区块链：研究与应用3（2022）100067

内容列表可在科学直接获得

区块链：研究与应用

期刊主页： www。杂志爱思唯尔。研究和应用程序

关于区块链技术及其安全性的调查

郭华群[a]，*于星杰[b]，[1]

[a] 新加坡A星空信息通信研究所

[b] 新加坡

ARTICLE INFO

关键词：
区块链
共识算法
智能合约
风险
区块链安全

ABSTRACT

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是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，e所支持和保护的。g.，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，e。g.，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。

*通讯作者。
电子邮件地址： guohuaqun@u。nus.edu，guohuaqun@yahoo.com（H.郭），stefanie_yxj@热邮件。com（X.南斯拉夫

[1] 这项工作是在作者在新加坡A*星的信息通信研究所完成的。

https://doi.org/10.1016/j.bcra.2022.100067
2021年10月6日收到；2022年2月2日收到修订表格；2022年2月12日接受

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。

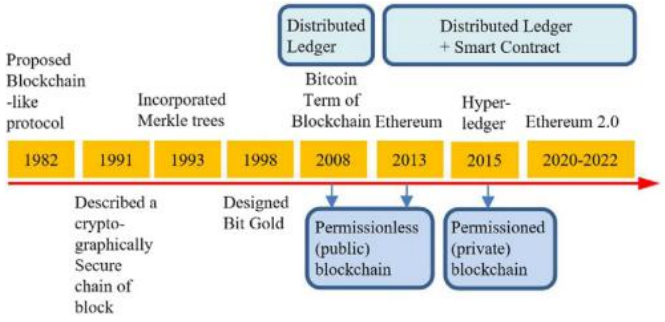

图1.区块链的历史。

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。A number of unique consensus mechanisms have been designed for blockchains, which include Proof of Work (PoW) [8], Prof of State (PoS) [12], Delegated Proof of State (DPoS) [13], Proof of Elapsed Time (PoET) [14], Practical Byzantine Fault Tolerance (PBFT) [15], Directed Acyclic Graph (DAG) [16,17], Proof of Authority (PoA) [18], Tendermint [19], Ripple [20], Scalable Byzantine Consensus Protocol (SCP) [21], Proof of Bandwidth (PoB) [22], Proof-of-Importance (PoI) [23], Proof of Burn [24], Proof of Capacity [25], depending on their unique requirements.

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（PoW）。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nonce值，这样当使用事务数据和nonce值作为哈希函数的输入时，它的哈希输出需要匹配难度，e。g.，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nonce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PoW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PoW作为其共识算法。PoW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）。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nonce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。g.，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]。

表1
共识算法的比较[13、37-40]。

	PoW	PoS	DPoS	波特	PBFT	戴格
设置	无公共许可/私有区块链	无公共许可/私有区块链	公共/私人车链	私有的permissioned/允许少车链	私人许可车链	公开许可非区块链
进入成本和回复	相对较高的成本输入，但高回报	低成本的进入成本，但是低回报	降低成本，降低成本返回比PoS	非常低的成本条目，但低回复	所有参与没有返回	所有参与没有返回
激励措施	获胜的矿工会收到新的硬币，包括他/她验证的区块和交易费用	获胜者收到与新区块相关的交易费用。如果一个区块赢家试图添加一个无效的区块，他/她将失去他/她的股份	损失的威胁声誉和收入可以激励代表们诚实行事，并保持网络的安全	获胜的矿工将通过其验证的新区块获得交易费用。	无	无
最终性 可伸缩性 网络	概率性 高	概率性 中	概率性 中	概率性 中	立即 低的(迅速成长为一个巨大的通信成本作为节点的数量向上伸缩）	概率性 高
能量效率	极低（能量加强的计算，e。g.，比特币消费约121.36每年太瓦时（TWh）	高	高（无矿工必须的	高	中等(一些PBFT系统使用PoW来防止Sybil攻击，但只有在一定数量的块(i。e.,而不是每个街区)	中等(一个小PoW当节点提交事务，以确保网络没有被垃圾邮件，并验证以前的事务)
多数或51%攻击	的数量恶意节点>占25%的所有节点进行攻击	减少51%的攻击概率	更容易组织51%的攻击如果代表们结合了他们的权力	减少51%的攻击概率	恶意的数量节点>占所有节点的三分之一以进行攻击	未进行规模测试
易受影响西比尔攻击	不	是	是	不	是	不
示例	比特币，以太坊，莱特币，莫纳罗，Dash，新西兰现金，降级，等等	以太坊2.0，Cardano，波尔卡多黑硬币和佩尔硬币。	EOS、比特股、Lisk、Steem、方舟、Nano、卡达诺和Tezos。	超分类帐锯齿形	超分类帐结构，齐利卡	希腊文的第九个字母
事务处理每第二（TPS）	比特币：最多7个27	以太坊：15	EOS：3996 BitShares：3300	超分类帐 锯齿形：2300	超分类帐结构：约3500	日耳曼：250 IOTA花粉V0.2.2：>1000
块确认时间(s)	比特币：6000 Litecoin：150	以太坊：15	EOS：0.5 BitShares：3	没有实际时间建立	在秒级（否找到实际时间）	120

