**关于区块链技术及其安全性的调查**

作者：Huaqun Guo, Xingjie Yu

摘要：区块链是一种具有去中心化、自治性、完整性、不变性、验证性、容错性、匿名性、可审核性和透明度等理想特性的技术。在本文中，我们首先对区块链技术进行了更深入的调查，特别是其历史、共识算法的定量比较、公钥密码学的细节、零知识证明、区块链中使用的哈希函数，以及区块链应用程序的综合列表。此外，区块链本身的安全性本文关注的一个重点。特别是，我们从风险分析中对区块链的安全性进行了评估，得出了全面的区块链安全风险类别，分析了针对区块链的真实攻击和bug，并总结了最近对区块链开发的安全措施。最后，提出了为大规模部署实现更可扩展和更安全的区块链系统的挑战和研究趋势。

1.介绍

在区块链中，数据被保存在一个分布式的分类帐中。区块链技术提供了完整性和可用性，允许区块链网络的参与者编写、读取和验证记录在分布式账本中的交易。但是，它不允许对交易和存储在其分类账上的其他信息进行删除和修改操作。区块链系统是由加密原语和协议，例如：数字签名、哈希函数等。这些原语保证了记录在分类账中的交易是受完整性保护、真实性验证和不可否认的。此外，作为一个分布式网络，为了让整个参与者就一个统一的记录达成一致，区块链技术还需要一个共识协议，它本质上是每个参与者都要遵循的一套规则，以实现全球统一的观点。

在不可信任的环境中，区块链为用户提供了理想的分散化、自治、完整性、不变性、验证、容错性，近年来吸引了学术和行业的广泛关注，匿名性、可审核性和透明度[1–3]。凭借这些先进的特点，区块链技术近年来引起了学术界和业界的极大关注。

帮助和帮助某人了解区块链技术和区块链安全问题，特别是对于使用区块链的用户。

进行交易，对于将开发区块链技术和解决区块链安全问题的研究人员，我们投入精力和时间对区块链技术及其安全问题进行全面的调查和分析。首先，我们识别关键词，即区块链、调查、共识算法、智能合约、风险和区块链安 全，以便在互联网上搜索出版物和信息。其次，我们调查了发表在顶级安全会议和期刊上的区块链相关论文，例如，USENIX安全研讨会、IEEE安全与隐私研讨会、IEEE交易期刊等。这样，我们已经调查了尽可能多的论文，以克服研究和结果的偏差。我们的调查论文介绍了来自其他研究工作的综合发现。

我们调查的主要贡献包括： 1)我们比较了各种共识算法与详细的分析和数字数字，提出了区块链的密码基础；2)提供了智能合约及其安全性的丰富信息；3)探索区块链技术的广泛应用，包括但不限于不同的加密货币；4)对区块链本身的安全风险、真实攻击、漏洞、根本原因和近期安全措施进行全面分析；最后但并非最不重要的是，5)本文总结并提出了挑战和研究趋势，以进一步努力开发区块链技术的大规模部署。

本文的其余部分组织如下：第2节介绍了概述。第3节详细描述了区块链 技术，包括区块链的共识算法、智能合约和密码学，而第4节则介绍了综合的区块链应用程序。对区块链的安全风险和真实攻击详见第5节，安全措施详见第6节。第7节分析了区块链所面临的挑战和研究趋势。第8节总结了相关的调查工作，以显示我们的贡献。最后，第9节总结了我们的工作。

2.区块链历史概述

1982年，乔姆是已知的第一个在博士学位中提出区块链协议的人。D.论文[4]。1991年，哈伯和斯托内塔描述了一个加密的[5]安全块链。1993年，拜耳等人。将Merkle树纳入设计[6]。1998年，Szabo [7]设计了一种去中心化的数字货币机制。2008年，中本聪推出了比特币，即具有纯点对点网络[8]的电子现金。也是在2008年，区块链一词首次作为比特币交易[9]背后的分布式账本被引入。

2013年，布特林在他的白皮书[10]中提出了以太坊。2014年，以太坊的开发被众筹，2015年7月30日，以太坊网络上线。以太坊的出现意味着区块链2.0的诞生是因为不同于所有不同的块专注于开发银币（其他类似比特币的硬币）的连锁项目，以太坊使人们能够通过自己区块链上不信任的分布式应用程序进行连接。换句话说，比特币是为分布式账本开发的，而以太坊是为分布式数据存储和智能合约开发的，这是一种小型计算机程序。以太坊2.0升级了以太坊网络，旨在提高网络的速度、可伸缩性、效率和安全性。从2020年到2022年，这些升级有3个阶段的跨越。

2015年，Linux基金会宣布了超账本项目，这是一个针对区块链的开源软 件。为了建立企业区块链，超账本区块链框架不同于比特币和以太坊。在超分类帐下，有八个区块链框架，包括超分类帐结构、超分类帐结构、超分类 帐锯齿，超分类帐洞穴，超分类帐网格和超分类帐实验室，包括超分类帐工具、超分类帐仙人掌、超级分类帐卡尺、超分类帐大提琴和超分类帐管理器，以及四个图书馆，包括超分类帐白羊座、超分类帐被子、超分类帐交易和超分类帐URSA [11]。

区块链的历史总结如图所示。1.比特币和以太坊都是公共区块链，因为任何人都可以参与他们的区块链网络，这也被称为无许可区块链。各种超账本区块链网络都是私有区块链，因为参与者在加入网络之前需要先进行验证，这也被称为许可区块链。

3.区块链技术

3.1.共识算法

作为区块链的特性之一，匿名在信任方面也带来了问题。当匿名用户添加交易时，如何100%确保他们是诚实的？答案是验证每个事务都是合法的（不是恶意的，双等待等）。然后把这些交易放入一个块中。在区块链中添加一个块的共识是通过共识算法。这些共识算法利用了这样一个事实，即区块链上的大多数用户对保持区块链的诚实有共同的兴趣。区块链系统使用共识算法来建立信任，并正确地存储交易块上。因此，共识算法可以被认为是区块链中所有交易的核心。

