特币的融资融券。银行转账是从海地银行购买比特币的唯一途径。

❑Bitrush 加密货币交易所位于欧洲。人们可以用信用卡、iDEAL、Bancontact 和MyBank购买货币。

❑Bitstamp是第一个在欧盟许可下的虚拟货币交易所。用户可以通过银行转账和购买比特币来存入资金。Bitstamp也是一个交易平台。

❑Gemini是加密货币交换和交易的平台。目前，它只在美国运营。它允许个人和机构客户购买、销售和存储数字资产。此外，平台的保险金额最高可达25万美元／人。你可以通过银行存款购买比特币。

❑OkCoin是中国最大的交易所和交易平台。

❑Coinmama是比特币代理商,允许用户使用借记卡或信用卡购买比特币。

比特币自动取款机

公共场所的自动取款机让人们有机会用现金购买比特币。你需要先安装一个钱包，以便将货币转移到你选择的地址。

比特币卡/礼品卡

在你所在地区的商店里可以买到代金券。这些看起来像其他的礼品卡，可以在网上兑换。这些卡片适用于小额购买。

钱包:管理货币的地方

像比特币这样的货币可以储存在“钱包”里，可以把钱包看作你的银行账户。不同之处在于，在密码世界里，你没有像金融机构那样的第三方来保管你的钱。在资本损失或安全漏洞的情况下，没有赔付。采取正确的步骤对保障资金安全至关重要。做你自己的银行需要更多的谨慎和责任。

要开始使用比特币或其他类型的加密货币，你首先需要一个加密钱包。该钱包存储用户的私钥和公钥，允许发送和接收货币。不同的加密货币提供他们自己的桌面或在线钱包，可以在他们的网站上找到。钱包不储存任何硬币。钱包的唯一作用是保持用户的私钥的安全，并连接到相应的区块链。私钥允许双方资金流动。把你的私钥当作你的家庭钥匙，如果你把它交给别人，他就会和你一样有力量。注意，货币永远不会储存在你的钱包里。谁拥有多少比特币的记录保存在区块链里。在可用性和安全级别上

有四种类型的钱包。

❑桌面或移动钱包

这是最常见的一种钱包。一个应用程序必须在你的电脑或移动设备上下载。它会将用户的私钥存储在设备上，这就是为什么它强烈建议定期备份钱包，并将其存储在不同的设备上，除了你的电脑(u盘等)。一个移动钱包可以和一个真正的现金钱包相比较。人们不会把他们的全部财富放在他们裤子后面口袋里，你不应该把所有的密码都储存在你的智能手机上。移动钱包可以与真正的现金钱包相比较。

❑ Copay.io (桌面/移动)

❑ Jaxx.io(桌面/移动)

❑ Mycelium.com (移动)

❑ Electrum.org(桌面)

❑ Exodus.io (桌面)

❑在线钱包是基于网络的钱包,托管在一个服务器上。每个在线钱包都需要一个密码登录。这些钱包的好处在于可用性。他们是最友好的因为设置很少 。缺点是，钱包的主人依赖于第三方，而第三方可能是盗窃的受害者，或撤销对钱包的访问。建议不要在网上钱包中储存大的数值。强烈建议在登录时启用双重身份验证(2FA)。尽管已经启用了2FA，但仍有用户报告被盗货币被偷的情况。黑客利用社会工程技术将受害者的电话号码劫持。即使是在网上银行，这些电话号码也会被用作2FA的在线钱包。像谷歌认证器这样的应用程序为2FA提供了更大的安全保障，也是许多人保护他们的在线档案的首选方式。

Blockchain.info

Coinbase.com

❑硬件钱包是一种特殊类型的钱包,将用户的私钥存储在一个安全的硬件设备(如u

盘)。硬件钱包通过在电脑或手机上安装一个专用的应用程序，并通过USB将其与物理设备连接起来。这样，私钥就会离线存储，因此不会受到病毒或来自internet的攻击。缺点是你必须先购买设备。

Ledgerwallet.com

Bitcointrezor.com

Bitcointrezor.com

❑ **纸钱包:**在这种情况下,人们可以生成自己的私钥和公钥和离线存储打印在纸上。

这种方法避免了在任何设备上存储数字数据，提供了最强大的安全性，但牺牲了可用性。一旦印在纸上，这些钱包就必须放在安全的地方。丢了那张纸，钱包里的钱就不能用了。

Bitaddress.org

纸钱包案例:

