什么是智能合约?

币学院 副船长 船龄 3.4年 2018-05-03 17:49:00 来源 ethfans

智能合约是 1990s 年代由尼克萨博提出的理念，几乎与互联网同龄。由于缺少可信的执行环境，智能合约并没有被应用到实际产业中，自比特币诞生后，人们认识到比特币的底层技术区块链天生可以为智能合约提供可信的执行环境，以太坊首先看到了区块链和智能合约的契合，发布了白皮书《以太坊：下一代智能合约和去中心化应用平台》，并一直致力于将以太坊打造成最佳智能合约平台，所以比特币引领区块链，以太坊复活智能合约。

怎样向尚未接触过比特币理念的人介绍以太坊及智能合约在金融合约方面的应用？下面是一种尝试。首先介绍区块链，解释它为什么值得人们的信任，其次介绍智能合约，然后介绍以太坊系统，最后介绍智能合约与金融合约的结合。

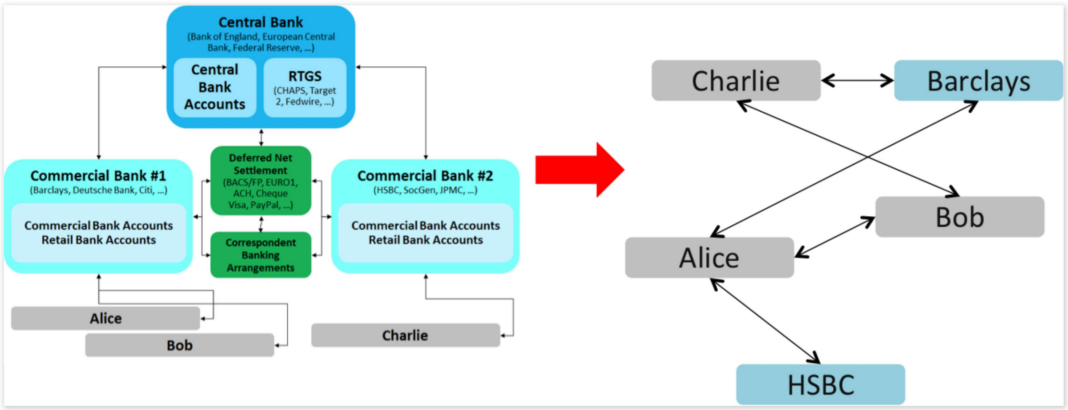
比特币的共识机制

比特币的核心技术区块链可以理解成可复制、共享的账本。

比特币的最核心创新：它教会世界如何在不需要信任第三方的情况下远距离转移价值。

人们当然可以面对面地转移实体纸币，但是，在比特币出现以前，我们做不到：在不需要信任中心化第三方机构（邮局、银行等）的情况，远距离向某人转移价值。

就好像银行和支付系统的传统转账模式的基础设施被重构为点对点支付网络。这种转变如下图所示：



比特币打开了点对点的电子价值转移模式的大门，完全不同于现在的银行系统、中央银行和支付系统。 但是，上面的图并没有解释比特币是怎样实现点对点价值转移的。

答案是：比特币系统建立在“可复制、共享的账本”之上。比特币网络中的每个参与者（完全节点）拥有一个完整的交易账本的副本，这一系统的神奇之处在于：它是如何做到使每个人的副本与其他人的副本保持一致的。

所以，正确的示意图应该是下图，每个参与者都能够从相同的可复制、共享的账本中获取信息。

推荐教程

深度解析POS和POW的区别

以太坊的挖矿机制是怎样的?