共识协议本质上是每个参与者都要遵循的一套规则。区块链作为一种没有普遍信任的分布式技术，需要一个分布式共识机制，让所有参与者对区块链的当前状态达成一致。区块链的共识是基于稀缺性，即控制更多的稀缺资源可以使其对区块链的操作有更多的控制权。

基于其他调查工作中出现的算法[2,3,26 32]，PoW、PoS、DPoS和PBFT是 最常见的共识算法。DAG是与其他共识算法有最大不同的算法。诗人是由英特尔公司开发的，用于超级分类帐锯齿。因此，下面将进一步描述这六种共识算法。

工作证明。战俘选择了一个只能通过猜测来解决的问题。例如，当需要创建和验证一个完整的块时，问题是猜测一个值，这样当使用事务数据和值作为哈希函数的输入时，它的哈希输出需要匹配难度，例如，从四个前导的零开始。网络上的每个节点（也称为挖掘节点）现在都在随机猜测不同的单次值，直到一个节点第一次找到匹配难度的值。因此，一个挖掘节点必须在其上花费大量的计算资源（因此称为工作），并比其他节点更快地解决这个问题，以便成功地创建一个块来链接到区块链，并获得激励挖掘奖励，这通常是加密货币。另一方面，哈希函数作为共识算法的核心密码难题非常重要。比特币网络采用加密哈希函数SHA-256 [8]。我们将在下一节中更多地讨论哈希函数。比特币和以太坊公共区块链使用作为其共识算法。共识过程的一个大问题是，它需要大量的时间和电力来完成。

股份证明。PoS [12,33]是第二突出的共识方法，比PoW需要更少 的挖掘计算。PoS解决了PoW存在的时间和用电量问题，因为电力需求与矿工找到一个有关，这个过程需要一些时间。PoS有一个节点，可以被选择为下一个块的创建者。当选择了一个块时，创建者将收到与该块关联的交易费用。如果阻塞获胜者试图添加无效阻塞，则其将失败桩在以太坊2.0升级的第一阶段，区块链世界计算机从PoW转换到PoS共识算法。

委托股份证明（DPoS）。在DPoS中，所有令牌持有者都可以投票给一些代表，也可以将其投票权委托给其他用户。代币持有者拥有的代币越多，数量就越多令牌持有人所拥有的投票权。然后，委托负责验证事务和块，以保护网络 [13]。与PoW中最强大的计算能力或PoS中最强大的令牌不同，DPoS中的令牌 持有者被允许投票决定谁来开采新的区块，并只奖励最好的矿工。EOS是使用DPoS算法[34]的区块链系统之一。

时间证明（PoET）。英特尔公司开发了诗人，使一种不同的方式来确定赢家挖掘一个区块[14]。在PoET中，每个潜在的验证节点请求一个随机等待时间，该时间在可信计算平台上生成。例如，英特尔的SGX。在等待分配的时间后，完成等待时间的第一个节点是验证的赢家，并能够添加新的块。可信的计算平台使每个节点都有机会成为赢家[35]。

实用拜占庭容错（PBFT）。拜占庭容错（BFT）是为了解决一个著名的普遍问题，一些将军不诚实，但需要达成正确的共识。PBFT是一种优化BFT[16]的共识算法。在PBFT中，只要恶意或敌对节点少于区块链系统中所有节点的三分之一，区块链系统就会对区块链的当前状态达成一致。区块链系统中的节点越多，区块链就越安全。当前的超分类帐结构使用PBFT。定向无环图（DAG）。DAGs[17]由顶点和边（连接它们的线）组成，这与其他的不同共识算法。顶点和边是有方向的，因为它们指向一个方向，而它们是无环的 ，因为顶点不会向自己循环。该结构中的每个顶点都代表一个事务。这里没 有块的概念，挖掘也不需要添加事务。每个事务不是建立在块上，而是建立在另一个事务之上。不过，当节点提交事务时，仍会执行一个较小的PoW操作。这可以确保网络不会被垃圾邮件发送，也可以验证以前的事务。IOTA [36]采用DAG共识算法。表1列出了这六种共识算法的比较。我们用尽可能多的细节和尽可能多的定量来比较它们。

3.2.智能合约

智能合同使区块链的另一个美丽的一部分，区块链不仅提供了一个分布式的，不变的记录发生的所有不同的事件，但也允许写非常非主观的计算机代码，定义了这个过程是如何管理和将采取什么步骤当事件发生。以太坊提出的智能合约的一个目标是打破比特币的限制。智能契约是关于为响应某些类型的重大事件而编写的计算机代码。智能合同不必涉及两个或两个以上的当事人，也不必是具有法律约束力的[41]。

智能合约将彻底改变我们的经营方式这是企业区块链应用程序的基石。任何人都可以开发智能合同，而不需要中介机构。智能合约提供了自主性、效率、准确性和成本节约。

3.3.区块链密码学

区块链在不受信任的各方之间创建了一个信任层，以使安全和受信任的记录和事务能够发生。如果没有区块链来创建可信的记录和交易，就需要一个第三方中介。区块链使用密码学和协作来创建信任，因此，它消除了一个集中式机构作为中介的需要。区块链上的信息使用密码学存储在分类账上。区块链使用了一些密码学构建块，如下所述：[41]：

·公钥密码学：用于数字签名和加密。

·零知识证明：证明一个秘密的知识而不透露它。

·哈希函数：单向伪随机数学函数。Merkle树采用哈希函数来形成块头的一个组件。

公钥加密。它被用来证明一个交易是由正确的人创建的。在区块链中，私钥保存在一个数字钱包中，要么是一个硬件钱包（存储私钥的物理设备），要么是任何软件钱包(e。g., 桌面钱包应用程序、移动钱包应用程序或网络钱包)。用户访问其私钥来签名一个称为数字签名的消息，该消息将被传输到区块链，它的公钥是确认消息确实来自用户。例如，在图中。2，用户将其事务数据哈希成哈希值1，然后用其私钥在哈希值1上签名，以生成数字签名。然后，用户将其数字签名及其交易数据一起发送到区块链网络。挖掘器使用用户的公钥来解密接收到的数字签名以获得哈希值A，并且挖掘器还对接收到的事务数据进行哈希处理以获得另一个哈希值B。然后，矿工会检查哈希值A是否等于哈希值B。如果它们相等，则挖掘器将验证用户的事务。

