很多朋友对于区块链到的安全性和区块链的安全性不太懂，今天就由小编来为大家分享，希望可以帮助到大家，下面一起来看看吧！

本文目录

区块链技术在保险方面有什么应用？

区块链技术的可溯源性、分布式记账的属性，被许多从事保险领域的企业重点关注。中国人民财产保险股份有限公司执行董事王和曾多次在保险论坛上表示，保险与区块链的基因是十分相似的。区块链本身具备的加密技术和全网共识的机制，本身具备的不可篡改、分布式储存等技术，能让保险行业的资金和信息进行安全的储存。区块链的最大特点就是基于社会性的管理，这与保险行业的特性是共通的，因为保险行业的特性也是社会性的，两者天然存在密切的联系。

虽然目前有许多保险行业巨头已经着手布局区块链在保险行业的相关应用，但他们仍然停留在技术层面，研究如何利用区块链技术将保险的信息、客户的信息以及理赔的信息储存在区块链上，以保证其安全性。从现在保险行业实现真正区块链项目落地就可以发现，如今保险行业真正落地的项目少之又少，一些中小型保险企业还是停留在观察的阶段。

区块链技术与保险行业的融合应用，一方面能够保证数据信息的公开性、安全性，让保险公司更好地进行风险定价，另一方面也能考验保险公司的风险定价能力。区块链技术在保险行业的应用，或将有效缩短保险行业理赔的时间，保证客户信息的安全。

区块链在供应链金融的应用的优势

区块链在供应链金融中的应用可以带来多重优势：

区块链可以解决信息孤岛问题，实现多个利益相关方之间的数据共享和互通。

区块链可以提高供应链金融的透明度和可信度，降低交易成本和风险。

区块链可以为中小企业提供信用担保，促进贸易便利化和金融普惠。

区块链可以实现智能合约自动清算，减少人工干预，降低操作风险。

区块链可以促进供应链上下游企业的协同合作，提高整个供应链的效率和灵活性。

因此，区块链技术在供应链金融领域的应用前景广泛，有望为行业带来更多创新和价值。

区块链有何安全问题？

著名咨询公司Gartner在预测2018年对大部分企业公司影响显著的十大战略技术时，将区块链列为十大关键技术之一。2017年最近的普华永道国际会计事务所（PwC）对全球金融科技调研结果显示，区块链技术正快速从实验阶段迈向企业应用阶段。区块链技术融合了分布式架构、P2P网络协议、加密算法、数据验证、共识算法、身份认证、智能合约等技术，利用基于时间顺序的区块形成链进行数据存储，利用共识机制完成各节点之间数据的一致性，利用密码学体制保证数据的存储和传输安全，利用自动化的脚本建立智能合约，实现交易的自动判断和处理，解决了中心化模式存在的安全性低、可靠性差、成本高等问题。本文重点分析了区块链技术的安全特性和应用区块链提升网络空间安全的方法，并给出了区块链应用面临的安全挑战。

1区块链工作过程

区块链的基本工作过程如图1所示，当节点A向节点B转账时，产生的交易信息会以区块的形式以P2P的方式广播到网络中所有有效节点，节点通过共识机制对该区块进行认证，当该区块的正确性和有效性被认可后，该区块按顺序被添加到网络现有区块链中，A向B的转账完成。由于区块链中的信息得到了网络中大部分节点的一致性认同，因此该信息是无法擦除和篡改的，且所有节点都可以读取和查询交易信息。

图1区块链工作过程实例

2区块链具备优越的安全特性

区块链解决了在不可靠网络上可靠的传输信息的难题，由于不依赖与中心节点的认证和管理，因此防止了中心节点被攻击造成的数据泄露和认证失败的风险。区块链以其数学算法和数据结构，相比传统网络安全防护具有以下特点：

（1）共识机制代替中心认证机制。传统网络的用户认证采用中央认证中心（CA）方式，整个系统的安全性完全依赖于集中部署的CA认证中心和相应的内部管理人员

身上。如果CA被攻击，则所有用户的数据可能被窃取或者修改。而在区块链节点共识机制下，无需第三方信任平台，写入的数据需要网络大部分节点的认可才可以被记录，因此，攻击者需要至少控制全网络51%的节点才能够伪造或者篡改数据，这将大大增加攻击的成本和难度。

（2）数据篡改“一发动全身”。区块链采用了带有时间戳的链式区块结构存储数据，为数据的记录增加了时间维度，具有可验证性和可追溯性。当改变其中一个区块中的任何一个信息，都会导致从该区块往后所有区块数据的内容修改，从而极大增加数据篡改的难度。

（3）抵抗分布式拒绝服务（DDoS）。区块链的节点分散，每个节点都具备完整的区块链信息，而且可以对其他节点的数据有效性进行验证，因此针对区块链的DDoS攻击将会更难展开。即便攻击者攻破某个节点，剩余节点也可以正常维持整个区块链系统。