左边：公共地址用于接受资金

右边：私有密码用于检查资金

备份:如何保护你的货币

在创建了一个钱包后，你应该做的第一件事就是备份。丢了钱包就等于烧了你的钱。

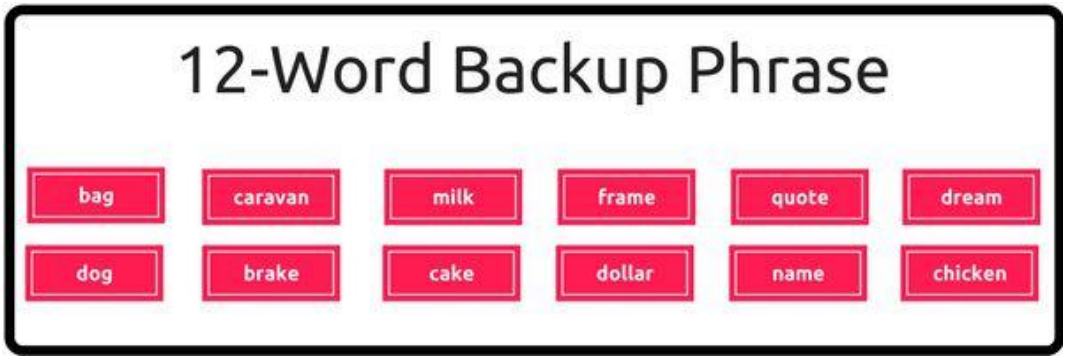
在你第一次启动钱包后，你会得到一个12字的回复短语(这个短语可能在12到24个单词之间)。有些钱包只显示这个短语一次。

一定要把单词写下来，保证它们的安全。如果有人获得了这些词语的使用权，他或她就可以获得你的资金(在这篇指南中，有一些不同的场景是不会涉及到的，但是一般来说，这句话应该对其他人保密)。

请考虑火灾和其他自然灾害的可能性。拥有一个防火的存储盒是一个不错的安全附加组件。如果你需要从这个12字的短语中找回你的钱包，你只需要在任何设备上安装一个新的钱包程序，然后在启动时输入这个短语。

然后奇迹发生了，你的钱包和里面的钱一起被修复了。在12字短语的丢失的情况下，强烈建议将你的资金转移到一个新的钱包，这个钱包是适当的备份。在你的电脑上储存12个单词是很危险的，因为总会有安全漏洞。

有些情况下，12个字的短语不会用于备份。第一个场景是在线钱包。用户不拥有这些钱包的私钥，交易所代为保留。如果网站宕机，密钥就会随之消失，用户的资金也将不复存在。第二种情况是纸质钱包。这个短语是不需要的，因为所有的信息，包括私钥，都是打印在纸上的。



有些钱包仍不使用12字的备份短语作备份(例如:完整的节点钱包)。这些钱包被称为不确定性(随机)钱包。这样的钱包是比特币核心的完整节点客户端。这些钱包需要用户手动备份。这是通过将包含私有密钥的文件复制到一个单独的存储设备(例如USB-stick)来实现的。建议复制这些文件的多个副本。

发送和接收加密货币

你钱包里最重要的部分是你的地址。你使用地址发送和接收硬币。几乎所有夹馍货币的地址都类似于:1 kdcn9xlvu3xnyr7ox64yjlw3kvkm1badm。

把这当作你的银行账号。这些字符串也可以通过qr代码表示。qr代码在移动钱包中得到了广泛的应用。加密货币交易有其唯一的交易代码，不能被撤销。一旦你把钱寄给某人，就不能反悔。

代表用户地址的QR密码和字符（移动钱包）

要使交易有效，需要通过网络进行验证。这个过程叫做“确认”。根据网络的负载情况，确认可能会持续几秒到几分钟。对于每笔交易，用户都要支付少量费用。费用可能从1美分到几美分不等，有时甚至是1美元，它会自动从你的余额中扣除。