由于私钥仅由其所有者安全保存，相应的数字签名确保交易的作者。该算法可以根据每个用户的个人私钥在每个事务上进行数字签名。这对公钥和私钥与区块链作为区块链的主干相结合，它们被用于签名和验证用户所进行的交易。

以太坊和超分类帐结构都在交易和块上使用数字签名来确认创建者的身 份，并且已签名的数据在签名后没有被修改。椭圆曲线数字签名算法（ECDSA ）被广泛地用于创建一对公钥和私钥。用户的公钥可以在逻辑上被选择为用户的身份，因为对公钥的知识对于验证数字签名是必需的。它在区块链中被用作一种管理用户身份的方法，而不揭示真实世界的身份。

零知识证明。区块链中零知识证明的一个主要用例如下所示。当用户请求向另一个用户发送一些钱时，区块链自然希望在提交此交易之前确保，发送钱的用户有足够的钱来发送。然而，区块链并不需要真正知道或关心谁在花这笔钱，或者他/她总共有多少钱。在这种情况下，区块链知道用户把钱发送给谁以及用户有多少钱。

零知识证明是一些区块链中用于提高用户隐私性的密码原则。目前，以太坊并不支持零知识证明，但为zkSNARKS添加了必要的功能，这是一种零知识证明，目前已经包含在以太坊的开发路线图中。

哈希函数。哈希函数是区块链中使用的一个关键技术。哈希函数是一个具有密码学的五个重要性质的数学方程：

·固定尺寸。哈希函数可以将任何内容作为输入，并创建一个固定大小的输 出。这使得将任何东西压缩成一个固定大小的数据块成为可能。因此，区块链使用哈希函数来压缩针对数字签名的消息。

·预映像电阻。给定一个输入，计算一个哈希输出并不难。然而，给定哈希 输出，在数学上不可能对原始输入进行反向工程。事实上，唯一可能的方法是将数据随机输入到哈希函数中，直到产生相同的输出为止。

·第二个预映像阻力。如果给出了一个输入及其哈希输出，那么获得产生相同哈希输出的第二个输入在计算上是不可行的。

·碰撞阻力。找到任意两个不同的输入在计算上是不可行的，以产生相同的哈希输出。

·大的变化。如果输入的任何一位被更改，它将产生一个完全不同的哈希输出。

图3显示了加密哈希函数提供了一种将区块链上的所有块链接在一起的方 法。在块级别上，前一个块i2头的哈希存储在块i1中，前一个块i1头的哈希 存储在块i中，前一个块i头的哈希存储在块iþ1中，以此类推。

在一个块内，有多个事务。区块链还散列了每一个事务，并在图的底部为一个Merkle Tee。3和Merkle根存储在块头中。通过这种方式，区块链创建了一个不可变、安全和极其值得信赖的分布式账本。如果任何块或该块上的任何事务或信息被修改，无论它有多小，都将立即被发现，并且该块和所有后续块之间的链接将被破坏。

P2PKH地址。除了区块链连接结构、Merkle Tree和上一节提到的PoW挖掘算法外，在比特币支付到公钥哈希（P2PKH）地址[42]中也使用了加密哈希函数。使用哈希函数和公钥密码学为比特币用户创建P2PKH地址，以供比特币用户发送和接收资金(图。4).由于单向功能，不可能将工程从地址反向转换为公钥和私钥。

键的长度不会被更改。私钥的大小为32字节，公钥的大小为65字节（或 压缩的公钥为33字节）。P2PKH地址的大小为20字节。

4.区块链应用程序

从调查来看，区块链的应用包括加密货币、金融（证券交易所、金融服 务、P2P金融市场、众筹等），物联网（物联网）（安全和隐私、电子商务 等），声誉系统（网络社区、学者等），安全和隐私（安全增强、风险管理、隐私保护等）[3]、医疗保健、保险、版权保护、能源、社会应用程序（区块链音乐、区块链政府）、广告[43]、国防、移动应用程序、供应链、汽车[28]、农业部门[44]、身份管理、投票、教育、法律和执法、资产跟踪[45]、数字记录、入侵检测[46]、数字所有权管理、产权登记，等等。图5说明了区块链技术的螺旋式增长的应用。预计区块链系统的用例将会越来越多。

在接下来的子会议中，选择加密货币作为第一个应用程序，供应链作为一个广泛使用的案例，以及智能迪拜办公室作为第一个完整的政府服务应用程序来提供进一步的信息。

4.1加密货币

第一个加密货币是比特币，它于2008年宣布，并于2009年推出。比特币 的最大数量是2100万BTC。一旦一个采矿节点（矿商）找到与难度匹配的一次性值，并成功接受一个区块，矿商此时将获得交易费（24美元和31美元）和6.25 BTC的采矿奖励。每2 1 万个区块（大约 每4年一次），采矿 奖励就会减少一半。目前，不到90%的BTC已经被开采出来。继比特币之后，以太坊（ETH）的市值约为19%。它是目前的第二大加密货币。加密石板软件在其硬币排名[47]中列出了2403种顶级加密货币。其中，表2显示了在上一节中作为共识使用示例提到的7种加密货币。