智能合约也被称为链码[41]：

0程序规则和决策点进入区块链事务和流程。
0自动化事务处理，并确保它们都遵循相同的规则。
0，在区块链上运行。

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]：

0公钥密码学：用于数字签名和加密。
0零知识证明：证明一个秘密的知识而不透露它。
0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。

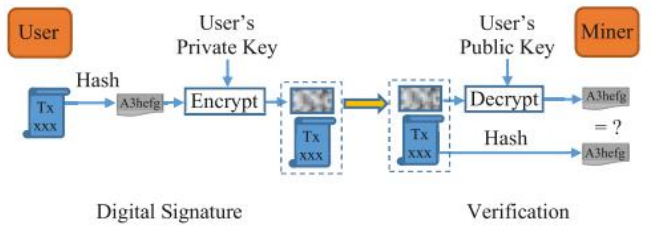

图2.在区块链事务中使用的数字签名和哈希。

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：

0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。
0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。
02预映像电阻。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。
0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。
0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ip1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。

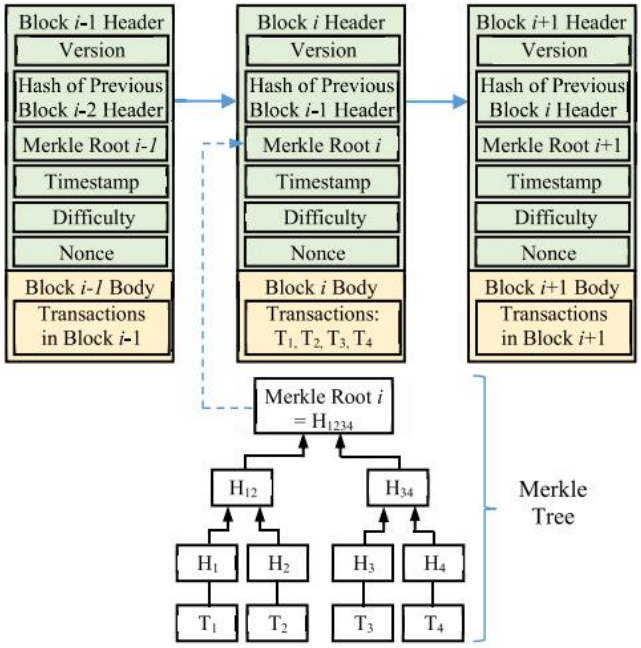

图3. 区块链连接结构和一个带有哈希函数的Merkle树。

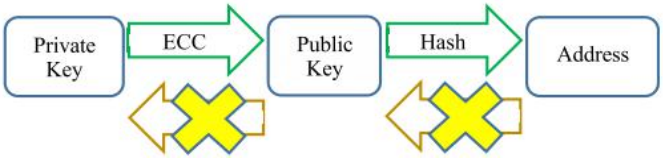

图4. 比特币地址的公钥密码学和哈希函数。

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。

. 1. 4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21万个区块（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%

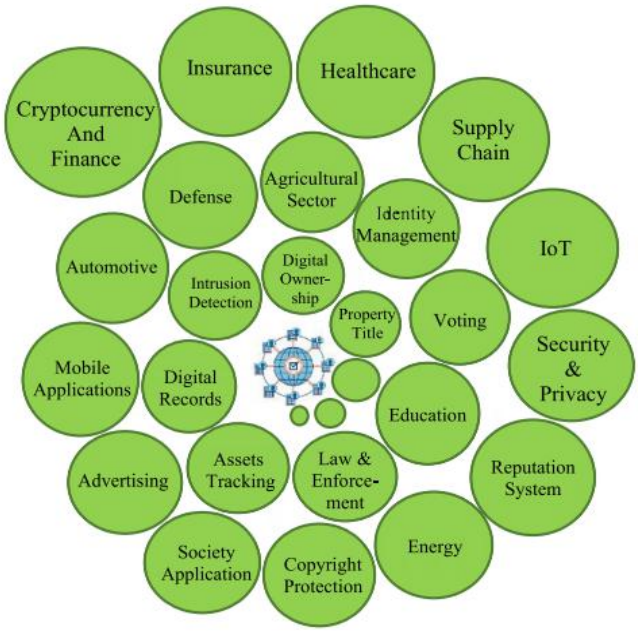

图5. 区块链应用程序。

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：

0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。
0付款直接从一个人转到另一个人。
0.手续费很小。
0：寄钱没有延迟，也没有限制。

加密货币的缺点包括：

0，没有控制，这可能会招致黑钱。0它可能会遭受安全攻击，
失去数字资产。
0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。
0一些评论说，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。

