大家好，今天小编来为大家解答区块链 零知识证明这个问题，区块链零知识证明应用很多人还不知道，现在让我们一起来看看吧！

本文目录

什么是区块链共识机制？

共识机制是什么？

由于点对点网络下存在较高的网络延迟，各个节点所观察到的事务先后顺序不可能完全一致。

因此区块链系统需要设计一种机制对在差不多时间内发生的事务的先后顺序进行共识。这种对一个时间窗口内的事务的先后顺序达成共识的算法被称为“共识机制”。

币姐插播

在区块链系统当中，没有一个像银行一样的中心化记账机构，保证每一笔交易在所有记账节点上的一致性，即让全网达成共识至关重要。共识机制解决的就是这个问题。

PoW和PoS优缺点

币姐解释

目前主要的共识机制有工作量证明机制PoW和权益证明机制PoS。

PoW(什么是PoW?)

PoW通过评估你的工作量来决定你获得记账权的机率，工作量越大，就越有可能获得此次记账机会。

PoW即工作量证明，它的优点是：

算法简单，容易实现；节点间无需交换额外的信息即可达成共识；破坏系统需要投入极大的成本；

它的缺点：

浪费能源；区块的确认时间难以缩短；新的区块链必须找到一种不同的散列算法，否则就会面临比特币的算力攻击；容易产生分叉，需要等待多个确认；永远没有最终性，需要检查点机制来弥补最终性；

PoS(什么是PoS?)

PoS通过评估你持有代币的数量和时长来决定你获得记账权的机率。这就类似于股票的分红制度，持有股权相对多的人能够获得更多的分红。

DPOS与POS原理相似，只是选了一些“人大代表”。与PoS的主要区别在于节点选举若干代理人，由代理人验证和记账。

PoS即权益证明，它将PoW中的算力改为系统权益，拥有权益越大则成为下一个记账人的概率越大。

这种机制的优点是不像Pow那么费电。

它的缺点：

没有专业化，拥有权益的参与者未必希望参与记账；容易产生分叉，需要等待多个确认；永远没有最终性，需要检查点机制来弥补最终性；

币姐插播

随着技术的发展，未来可能还会诞生更先进的共识机制。

如果觉得好，觉得给我点赞哦~！

更多区块链的知识，可以关注币姐的公众号：币姐说（bjiebtc）

各位能不能用通俗易懂的法子帮我解释一下什么是区块链？

“

最近网络上在热炒区块链概念，我也抱着凑热闹的心态跟着了解学习了一些。

区块链到底是什么？

简单的说，区块链就是一个去中心化的信任机制。

最近我个人正在学习区块链方面的相关知识。通过学习，对区块链也有了一定的认识。也让我感觉到人类的智慧的伟大，区块链将继互联网之后，再一次改变人类生活。

那么到底什么是区块链技术，区块链该如何去理解呢？

其实区块链不能单纯的叫区块链，应该叫做区块链技术。

区块链技术就指的一种全民参与记账的方式。所有参与记账的人都是一个数据库，你可以直接把数据库看成一个账本。区块链就是一个账本与一个账本相互链接而又独立存在。

那么您对区块链有了一定认识厚。你肯定会就会问，这种全民记账的方式有什么好处呢？

安全，肯定是安全。因为这种记账方式首先是去中心化，没有中央大账本，就无法篡改和摧毁。其次就是无法作弊，你想每个人都有一本账本，按照少数服从多数的原则。你就要至少所有账本中的51%的账本进行统一修改。全世界有多少账本，或者有多少台记账的计算机，要改掉其中的51%能实现么？

没有中心化的中介机构存在，让所有东西都通过预先设定的程序自动运行，不仅能大大降低成本，也能提高效率，而且由于每个人都有相同的账本，能确保记录过程是公开透明的。

就拿目前最热的比特币来说，其实区块链技术就是比特币的最底层技术，比特币在没有任何中细化机构运营和管理的情况下，多年来一直运行非常稳定。没有出现过任何问题。所以有人注意到他的底层技术，把比特币技术抽象的提取出来，就称之为现在的区块链技术，也有很多人称之为分布式账本技术。

虽然区块链技术的提出或者说概念上其实不难理解。但是在实际运用中该如何运用呢？或者说哪些行业可以用到区块链技术呢？

区块链主要的优势就是无需中介参与，过程高效透明且成本极低，数据高度安全、

如果在这三个方面有任意一个需求的行业都有寄回使用区块链技术。

比如金融行业，金融行业目前由于防止单点故障和系统性风险，需要进行层层审计来控制金融风险，但由此会付出高昂的内部成本。在这种情况下，区块链技术能够通过防止篡改和高透明的方式让整个金融系统极大的降低成本。