加密货币的优点包括：

·加密货币是区块链的充分利用案例，它充分利用了区块链的高级特性。

·付款直接从一个人转到另一个人。

·手续费很小。

·寄钱没有延迟，也没有限制。

加密货币的缺点包括：

·没有控制，这可能会招致黑钱。

·它可能会遭受安全攻击，失去数字资产。

·缺乏政府法规，可能会推出一些政策来管理或控制加密货币。

·一些评论说，投资加密货币是高风险和投机性的。例如，特斯拉在提交给SEC的[49]文件中提醒投资者比特币价格的波动性。

4.2供应链

区块链技术提供分布式账本，创建每个交易的永久和共享记录。所有记录的交易对授权参与者都是可见的，可以在分类帐内追踪，不可改变和不可撤销，这促使供应链中的数据共享。例如，IBM已经发布了基于区块链的供应链数据共享解决方案，特别关注物流[3]；VeChain的冷链物流解决方案使用区块链跟踪和监控物流信息，以实现透明、规范、安全和可靠的数据共享[4]。在创客链[50]中，将独特的化学特征数据与区块链结合起来，呈现为一种防伪方法。

此外，各种区块链技术，以提高供应链的安全性、透明度和可追溯性。参考文献。[51]，区块链技术用于确保工业4.0中的智能制造安全，以解决制造系统中的网络安全问题。参考文献。[52]，区块链用于从制造系统的角度实现可持续性。产品生命周期管理的视角。提出了基于许可区块链网络的手动Chain[53]，以消除个性化制造系统中整体规划和局部执行之间的不平衡/不一致。

4.3智能迪拜办公室

迪拜正在投资智能迪拜办公室，并实施区块链技术，将政府在全市范围内从服务提供商转变为服务推动者。它将在多个层面上资助区块链的实现。政府服务采用区块链技术实现。O授权初创企业和企业创建区块链行业。建立一个基于区块链技术的政府服务的先锋实例。

5.使用区块链的安全风险和攻击

由于区块链是去中心化的，没有任何第三方，需要确保对不信任信的基础设施的信任，区块链本身的安全性值得进行研究。本节将重点讨论区块链技术的安全风险，以及对区块链系统的真实攻击和漏洞的调查。

5.1.区块链上的安全风险

通过区块链技术[54]对OWASP Top 10名列出的前10名Web应用程序安全风险进行分析和评估，其评估结果总结见表3。OWASP Top 10是一个关于web应用程序中最关键的安全风险的知名文档，区块链技术面临着前10个风险中的 9个，如表3所示。因此，区块链上的安全性是区块链业务应用程序成功的关 键组成部分之一。

一个研究小组对2009年至2017年5月区块链系统的漏洞进行了调查和分析，并在表4 [29]中列出了9类低级别区块链安全风险。

另一个研究小组对区块链提供了更高水平的安全性。他们指出，与传统计算一样，区块链也面临着拒绝服务（DoS）、端点安全、故意误用、代码漏洞和数据保护等潜在攻击，但发起攻击的细节各不相同。除了DoS攻击，一些研究工作也提出了BGP（边境网关协议）劫持通过操纵路由广告，路由攻击通过延迟传播块或隔离区块链网络的某些部分，日食攻击通过隔离一个受害者的网络，EREBUS攻击通过恶意交通自主系统（ASes）作为中间的比特币节点网络推断节点的决策作为一个更稳定的攻击，DNS攻击，和远程侧通道进攻我们把这些攻击归入网络攻击的类别。我们的论文增加了一个人类过失的风险类别，因为人类是任何系统中的弱点。表5列出了攻击者可能利用它们来发起攻击的6个风险类别。

结合表3-5，我们可以全面了解区块链上的表6所示的安全风险。其他一 些低级别的安全风险，如钱包安全，西比尔攻击，个人密钥安全突出其重要 性，和活力攻击，平衡攻击，时间劫持攻击，芬尼攻击，种族攻击，和自我持有攻击，我们把故意滥用类别也列出。在表6中，很明显，代码漏洞在区块链上具有最大的风险表面。在代码漏洞下，我们将代码划分为以区块链1.0和 2.0为基础的核心软件代码和智能契约它只存在于区块链2.0中。在核心软件代码下，我们强调钱包安全，因为相当多的攻击攻击钱包。

5.2.对区块链系统的5个真实的攻击和错误

在本文中，我们调查了区块链系统上的一些真实攻击和漏洞，以提高人们对区块链系统安全需求的认识。用户使用交换平台在区块链上进行交易，区块链上的私钥保存在一个数字钱包中。因此，交换平台和钱包是区块链系统的一部分。

5.2.1.核心软件错误

发生在2010年8月，CVE-2010-5139漏洞是比特币网络中最著名的软件漏 洞，原因是其协议中存在整数溢出漏洞。由于这个错误，在一个正常的块中添加了一个将0.5 BTC替换为184万亿BTC的无效事务，并且花费了超过8小时 来解决这个问题[55]。此外，当比特币版本从v0.7升级到v0.8时，有一个错 误，即在v0.8中处理的块在v0.7中没有被处理，因为数据库在v0.8中使用了 BerkeleyDB，而在v0.7中使用了LevelDB。此错误导致在v0.8和节点v0.7 [55]。

5.2.2.与加密货币交换平台相关的攻击

2011年，攻击者从Mt。由于网络协议的缺陷，2014年3月，其在线金库中 的另外65万台BTC被黑客窃取，导致Mt。Gox申请破产，因为比特币软件的一 个漏洞允许用户修改交易id[56]。2013年12月，匿名市场绵羊市场不得不关 闭，因为它宣布一家网站供应商利用了一个漏洞，偷走了5400个BTC [57]。 2016年8月，黑客从第三大比特币交易所比特币交易所[58]窃取了119,756个 BTC。2020年7月，黑客入侵了英国加密货币交易所Cashaa，并窃取了 336þBTC。2020年8月，黑客攻击了一个欧洲加密货币交易平台2gether的服 务器，偷走了139万美元的[59]。

5.2.3.个带钱包的攻击

区块链系统中的用户钱包存储其凭证，并跟踪与其地址、用户凭证以及与其账户相关联的任何其他信息相关联的数字资产。在过去的10年里，曾发生过一些袭击事件。据2012年9月5日报道，以美元交易的第四大交易所比特楼宣布，黑客入侵比特楼的服务器，以访问钱包密钥的未加密备份，并转移了24,000个BTC[60]。