许多钱包提供了一个机会，让你看到你的比特币余额为美元或欧元等值。这样您就可以输入您想要发送给某人的美元或欧元的金额，而钱包将自动计算交易所需的比特币数量。

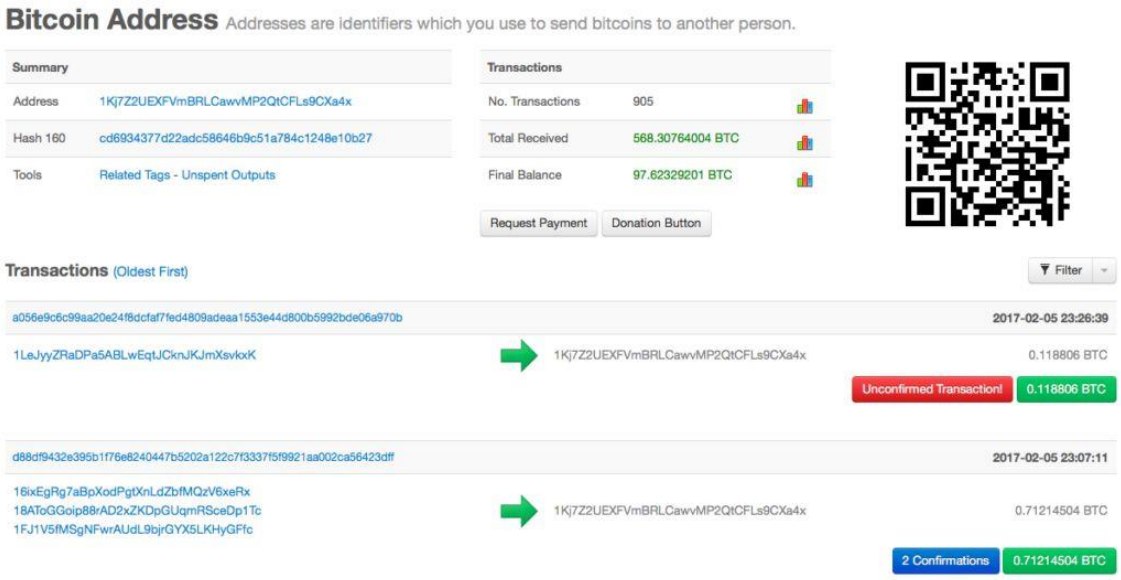
跟踪区块管理器上的交易

区块链是包括比特币在内的任何加密货币的主干。几乎所有的加密货币都是在公共区

块链上运行的。此外，比特币区块链上的每一笔交易都可以通过访问所谓的区块链管理器来保存，任何人都可以在线查看。这些管理器是在网络上显示交易的实时反馈的网站。

要跟踪交易，可以将交易代码粘贴到搜索框中。这些交易代码对于每个交易都是唯一的，并且显示在钱包中。另一种跟踪交易的方法是将地址粘贴到搜索框中。这样，资源管理器显示与此地址关联的所有传入和传出交易。

区块链管理器可以用于不同的数据，例如在区块链上的总交易数或唯一的比特币地址数。(区块链管理器示例:Blockchain.info)



来源： https://blockchain.info

投资比特币常见问题解答

第一次投资比特币时会有很多问题，我们将设法解决。

在我们的比特币投资FAQ里，人们最常问的问题。

❑我可以买少于1个比特币吗?是的!

每一个比特币都能被小数点后的第8位所分割。

你可以购买价值不到一美分的0.00000001比特币。

❑BTC是什么?

BTC是比特币的货币代码，就像美元对美元一样。

❑Satoshi是什么?

Satoshi是比特币0.00000001的最小单位。

它是以比特币的发明者中本聪(Satoshi Nakamoto)的名字命名的。

❑有比特币供应限制吗?

是的。

比特币是通过挖币的过程创建的。

每次创建新的区块时，都会创建一个固定速率的比特币。每10分钟创建一个块。

2009年区块的奖励是50个BTC，每四年就减少一半。目前，区块奖励设定在12.5 BTC。

比特币的开采——比特币的总供应量仅为2100万比特币。

这个限制被硬编码到协议中，不能更改。

用你自己的方式改变供应就等于攻击比特币网络。

❑我在哪里可以买到比特币呢?

能购买比特币的最常见的地方是网上加密货币交易所。需要通过提供你的身份证进行注册，在获得批准后，可以使用银行账户或信用卡以及法定货币，如美元、欧元、人民币等。

❑比特币钱包是什么?

比特币钱包是存储用户私钥的软件。

你的比特币钱包允许你访问比特币。

每当你想要发送或接收比特币时，这些钱包就会与比特币网络进行通信。

请注意:比特币没有储存在你的钱包里!

只有你的私钥储存在你的钱包里。

如果你丢失了私钥，你就失去了对比特币的访问权，再也无法访问它，它将永远丢失。

❑私钥是什么?

你的钱包永远不会储存比特币。

钱包的唯一目的是保持你的私钥，并与比特币网络进行通信。私钥是一长串随机数和字母，它总是与一个比特币地址配对。它创建了签名，需要通过证明您是该事务中使用的资金的所有者来使用您的资金。

失去对私钥的访问权等于把你的钱放在火上!