3区块链可用于增强网络空间安全

区块链技术以其去中心化结构具备的安全特性，已被国外金融、医疗、互联网等领域各大公司用来提升网络安全。

（1）管理和保护用户认证数据。麻省理工大学推出的虚拟货币CertCoin最先采用了基于区块链的公钥基础设施，摒弃传统中心认证方式，采用公共密钥实现分布式节点之间的互相认证，从而防止网络单点故障。乌克兰公司Ukroboronprom与网络安全公司REMME合作，通过在区块链上管理用户认证相关数据，几乎完全阻断了黑客使用虚假认证消息获取用户身份的可能。

（2）提高网络数据安全。全球最大规模的区块链公司Guardtime通过分布节点之间协商来提供区块链上数据的机密性和完整性，实现了爱沙尼亚100万份用户医疗数据的安全性保证。美国国防部高级研究计划局DARPA也开始采用该方式为军方敏感性数据提供安全保护。

（3）有效阻止DDoS攻击。区块链初创公司Nebulis目前正在开发基于区块链的分布式互联网域名系统，只允许授权用户来管理域名，其他公司诸如Blockstack和MaidSafe也开始使用分布式Web技术，替代原有第三方管理Web服务器和数据库的模式，从而阻止网络DDoS攻击。

（4）增强物联网安全。通过智能合约模式，区块链一方面可以利用P2P网络中的网络设备节点对待接入设备进行鉴权；另一方面可以有效抵挡物联网DDoS攻击。在2016年爆发的Mirai僵尸网络DDos攻击事件中，大规模的物联网设备被入侵，致

使大半美国网络瘫痪。在区块链系统中，当某个节点被入侵时，其他设备会检测到该设备异常，并且将其列为异常和不信任节点，从而将其排除。

4区块链应用面临诸多安全风险

虽然区块链以其天然的技术特点具有用户认证、保护数据、防DDoS攻击等安全优势，但现阶段区块链技术还不成熟，在实际应用时仍然存在诸多安全风险。

（1）区块数据可靠性随时间降低。早期生成的区块由于当时使用的算法过时或者密钥长度不够，此部分交易历史有可能会被篡改伪造。由于区块链采用关系型的数据结构，而且现有机制还没有删除历史交易数据的机制，将会导致新产生的区块也不可以被信任。此外，所有交易记录不断累加也会造成节点超负荷，增加安全隐患。

（2）配套软件可能存在漏洞隐患。由于区块链系统由代码维持，攻击者会通过系统中存在的漏洞恶意篡改或者盗取数据。在2016年的TheDao事件中，由于以太坊智能合约程序存在严重漏洞，该合约筹集的公众款项不断被一个函数的递归调用转向它的子合约，被窃取了价值超过60万美元的以太币。2017年7月黑客同样利用以太坊智能合约漏洞盗取了超过约3000万美元的以太币。

（3）区块链可能会造福犯罪分子。基于区块链本身的匿名和安全特性，不法分子可能采用区块链技术来进行违法网络交易，例如暗网交易和洗钱犯罪。美国参议院已通过7000亿国防法案，其中就包含研究区块链技术潜在的安全风险，以及评估网络罪犯利用该技术造成的危害。

区块链具有可靠的信息交互，完整的数据存储、可信的节点认证等安全性特点，为网络空间安全提供了一种崭新的安全防护思路和模式，转变传统网络边界式防护为全网络节点参与的安全防护，通过分布式的节点共识机制来抵抗恶意节点的攻击，在网络空间安全领域具有极大的应用潜力。现阶段区块链技术还不成熟，系统仍然存在许多安全隐患和漏洞，在未来应用中，应加强区块链的监管和安全技术研究与实践，推动区块链产业应用的稳步发展，充分发挥区块链技术的安全优势，有效提升网络空间的安全防护水平。

举例子说明什么是区块链

区块链是一种分布式数据库，它由一系列按照时间顺序排列的数据块组成，并采用密码学方式保证不可篡改和不可伪造。区块链技术最初起源于比特币，作为比特币的底层技术，用于去中心化和去信任地维护一个可靠的数据库。区块链技术可以从比特币中分离出来，应用到各种不同的场景中。

举个例子，在一个村子里，有三个农民A、B、C，他们想合作生产面粉，但是他们之间不信任对方，担心自己提供的麦子会被对方偷走。这时，他们可以引入一个中心化的第三方机构，来监督他们的合作过程，保证他们的公平性。但是，这个机构也可能被收买或者作弊，无法保证他们的公平性。

现在，他们可以应用区块链技术来解决这个问题。他们可以把所有的麦子都放在一个共同的仓库里，并且把仓库的钥匙放在区块链上，每个人手上都有一个副本。每当有人想要取出麦子时，必须获得所有人的签名授权，并且把授权记录写在区块链上。这样，每个人都可以通过区块链查看仓库的当前状态，并且无法篡改记录。如果有人不遵守规则，就会被其他所有人知道，并且被排除在合作之外。

这就是一个简单的区块链应用的例子，它可以在没有中心化的第三方机构的情况下，实现多方的合作和信任。区块链技术还可以应用到其他各种场景中，例如金融、物流、医疗等。

好了，文章到此结束，希望可以帮助到大家。