2013年4月3日，黑客入侵钱包，窃取了35000BTC，导致钱包无限期暂停 运营。

在2013年8月11日，比特币基金会宣布，黑客利用了一个旧的伪随机数的生成漏洞，使他们能够解决私钥，并从用户的钱包[62]中窃取余额。

在2013年10月23日和10月26日，一家澳大利亚比特币银行被黑客攻击，存储在美国服务器上的钱包服务的4100 BTC被黑客[63]窃取。

由于平价钱包存在多签名漏洞，一名黑客在2017年7月19日[64]从至少三个以太坊账户窃取了3000万人的地址。不幸的是，当时部署的新版本的平价钱包库合同存在一个未被发现的不正确初始化的漏洞，并导致在2017年11月6日触发了另一起事故，受影响的多网站钱包中的资金被冻结了[65]。

5.2.4.对智能合约的攻击和错误

攻击智能合约的一个真实实例是，当一个特定的智能合约DAO（分散自治 组织）建立在以太坊的风险投资基金上，黑客利用其代码弱点，窃取了价值超过5000万美元的加密货币，2016 [66]。一名黑客利用草率的智能合同编码来耗尽智能合同[67]中的资金。2016年6月19日，维塔利克·布特林列出了以太坊合同的错误类别，包括变量/函数命名混淆、不应该公开的公共数据、重入性（调用B）、由于2300气体限制、阵列/循环和气体限制，以及微妙的博弈论弱点[68]。

2017年1月，以太》出现了。营地的黑客发现了一个漏洞，合同代码是“¼þ”而不是“þ¼”[69]。2017年10月，发生了一场50万美元的黑客挑战还有两名黑客入侵并拿走了400个ETH（12万美元），黑客马拉松被数十亿[70]阻止。2018年1月，一名黑客发现了一个使用弱手（PoWH）硬币的整数溢出漏洞，并偷走了888 ETH [71]。2018年10月，一名攻击者发动了一次再入性攻击针对跨链的智能合约，并排水165.38ETH [72]。

5.2.5.网络攻击

2014年8月，戴尔安全工程反威胁部门的一个研究团队发现，一名BGP劫 机者将加密货币矿工的连接重定向到一个劫机者控制的采矿池，并在4个多月的[73]内获得了估计8.3万美元的利润。2016年9月，发现DDoS（分布式 DoS）攻击攻击以太坊网络，攻击事务每块调用外码操作码约5万次，从而大 大减缓了网络[74]。

5.2.6.个端点攻击

恶意软件是端点攻击之一。据报道，恶意软件感染了100多万台电脑，攻 击者利用这些电脑来挖掘26þ百万加密货币的代币[75]。加密劫持是另一种端点攻击，在用户访问网络时的web浏览器中挖掘。攻击者向海盗湾[76]、2017年的Showtime [77]和2018年的印度政府网页[78]注入了加密挖掘脚本，并通过使用访问者的电脑进行采矿获得了访问者的采矿奖。攻击者还将加密劫持代码注入了第三方软件(e。g., 谷歌标签经理[79]和WordPress[80]，以及2018年的Drupal[81])，和广告(e。g., YouTube在2018年发布了[82]的广告)。 2018年，20万名[83]感染了MikroTik路由器，2017年在布宜诺斯艾利斯的星巴克咖啡馆的WiFi[84]，让受感染的电脑挖掘加密货币。

5.2.7.IOTA攻击

2019年1月，一名黑客发起了一场网络钓鱼攻击，收集了用户6个月的隐 私密钥，然后窃取了用户价值300万美元的[85]IOTA。.94与此同时，IOTA网 络遭到了DDoS攻击，因此IOTA的开发人员太忙了，无法发现黑客的盗窃活动 [85]。2020年2月，为了阻止攻击者窃取资金，IOTA基金会不得不关闭协调 器节点超过12天，该节点负责确认所有交易。黑客破解了IOTA自己设计的哈 希函数，并可能创建交易[86]。

从Hydra [87]和KEVM [88]开始扩展，我们在表7中总结了攻击、攻击年 份、基于表6的类别、利用值和根本原因。在当前BTC和ETH价格下，开发价 值超过400亿美元。因此，黑客已经并将继续激励黑客入侵区块链系统，以获得巨大的利益。

6.区块链的安全措施

6.1.安全分析

智能契约字节码漏洞分析。2016年，Oyente被开发出来，用于发现智能 合约[89]中潜在的安全漏洞。2018年，安全纯化作为一种安全分析仪被提出 ，以自动证明以太坊智能合约是不安全/安全的[90]。2018年，宙斯使用符号模型检验和抽象解释来验证公平性，确认智能合同的正确性，约94.6%的合同被评估为脆弱[91]。表8列出了著名的智能契约字节码漏洞分析工具。除了 Oyente、安全化和宙斯之外，感兴趣的读者还可以通过他们的参考文献找到更多关于分析工具的详细信息。

在表8中，所有工具都检测到了一些智能契约中的某些漏洞，尽管有些工具检测到更多的漏洞和/或检测到更脆弱的契约。换句话说，开发人员应该非常注意设计智能合同来抵御已知或未知的攻击，因为并不是所有的合同都足够安全。表中还列出了单个工具的其他特性，以便于用户更多地了解智能契约的分析工具。

事务处理和事务处理日志分析。2020年，TxSpector [99]是第一个对以太坊事务执行字节码级逻辑驱动分析的通用框架，用于攻击检测，如重入、未检查调用、自杀漏洞、时间戳依赖、误用、失败发送、错误处理的异常、不安全平衡和DoS。基于交易日志，我们还在2020年推出了一款不断发展的游戏，以分析现实世界中的攻击和野生[100]中采用的防御。

