大家好，今天小编来为大家解答超级暗网区块链这个问题，区块链能火多久？很多人还不知道，现在让我们一起来看看吧！

本文目录

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。

区块链是否是骗局？

所谓区块链就是资本家携手！挖掘社会财富资源！为了收割社会财富资源，除了抛出根本不可能兑现的红利分配诱饵，别无方法。因为世上绝对不会有什么资本家真

心带领平民百姓致富！

你怎么看待区块链技术？

区块链的本质是一个去中心化的信任机制，通俗来说，区块链相当于一种全民记账方式（分布式数据库），所有系统的背后都有一个数据库，数据库就类似一个大账本，每个人都可以来记账，所有人共同选定一份最好的记录正式写入账本（共识机制），并将账本的内容发给系统中所有的人进行备份；不存在保密的高级中心账本，自然也就不存在暗箱作弊修改/丢失遗漏数据的情况；每个人都有相同的账本，记录过程都是公开透明的，所以高度安全；同时无须第三方中介则大大降低成本，也能提高效率；存储在区块链上的交易信息是公开的，但是用户身份信息是高度加密的，只有被数据所有者授权后才可以访问该数据（非对称加密和授权技术），从而保证了数据的安全和个人的隐私。

区块链能火多久？

没那么高深，别听他们说的那么玄，区块链的最大作用不是虚拟币，而是信用记账体系，你现在用支付宝买东西就是信用体系。

你可以这么理解，假设有一笔交易，以支付宝的模式就是你付款成功的同时，就可以拿东西走了，其实支付宝充当了中介，见证了你和卖家，并做了担保。

区块链就是你有这次交易，记账的不是中介，而是其他用户，一群人为你做了见证，并把记录写进区块，然后很多区块构成链，这就是最简单的方式。

所谓虚拟币就是别人为你见证交易了，你总得付手续费吧，给现金转账都不可能，那就用虚拟信用吧，这就是虚拟币的作用，如果说区块链是一台永远运转的机器，虚拟币就是驱动的柴油。

至于火多久，一项新技术出来特别是区块链这种无法作弊的记账出来，会在很多领域取代可以被篡改的记录，比如个人或公司财务记录，信用记录，医疗记录，行车记录，健康记录，等等，多人记账保证了记录无法被篡改和真实性，可以说在某些特定领域，区块链会一直火下去，直到出现可替代的新技术为止。

关于本次超级暗网区块链和区块链能火多久？的问题分享到这里就结束了，如果解决了您的问题，我们非常高兴。