一定记得备份你的私钥!

❑ 哪一种比特币钱包最安全?

不同类型的钱包提供不同程度的安全保障。

在可用性和可访问性之间存在权衡。

最不安全的钱包是在线钱包，最安全的钱包是硬件钱包，纸质钱包也被称为“冷藏”。

❑一些交易所交易BTC 对USDT。USDT是什么?

像Poloniex这样的在线交易所不会使用真正的美元进行交易。

他们使用USDT代替美元，这是一种很容易交换的P2P，就像比特币一样。

USDT是一个资产支持的标志，这意味着USDT的每个单位都有一个真正的美元支持。USDT的单位称为tethers。每一个代表一个真正的美元。

一些交易所更喜欢使用USDT，因为与实际的美元相比，集成更容易。

与国际银行转账不同的是，Tether令牌也在国际上转换几乎不需要花费。

❑如何开始交易比特币?

在加密货币网上交易注册。

在这样的平台上注册需要用户发送他们身份证的副本。根据用户的流入，验证过程可能需要几周的时间。

比特币交易所的例子:Bitstamp, Gdax, Kraken, Gemini, Bittrex。

❑有比特币的首席执行官吗?

比特币是一个分散的自治组织(DAO)，由社区管理。比特币缺乏传统的自上而下的结构。比特币不是在任何国家注册的公司。比特币是一种生活在互联网上的软件协议。

❑交易费用是什么?

每次用户发送比特币时，必须支付交易费。

这些费用不是固定的，取决于网络负载。

如果有一个巨大的交易，交易费用会相应增加。

目前，比特币网络可以处理少量交易，任何使用量的增加都反映在收费价格上。

比特币社区正致力于解决这个问题。

❑为什么比特币交易费用这么高?

比特币的收费是动态调整的。

当使用增加时，费用相应增加。

❑融资融券交易是什么?

融资融券交易实质上是用借来的资金进行交易，而不是你自己的。

当你下一个保证金订单时，你所使用的所有资金都是从其他用户那里借来的，这些用户提供他们的资金作为点对点贷款。

你的保证金账户里的资金只能作为这些贷款的抵押品，并将债务偿还给贷款人。

来源:Poloniex

❑比特币市值如何计算什么?

加密货币的市值可以让人对该市场的大小有所了解。

目前的比特币市值约为410亿美元。

为了计算它，你需要将今天的价格乘以总硬币供应量。

市场上限=价格x循环供应。

$41 538 444 951 = $2526.85 x 16 438825 BTC。

❑BTC价格图表在哪里可以看到?

Bitcoinwisdom

Coinigy

❑比特币有什么支持吗?

比特币没有任何支持。

它的价格由市场决定。

❑为什么比特币有价值即使它没有任何东西支持呢?

比特币之所以有价值，是因为其作为数字资产的特性:

——供应有限。

——简单的存储。

——容易转移。

-它不是由中央银行控制的。

-人们接受它作为一种货币来换取商品。

如何参与ICO？

最初代币发行(ICOs)或令牌销售受到了机构投资者和个人的广泛关注。ICOs指的是新的ipo或下一代众筹。但是区块链的生态系统还很年轻，缺乏标准，因此代币的销售参与对普通人而言有较大的障碍。在这篇文章中，我们解释如何通过一步一步的引导来参与代币的销售。

现在大多数的ICOs都是通过一个智能契约运行在Ethereum区块链之上的，它收集了Ethereum令牌，并自动交换这些标记，以获得新成立公司提供的新令牌。整个过程完全是P2P，没有任何交易所或经纪人作为中间人。每个ICO都有不同的定价机制。

步骤1:在加密货币交易所注册

要参与ICO，你需要加密货币，通常是以太或比特币。你不能用法定货币参加一个ICO。如果你没有加密货币，你首先需要购买。购买大量比特币的最佳方式是通过在线交易所。从您的银行帐户转帐到新创建的帐户和一个加密货币交易所。请注意，由于严格的KYC和AML规定注册过程可能需要几天。如果你没有银行账户，或者不想放弃你的隐私，把你的身份证发送给像Coinbase这样的第三方，还有其他的选择，比如从ATM机或从其他人那里购买比特币。更多信息请阅读我们关于如何购买比特币和其他加密货币的教程。