蜜罐智能合同。黑客们没有利用智能合同的漏洞，而是开发了具有隐藏陷阱的蜜罐智能合同猫头鹰该公司于2019年开发，旨在分析超过200万个智能 合同，并确定了690个蜜罐智能合同[101]。共识算法分析。2016年，来自苏黎世联邦理工学院和NEC实验室的一组研究人员提出了一个框架。定量分析了战俘队的安全性和性能[102]。2019年，Zhang和Preneel评估并表明，PoW无法达到理想的链质量，也无法抵抗自私采矿、双重消费和羽毛分叉[103]的攻击。

6.2.检测恶意代码和bug

2018年，Jiang等人。提出模糊智能契约检测漏洞[104]，Liu等人。在他们的演示论文中提出了一种基于模糊的分析仪，以自动检测智能合约[105]中最常见的错误类型的再入错误，而Hydra是由布莱登巴赫等人开发的。使用错误奖励来启用奖励关键的错误和运行时检测[87]。2019年，EVMFuzzer被提出使用一种微分模糊技术，不断生成种子契约作为目标EVM的输入，并基于执行结果来检测EVM [106]中的漏洞。在2020年，提出了一种轻量级的测试生成方法——harvey，以有效地检测智能合约[107]的安全漏洞和错误。

6.3.核心软件代码的安全性

2017年，智能池作为一个分散的采矿池，旨在防止这种现象，即接近80% 的以太坊和95%的比特币采矿能力位于不到6个和10个采矿池，分别为[108]。2019年，德里杰弗斯等人。指出了两轮多签名方案的细微缺陷，然后提出了mBCJ作为一种可证明的安全但高效的替代[109]。2020年，德里弗斯等人。提出了一种基于配对的前向安全多签名方案Pixel，以对抗后向腐败攻击[110]和Sun等人。提出了反猛禽来减轻和检测主动路由攻击[111]。

6.4.安全智能合约

2016年，Luu等人。提出了增强以太坊操作语义的方法来减少智能合约漏洞的[92]。在2016年，开发了Town Crier，以确保只将认证数据输入智能合同[112]。2018年，FSolidM作为一种工具提出，使开发人员能够将安全智能合同定义为FSM（有限状态机），并增强安全性和功能[113]，仲裁设计旨在验证虚拟机将做什么，以提高可伸缩性和隐私[114]。2020年，来自韩国大学的一个研究小组描述了V埃里斯马特以确保算法的安全，以解决以太坊智能合约[115]的安全问题。

6.5.智能合同验证

2018年，Amani等人。在字节码级别创建了一个程序逻辑来扩展现有的EVM形式化，以正式验证EVM智能契约[116]，阿卜杜拉夫和布鲁米歇提出了一种正式的建模方法来验证区块链和用户的智能契约[117]的行为。2020年，孙宇建立了一个智能合同安全漏洞验证框架。g., 币（BNB）合同[118]，佩梅涅夫等。提出了VerX自动验证以太坊上智能契约的功能特性。

6.6.隐私保护

2016年，Hawk被开发为保护交易隐私，而无需在区块链上存储明文。2018年，明暗对比提供了一个安全高效的比特币混合器，使支付者和收款人不能连接在一起，以实现匿名支付[121]。2019年，我们描述了使用加密的机器人来分析隐私保护的PoS协议[122]，并开发了BITE，以实现来自轻客户端[123]的隐私保护请求。在2020年，Zexe被证明可以实现一些流行的应用程序[124]的隐私保护类似物。2020年，在接收器隐私[125]上出现了远程侧信道攻击。6.7.监控和监管了黑客的钱包

加密货币交换平台可能会锁定任何来自被黑客攻击的钱包的资金。有关反洗钱（AML）的新规定被强制执行，使得黑客难以将资金转移到[126]上。

6.8.硬叉为了回应DAO的黑客攻击，以太坊被分为以太坊经典和新的以太坊。作为一个来自原始软件的硬分叉，新的以太坊可以防止进一步的恶意软件攻击。以太坊经典有标记称为ETC，而新的以太坊有标记称为ETH。新的以太坊和以太坊经典在192万区块之前都有一个共同的祖先。

7.挑战和研究趋势

有一些现有的调查显示了区块链技术的未来趋势或范围。区块链测试、大数据分析、区块链应用程序、智能合约、停止集中化趋势和人工智能都由同一研究小组在Refs中列出。[ 3 , 2 7 ] . 参考文献中提出了一种混合的共识机制、更有效的共识、代码混淆、针对隐私泄漏风险的执行可信计算、应用程序硬化以及高效的数据清理和检测机制。[29].本文提出了一种标准的测试机制、大数据分析、智能合同的开发和评价方法。[45].参考文献中描述了解决区块链技术中的漏洞，解决更多的用例和应用程序，以及提高人们对区块链技术的认识。[ 4 4 ] . 除了这些有效的趋势和范围外，本文还将突出以下面临的挑战和研究趋势。

7.1.可扩展性

交易的可伸缩性。在表1中，最大TPS（每秒交易）是从比特币的27到EOS的3996。PoW能够在全球范围内处理10到27 TPS。以太坊2.0将升级并切换到更有效的协议PoS，使以太坊更可扩展，并将支持1000个TPS [127]。在EOS中，使用DPoS共识算法的一些代表有权投票和验证块，因此EOS更加集中，对一些代表来说更容易组合在一起以启动51%的攻击。如果节点数量增加，PBFT中的通信成本就会迅速增长，因此它适用于没有大量节点但有许多事务的私有设置。目前，超分类帐基于PBFT的织物实现了约3500 TPS。基于PoET的超级分类帐锯齿机能达到2300 TPS。

2019年，Perun被提议作为一种链外支付渠道系统，而不是链上交易来增加TPS [128]，并为PoS侧链系统提供了一个侧链结构，以实现了可伸缩性 [129]。2020年，Yu等人。提议的O菲作为一种无许可协议，将事务吞吐量提高到4-10Mbps[130]。目前，以太坊和比特币平均只处理大约5 KB或10TPS。如此奥希可以达到8000-20000TPS。另一方面，Visa的支付网络可以处理超过65,000个TPS，如2017年8月的[131]所述。因此，区块链在真实分销环境中的TPS的可伸缩性仍然是一个突出的挑战。