怎样找回因转账0确认而卡住的比特币

喵懂区块链20期 | 不可能三角，区块

区块链引子+智能合约+Solidity

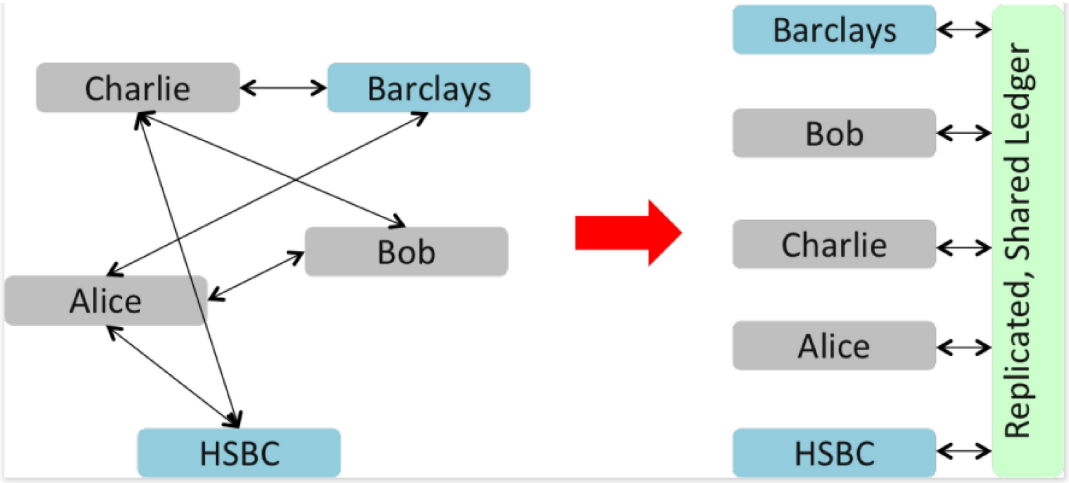
瑞波币RippleTrade身份认证图文教

比特币挖矿收益分析——几种场景下

深入浅出比特币交易 (transaction)

比特币交易网站BtcChina的使用指南

比特币地址和私钥是怎样生成的?



比特币和其它去中心化共识系统的窍门在于：它们怎样保证每个有一个账本的副本，并使每个人确信自己的账本与别人的账本是同步的。

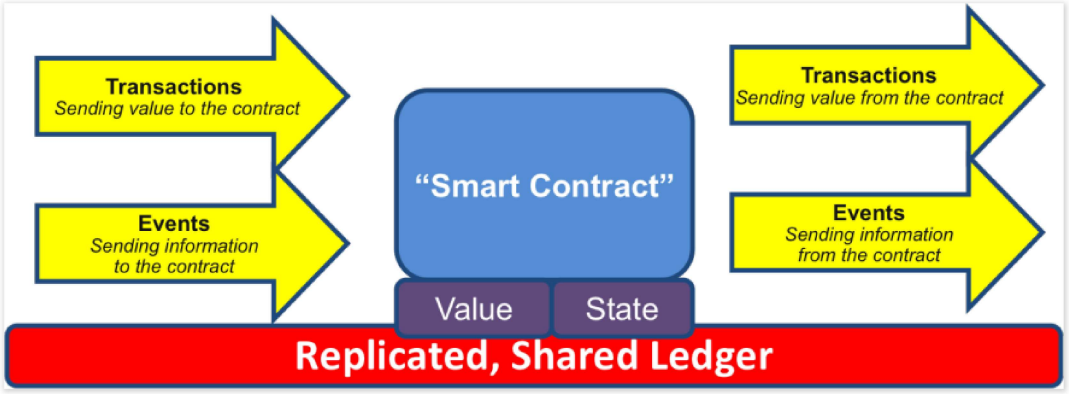
如果每个人拥有的账本的副本是相同的，那么人们就不再需要一个中心化的机构记录谁拥有什么。当你的账本更新，记录一笔新的资产所有权变动时，其他人的账本也会发生相同的变动。

智能合约

智能合约程序不只是一个可以自动执行的计算机程序：它自己就是一个系统参与者。它对接收到的信息进行回应，它可以接收和储存价值，也可以向外发送信息和价值。

这个程序就像一个可以被信任的人，可以临时保管资产，总是按照事先的规则执行操作。

下面这个示意图就是一个智能合约模型：一段代码（智能合约），被部署在分享的、复制的账本上，它可以维持自己的状态，控制自己的资产和对接收到的外界信息或者资产进行回应。



智能合约模型：它是运行在可复制、共享的账本上的计算机程序，可以处理信息，接收、储存和发送价值。

以太坊系统

以太坊项目借鉴了比特币区块链的技术，对它的应用范围进行了扩展。如果说比特币是利用区块链技术的专用计算器，那么以太坊就是利用区块链技术的通用计算机。简单地讲，以太坊 = 区块链 + 智能合约。