第二步:将虚拟货币换成比特币或以太币

一旦你注册了一个账户，你的银行账户里的钱已经到了，你可以用你的欧元、美元等兑换你想购买的加密货币。这个过程需要几秒钟。您的加密货币将被发送到您注册的交易所提供的在线钱包。在网上保存大量的货币可能是危险的，因为在线交易容易受到攻击。过去存在资金从网上交易所中被盗的例子。因此，建议你将加密货币发送到所控制的钱包中。有关如何安全地存储你的货币，请阅读我们关于如何购买比特币和其他加密货币的教程。

第3步:将你的货币从交易所转移到你控制的区块链钱包

另一个让你把货币转移到钱包的原因是代币的销售参与。除非交易所允许你的在线钱包参与特定的ICO，否则一般规则是不会从交易所钱包中发送资金的，因为将无法访问新的令牌。这意味着，如果你使用一个随机的在线钱包参与ICO，并把钱寄到ICO地址，你就不会收到你买的令牌，这等于失去你的投资。如果这发生在你身上，联系技术支持并尝试解决问题。请注意，大多数交易所目前都有大量的请求，而且大部分客户服务都很糟糕。此外，交易所可能没有义务根据其“使用条款”来处理您的请求。

第四步:设置你的钱包

如今，大多数代币销售都发生在Ethereum网络上。因此，您将需要一个Ethereum钱包参与令牌销售。不是每个钱包都适合ICOs。最容易使用和被广泛接受的Ethereum钱包是MetaMask和MyEhterWallet。MetaMask是谷歌Chrome浏览器的插件。它不仅是一个钱包，而且是一个轻量级的Ethereum dApp浏览器。MyEtherWallet是一个客户端钱包，不保存您的私钥。它还连接了硬件钱包，如:Nano S或Trezor。根据设置和ICO，ICO可能会指定钱包。如果该公司没有为指定首选钱包，我们建议使用MetaMask。

MetaMask是一个桌面类型的钱包，我们不建议在它里面存储大的值。使用它只适用于ICO，然后将你的资金转移到一个更安全的地方，如硬件钱包或纸袋。不要忘记备份你的钱包，把12字密码储存在一个安全的地方(而不是在云里)。在你的钱包被适当的设置和备份后，从你的在线交换帐户发送到你的MetaMask钱包。

步骤5:购买ICO代币

在开始之前，请务必阅读ICO和代币购买协议的一般条款。大多数创业公司都为象征性的销售参与提供了一步一步的指导，包括每一步的屏幕截图，务必记得阅读这些。你也可以加入社交媒体，包括Slack或Telegram，并关注ICO的新闻。有时代币销售会遇到技术上的问题，在代币销售过程中保持消息的更新是至关重要的。 所有的ICOs都是在特定的时间或指定的区块开始的。您可以使用Ethereum资源管理器来检查区块。如果有开始时间，请确保您转换了时差。需要注意的是，一些ICOs在几分钟内就结束了。因此，如果您希望代币销售快速结束，可以使用像Parity这样的钱包，这样可以提供更高级的设置选项。当代币销售开始时，您需要将货币发送到团队指定的地址。您需要设置一个适当的价格限制，由MetaMask控制。在您发送交易之后，有几个场景:

❑令牌销售结束后马上收到代币

❑你需要等待几天才能收到代币

❑您将需要手动赎回代币

需要注意的是，在某些情况下,黑客会操纵ICO网站,将他们的地址与真正的ETH地址进行交换,这意味着投资者获得的地址是错误的，他们的钱落入了黑客手中，而不是ICO团队。

步骤6:保护令牌

在 MyEtherWallet收到货币之后，确保将这些货币被转移到一个更安全的钱包。你需要在钱包里存一些额外的ETH(小金额)来支付从钱包到钱包的交易费用。请注意，一旦Ethereum更新，这些程序就会改变，但目前仍需牢记。

附录:

第一版

2017年9月30日

版权: Creative Commons - Attribution, Share Alike

作者: Shermin Voshmgir, Valentin Kalinov

出版商: https://blockchainhub.net/

此书可免费阅读并会定期更新

最新版网址: https://blockchainhub.net/blockchain-technology

如果你愿意为我们的活动捐款，以下为我们的捐款方式:

Paypal: hello@blockchainhub.net

比特币: 1NFwzutctYkY88Ak8Ybovcypu58fdWvBp5

如果你对此书有任何建议和疑问，欢迎联系: hello@blockchainhub.net

请注意:

区块链和其他去中心化网络技术仍在发展的初始阶段，相关技术、案例和公司都在飞速发展。虽然我们尽可能以概述为主，但仍不排除在出版该书后，部分信息已被迭代更新。