在链式数据共享上的可伸缩性。比特币、比特币现金和以太坊的块大小分别为1 MB，在8 MB和32 MB之间，以及低于60 KB。IBM区块链供应链解决方案[132]和VeChain [133]在区块链上记录共享数据，这限制了其解决方案的可伸缩性。可能涉及到大量的涉众，需要在涉众之间共享的数据可能是大量的，而不局限于逻辑数据。随着更多的利益相关者的加入和共享数据的增长，链上的数据共享系统将面临可伸缩性问题的危险。

为了提高可伸缩性，并利用区块链技术，数据可以在链外专用通道上共享，数据共享的链路甚至证据可以记录在区块链中进行跟踪和审计。链外数据共享解决方案需要公司间的渠道，这增加了公司建立和维护这些渠道的负担。此外，这些解决方案还不能保证由公司共享的数据的完整性。例如，A公司可以篡改原始数据，使数据满足B公司的具体要求，然后与B公司共享数据。为了减少相关公司的负担，这些数据可以在云平台上进行定位和共享。我们已经在这一领域提出了一种基于区块链的供应链访问控制和数据共享框架的技术，这可以在我们的专利申请文件[134]中进行参考。

7.2.安全软件代码

从表8中，我们可以知道，几乎每年都会发生对软件代码和智能契约的攻 击。安全性是任何与资产相关的软件的一个不可协商的方面。智能合同安全是一个很高的要求，因为智能合同处理有价值的信息。g., 加密货币、代币和其他数字资产。使用智能合约构建的交易是不可逆转的，如果发现了[135]上的bug，智能合约的软件代码很难被修改或打补丁。为了保护区块链环境免受攻击者的攻击。例如，除了通过加密散列链进行不可变和保护的帐户和事务之外，EOS还面临着保护智能合同执行以抵御恶意攻击[136]的挑战。2020年，一项关于Flash Boys 2.0的研究继续表明智能合约的风险，套利机器人和矿工在智能中提取交易排序依赖的价值合同对以太坊的[137]构成了现实的威胁。根据参考文献。[135]时，很难保证智能合约代码的安全性，因此保证智能合约的安全性是区块链面临的突出挑战之一。

7.3.审计、零信任和异常检测

智能合同审计。在部署智能契约之前，另一个步骤是审计智能契约。2018年，Erays被提出将智能合同反向工程成高级伪代码，然后手动分析多个合同属性[138]。研究趋势之一可能是进一步开发一种审计工具，以自动审计智能合同的更多或所有属性。

对端点安全的零信任网络访问。表7还清楚地显示了端点安全的关键重要 性，包括服务器安全，它需要安全地保护用户的凭据，确保钱包安全，加强服务器保护，并防止钓鱼攻击、内部攻击和其他未知攻击。因此，继续验证端点的零信任网络访问是研究趋势之一。

监测和异常检测。网络监控和攻击/异常检测是区块链安全的持续努力。 除了现有的解析方法[139]之外，机器学习、深度学习和对数据分析事务、 日志、行为和数据的联邦学习将是确保区块链系统安全的研究趋势之一。2020年使用随机森林分类来检测日食攻击[140]，这是利用机器学习技术进行攻击检测的一个例子。

7.4.隐私保护

随着越来越多的数据存储在区块链上，组织和个人的担忧是隐私泄露。其中有一些代码混淆、同态加密、可信执行平台等技术。g., 英特尔SGX)和智能隐私保护合同将是一个很有前途的方向。

7.5.量子计算对区块链的影响

椭圆曲线数字签名算法ECDSA，用于签名事务在区块链，公钥计算其私钥，单向函数容易计算公钥的椭圆曲线乘法，但不可能反向工程部门私钥因为解决数学离散对数问题的困难，假设需要一个天文数字的时间来解决，因此是不实际的。因此，区块链中的用户可以用私钥签名以显示其所有权。

IBM、英特尔、谷歌、里格蒂、D-Wave、IonQ、微软和主要民族国家都积极参与量子计算的研究和开发。1994年，Shor发布的量子算法可以打破公钥密码学[141]最常见算法的安全假设，改进的Shor算法有可能打破ECDSA[142]。

以太坊的开发人员正在测试新的量子电阻签名算法，如XMSS、哈希阶梯签名和括约肌，而以太坊2.0宁静号更新将取代ECDSA方案。后量子算法仍然是量子计算机面临的难题。美国国家标准与技术研究所（NIST）正在使用量子抗性来处理和标准化公钥密码算法。2020年7月，NIST从第二轮列表中的26种后量子密码学算法中选择了15种算法，现在这15种算法已进入第三轮公开审查[143]。

地址。哈希函数的预像电阻确保了给定P2PKH地址，在数学上不可能对其公钥进行反向工程。如果它的公钥是未知的，那么量子计算机无法派生其私钥。然而，一旦任何数量的资金从一个特定的P2PKH地址转移，它的公钥将被公开，以验证其交易数字签名，因此其私钥在量子计算下不再安全。最糟糕的情况是，收件人的公钥被直接用作比特币地址，称为“支付到公钥”（P2PH）。一项分析显示，大约25%的比特币（超过400万BTC）有可能遭受量子攻击[144]。 区块链社区还将解决量子计算对区块链的影响。只有后量子密码学才能抵抗量子攻击。研究趋势之一是研究如何应用后量子密码学来构建鲁棒和抗量子的区块链。然后它将不得不硬分叉区块链，e。g区块链3.0，它实现了新的后量子密码学协议，不同于当前的区块链。

7.6.IOTA安全

由于比特币和基于以太坊的加密货币遇到了可伸缩性和交易费用的问题，IOTA可能是一个很好的选择，因为它在使用DAGs时的顶点和边的性质结构非常不同。通过Tangle技术，IOTA声称它非常具有可扩展性，并且不收取任何交易费用。然而，Tangle技术面临着一些问题，即无法正确地存储交易的订单，以及[145]和他们自己设计的IOTA散列函数Curl的漏洞。IOTA需要克服这些挑战。当该技术成熟时，预计它将在物联网行业被广泛采用，这是一个快速增长和巨大潜力的潜在领域。