与比特币相比，以太坊最大的不同点是：它可以支持更加强大的脚本语言（用技术语言讲就是图灵完备的脚本语言），允许开发者在上面开发任意应用，实现任意智能合约，这也是以太坊的最强大之处。作为平台，以太坊可以类比于苹果的应用商店，任何开发者都可以在上面开发应用，并出售给用户。

以太坊智能合约的金融应用

每一类金融合约都可以程序代码的形式写成智能合约。

差价合约

金融衍生品是 "智能合约" 的最普遍的应用，也是最易于用代码实现的之一。实现金融合约的主要挑战是它们中的大部分需要参照一个外部的价格发布器；例如，一个需求非常大的应用是一个用来对冲以太币（或其它密码学货币）相对美元价格波动的智能合约，但该合约需要知道以太币相对美元的价格。最简单的方法是 通过由某特定机构（例如纳斯达克）维护的 "数据提供 "合约进行，该合约的设计使得该机构能够根据需要更新合约，并提供一个接口使得其它合约能够通过发送一 个消息给该合约以获取包含价格信息的回复。

当这些关键要素都齐备，对冲合约看起来会是下面的样子：

等待A输入1000以太币。

等待B 输入1000以太币。

通过查询数据提供合约，将1000以太币的美元价值，例如，x美元，记录至存储器。

30天后，允许A或B“重新激活“合约以发送价值x美元的以太币（重新查询数据提供合约，以获取新价格并计算）给A并将剩余的以太币发送给B。

代币系统（token system）

区块链上代币系统有很多应用，从代表如美元或黄金等资产的子货币到公司股票，单独的代币代表智能资产，安全的不可伪造的优惠券，甚至与传统价值完全没有联系的用来进行积分奖励的代币系统。在以太坊中实施代币系统容易得让人吃惊。关键的一点是理解，所有的货币或者代币系统，从根本上来说是一个带有如下操作的数据库：从A中减去X单位并把X单位加到B上，前提条件是(1)A在交易之前有至少X单位以及(2)交易被A批准。实施一个代币系统就是把这样一个逻辑实施到一个合约中去。

储蓄钱包

假设Alice想确保她的资金安全，但她担心丢失或者被黑客盗走私钥。她把以太币放到和Bob签订的一个合约里，如下所示，这合同是一个银行：

Alice单独每天最多可提取1%的资金。

Bob单独每天最多可提取1%的资金，但Alice可以用她的私钥创建一个交易取消Bob的提现权限。

Alice 和 Bob 一起可以任意提取资金。

一般来讲，每天1%对Alice足够了，如果Alice想提现更多她可以联系Bob寻求帮助。如果Alice的私钥被盗，她可以立即找到Bob把她 的资金转移到一个新合同里。如果她弄丢了她的私钥，Bob可以慢慢地把钱提出。如果Bob表现出了恶意，她可以关掉他的提现权限。

作物保险

一个人可以很容易地以天气情况而不是任何价格指数作为数据输入来创建一个金融衍生品合约。如果一个爱荷华的农民购买了一个基于爱荷华的降雨情况进行反向赔付的金融衍生品，那么如果遇到干旱，该农民将自动地收到赔付资金而如果有足量的降雨他会很开心因为他的作物收成会很好。 多重签名智能契约

多重签名智能合约

比特币允许基于多重签名的交易合约，例如，5把私钥里集齐3把就可以使用资金。以太坊可以做得更细化，例如，5把私钥里集齐4把可以花全部资金，如果只3把则每天最多花10%的资金，只有2把就只能每天花0.5%的资金。

下一篇： **UUPool双优矿池BTM挖矿教程**

全部 最佳

hahahehei 副船长 船龄 **2.3年** 2018-05-04 17:48:52

这个不错啊，区块链普及的东西很适合我这种小白

巴比特学院是巴比特旗下的教育培训品牌，由巴比特主办，与专业培训机构合作，邀请业内区块链专家和实践者作为培训导师，通过导师现场授课、行业高端论坛、企业调研走访等方式，打造国内一流区块链培训品牌，推动区块链在中国的发展与创新。2018年，巴比特学院的品牌影响力将向杭州以外的北京、上海、南京、成都、深圳、广州等地辐射。