根据西班牙最大银行桑坦德发布的一份报告显示，2020年左右如果全世界的银行内部都使用区块链技术的话。大概每年能省下200亿美元的成本。这样的数据足以说明区块链给传统金融领域带来的巨大变革和突破。

所以如果所有金融系统能够实现区中心化的实时结算和清算，不仅将极大的提高全球金融效率，并且由此能够改变全球金融格局。传统的快过结算就是因为要通过类似于SWIFT这样的机构，所以跨国电汇往往是按天来计算的。但是比特币在使用区块链技术时，在完全没有中心化运营机构的情况下，完美的运行了7年，不仅能够实现实时结算，而且没有出现过任何一笔账目错误。

对于区块链来说，挖矿是必须的吗？

你对区块链的理解有点偏。以比特币为代表的虚拟货币只是区块链的一种具现化应用形式，想要货币虚拟币又不想投入太多资金挖矿就成了最好的方式。然而区块链的应用在未来拥有很大的空间，挖矿对于虚拟币来说只是一种获取渠道，对于整个区块链行业来说只是冰山一角

区块链时代，如何保障资产安全？

在数据共享时代，隐私保护已成为一个日益严峻的问题。我们需要在大数据和绝对隐私之间找到平衡点，以便在信息使用的过程中保护我们的隐私。

特别是在中心化经济模式中，资产处于透明和非自主状态，我们花的每一分钱都是可追溯的，我们的资产安全面临着巨大的挑战。

BTC的出现让我们看到对资产的尊重，隐私和安全的希望。然后，随着中心化的干预和对交易平台信息及其严格的管理，BTC的隐私性不断弱化。近年来，各种具有高度匿名性的加密货币在市场中流行开来，我们不得不承认，市场对匿名交易有着强劲的需求。

通过匿名交易提高资产隐私的需求日益增加，因为只有通过匿名交易才能保证我们更高效，更自由地保护资产。当我们对资产拥有绝对的控制和自主权时，财务才能为人类带来更多的希望。

匿名交易不仅从根本层面保障了资产安全，也为资金流提供了更多的应用场景。在很多时候，我们需要一种隐秘的方式来进行收付款。匿名交易可以避免不必要的风险，尤其对于资金流通需要更高安全防护手段的大型商业活动来说，他是一项不可或缺的功能。

从技术上讲，联盟链使用ZcashSapling版本的零知识证明进行匿名交易，这是一种经过实战，非常彻底的匿名方式。这类匿名交易的隐私保障源于屏蔽交易可以在区块链上完全加密，但仍然可以通过使用零知识证明在网络一致性规则下验证为有效。

也可以认为，这相当于我们给账本中的账目进行了拍照，然后将账目页撕掉销毁。没人知道资金的去向，但我们手中的照片可以证明我们拥有这笔资产，可以被总帐本认可的资产存在与归属。零知识证明是一种证明方式，人们可以证明他们拥有某些信息，同时泄漏该信息，并且之间没有任何交互。“零知识”证明允许一方（证明者）向另一方（验证者）证明该陈述是真实的，并不会泄漏超出陈述本身有效性的任何信息。例如，拟定一个随机数的散列，证明者可以向验证者正式确实存在具有该散列值的数字，而不是去揭示它是什么。

在零知识的“知识证明”中，证明者不仅可以使验证者确信该数字存在，而且实际上他们知道这样的数字，而不会去泄漏有关该数字的其他信息。“简洁”的零知识证明可以在几毫秒内得到验证，证据长度只有几百字节，即使对于非常大的程序的陈述也是如此。在第一个零知识协议中，证明者和验证者需要来回传递多轮验证。但是，在“非交互式”构造中，证明包括从证明者发送到验证者的单个消息。目前，产生非交互性且足够短发布到区块链的零知识证明，最有效的已知方式是具有初始设置阶段，其生成在证明者和验证者之间共享的公共参考串。

用户可以在联盟链中实现对私有财产的绝对隐私。通过这种方式，我们可以完全隐藏双方的目标交易信息，并通过零知识证明实现绝对匿名，从而进一步确保信息的安全性。

联盟链中的匿名交易还使得联盟链具备了能够充当“现金”货币的职能，这也将衍生出更多的应用场景。同时，公开账本与隐私保护的彻底融合，也能够让用户更透明、自主的参与到社会以及金融的活动中。

文章到此结束，如果本次分享的区块链 零知识证明和区块链零知识证明应用的问题解决了您的问题，那么我们由衷的感到高兴！