7.7.法规和标准的发布

首先，预计加密货币将越来越受欢迎，这将为基金交易创造便利，并节省成本。另一方面，它也削弱了国家的金融政策和控制。其次，更多的国际性区块链应用程序正在出现。例如，区块链系统用于验证COVID-19疫苗注射证书。因此，需要在不同国家之间的法规和协议，相互接受存储在区块链系统上的注入证书。第三，即使在同一个国家内，多方也应同意使用区块链作为一个共同的基础设施，这可能是一个很大的挑战，更不用说制定一个共同的或国际性的标准了。因此，监管和标准将是区块链系统大规模部署面临的挑战之一。

8.相关工作

有一些关于区块链的调查论文。2017年1月，Sankar等人。描述了三种广泛类型的区块链，并定性地分析和比较了三种共识算法，即恒星共识协议、Corda和超分类账结构[26]。2017年6月，郑等人。对包括区块链类型在内的区块链架构进行了调查，并对共识算法进行了定性比较，提出了隐私泄露和自私的挖掘和迁移解决方案[27]的漏洞。2017年8月，纪。H.公园和乔。H.Park对区块链结构和比特币进行了调查，提出了包括大部分攻击（51%的攻击）、交易安全、软件安全和钱包安全等安全挑战，并将区块链安全应用于云计算[55]。2017年8月，另一项在线提供的工作对区块链安全进行了调查，涉及到2017年之前的安全风险、真实攻击和学术安全增强。2017年9月，林和廖提出了51%的攻击的安全问题和一些挑战，包括分叉问题、数据同步和确认时间、法规和集成成本问题[2]。

2018年5月，肯尼索州立大学的一项研究展示了使用区块链和密码学来确 保数据的机密性，各种区块链应用程序的真实性、完整性和隐私保护，而不是区块链本身[28]的安全性。2018年10月，郑等人。对区块链技术进行了调查，调查内容包括共识算法、应用程序、可伸缩性挑战、隐私泄露、自私挖掘、区块链测试的未来发展方向、大数据分析、停止集中化趋势、智能安全分析和人工智能[3]。2018年11月，突尼斯研究人员[146]对区块链面临的挑战和安全问题进行了调查。2018年12月，陈等人。只调查了在不同领域的[43]中的区块链应用程序。

2019年8月，Monrat等人。对区块链架构进行了调查，包括交易流程、区 块链的块结构和特征、区块链的类别、共识程序、区块链应用、权衡、区块链技术[45]的未来范围。2019年11月，Dave等人。调查了区块链技术在农业、教育、供应链管理、医疗保健行业等领域的实施情况。[44].2020年3月， Aguiar等人。调查并使用区块链技术，以提高医疗保健的安全性和可靠性， 并增强患者的隐私性[30]。2019年12月收到并于2020年4月发表的一份调查 工作介绍了区块链技术、应用程序，以及包括可伸缩性、无风险性等问题。 [3 1 ] .在20 2 0 年，萨阿德等人。对区块链攻击面[147]进行了系统的概述。2021年1月，Berdik等人。提交了他们关于区块链的调查论文，以确保信息的完整性和安全性的[32]。

目前已有一些关于区块链安全的调查论文。2019年，达斯古普塔等人。调查了区块链的潜在漏洞，并显示了区块链的发展趋势[148]。在2020年，冷等人。从流程级、数据级和基础设施层面考察区块链安全性，以确定研究差距，并提出区块链安全[149]的未来研究方向。

表9总结了本文的相关调查工作和我们的工作。我们也可以清楚地展示了 我们在本文中的贡献。首先，我们提供尽可能多的关于共识算法的定量比较，而其他的只提供部分比较。其次，区块链本身的安全性是本文关注的焦点，以往的大多数调查只是部分呈现或没有呈现，一些关于区块链安全性的调查论文分别调查了潜在的漏洞，并对过程、数据和基础设施级别的安全性进行了检查。在本文中，我们从风险分析来评估区块链的安全性，得出全面的区块链安全风险类别，分析针对区块链和根本原因的真实攻击和错误，以及介绍了区块链上最近开发的安全措施。最后，表9显示，其他调查论文分别覆盖了2-7个领域，而我们的工作是对区块链的8个领域进行了更全面的调查。

9.结论

本文首先从区块链技术的概述、共识算法、智能契约和密码学等方面对区块链技术进行了更深入的研究。介绍了区块链的历史，并尽可能详细和定量地比较了五种最常见的共识算法和一种最不同的共识算法。区块链中使用的公钥密码学、零知识证明和哈希函数已经详细描述了区块链系统中需要的完整性、身份验证、不可抵付性和支付地址。本文随后列出了区块链的综合应用。它进一步展示了8种加密货币的丰富信息和比较，作为第一个区块链应用程序，供应链作为一个广泛使用的案例，以及智能迪拜办公室作为第一个完整的政府服务应用程序。此外，区块链本身的安全性是本文关注的一个重点。它描述了基于十大Web应用程序安全风险、低级别风险和高级风险的综合安全风险类别。它调查了区块链系统上的许多真实的攻击和漏洞，并列出了它们的根本原因。然后介绍了安全分析、恶意代码检测、软件代码安全、隐私保护等领域的安全措施。特别提出并比较了11种智能契约字节码漏洞分析工具。最后，为大规模部署构建更可伸缩和更安全的区块链系统的挑战和研究趋势。 我们希望我们的努力将帮助人们理解区块链的技术和区块链的安全问题。使用区块链进行交易的用户会更加关注区块链本身的安全性。我们也希望研究人员将从我们的研究中受益，因为他们在开发区块链技术和解决区块链的安全问题。

利益冲突

作者声明，他们没有已知的相互竞争的经济利益或个人关系，这可能会影响本文报告的工作。