. 2. 4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

表2
加密货币[48]。

	推出年份	已启动价格	2021年1月1日的单价（美元）	2021年2月27日的单价（美元）	2021年2月27日的市值（美元）	矿床算术	总数
比特币（BTC）	2009	0.0008美元	28,994.01	47,781.33	8906亿	接近90%	21,000,000
以太坊（ETH）	2014	预售：0。30美元宅基地推出价格：12.50美元	737.71	1502	1725亿	114.84 M	目前没有实施困难上限，并限制在每年1800万美元
卡没有（ADA）	2017	0.019 EUR	0.31	1.36	434亿	约71%	45,000,000,000
波尔卡多（点）	2020	1.2美元	9.12	33.64	307亿	1,049,328,830	没有最大限度的供应
莱特币大变异细胞	2011	.34美元	124.67	176.31	118亿	约79%	84,000,000
比特币现金（BCH）	2017	543美元	低于400	501.3	.490亿	接近89%	21,000,000
EOS	2017	2.29美元	2.5975	3.68	.530亿	接近93%	1,027,393,754
希腊文的第九个字母	2016	未知的	0.2969	1.1532	.230亿	2,779,530,283	2,779,530,283

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。

.3.4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。

O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。
O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。

.1.5.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

表3
区块链技术[54]上的十大web应用程序安全风险。

十大Web应用程序安全风险	区块链技术评估	分析实例
注射液	区块链技术的投入卫生处理较差	在EOS主网启动之前，发现了EOS智能契约中缓冲区越界写入的漏洞，以及运行恶意智能契约的可能性
损坏的身份验证	没有适当实现认证功能，就存在一个大的攻击面	加密货币LISK是允许对身份验证进行攻击的一个示例
敏感数据暴露	造成此漏洞发生的可能性很高	容易受到数据挖掘工作的影响——在区块链上挖掘公共数据以获取有用的信息；量子计算将破坏用于在区块链上加密数据的公钥加密技术
XML外部实体（XXE）	不适用	
断开访问控制	智能合约的一个主要漏洞	由于访问控制漏洞，对奇偶校验多签名钱包的两次攻击
安全配置错误	影响区块链安全	当以太坊钱包被配置为从端口8545接收外部命令时，攻击者利用一个漏洞窃取加密货币
跨站点脚本（XSS）	在某些方面影响区块链	受XSS攻击的区块链探索者可能显示不受信任的交易数据；区块链探索者和受XSS攻击的钱包都可以访问用户的私钥并控制他/她的帐户
不安全的脱序列化	可能会危及区块链系统	如果恶意用户控制事务数据，区块链系统可能会受到脆弱的反序列化代码的破坏
使用组件与已知的漏洞	以太坊智能契约	以太坊中超过90%的智能合约确实重用了代码，并且可能包含已知的代码脆弱点
日志记录不足监控	日志所有者可以取消对其日志的监控	智能合同缺乏监控，黑客可能利用他们的漏洞正在检测

表4
区块链安全风险类别在较低级别的参考文献。[29].

S/N	类别
1	51%的漏洞
2	犯罪活动
3	私钥安全
4	交易隐私泄露
5	双重支出
6	刑事智能合同
7	低价经营
8	智能合约的漏洞
9	优化不足的智能合约

表5
区块链的高级安全风险类别。

风险	描述
网络攻击	如表1所示，区块链每秒的事务数量有限，DoS攻击可能提交比区块链的能力更多的事务，并导致区块链不可用。
端点安全	除了DoS，BGP（边界网关协议）攻击，路由攻击，月食攻击，更稳定的攻击，DNS攻击，和远程侧通道攻击也属于这一类。 端点可以是异构的，它们有更多的选择来利用这些漏洞。端点也可以是齐次的，其中一个系统中的缺陷可能存在于所有系统中。
有意的误用	如表1所示，攻击者可以控制更多的节点到发起类似于51%的攻击类型。
编码脆弱性	代码漏洞可能来自于智能合约 任何人都可以编写或编写底层的平台代码。由于分布式网络的存在，这些漏洞具有广泛的影响，代码不能修改一次 使展开故意编写恶意的智能合约。
数据保护	数据保护依赖于区块链，而不是数据所有者来提供数据的完整性和可用性。
人过失	日志所有者可以取消对其日志的监控。

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。

. 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。

. 2．1．5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]。

. 2．3．5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]。

表6
综合的区块链安全风险类别。

C1：网络攻击	C2：端点保护措施	C3：有意误用	C4：代码漏洞	C5：数据保护	C6：人为过失
DoS，BGP（边界门协议）劫持路由攻击，日食攻击，更健康的攻击，DNS攻击，远程侧通道进攻	51%的脆弱性，西比尔攻击，个人密钥安全，挖掘恶意软件，加密劫持攻击	注入，不安全的去序列化，51%的漏洞，犯罪活动，双期未决，自私的采矿，活力攻击，平衡攻击，时间劫持攻击，芬尼攻击，种族攻击，自我控制攻击	核心软件代码（区块链1.0,2.0）：注入，使用已知漏洞的组件、安全的错误配置、中断的身份验证、中断的访问控制、不安全的去序列化、XSS、事务隐私泄漏、双重支出、私钥安全 钱包安全 智能合约（区块链2.0）： 智能合约、刑事智能合约、定价低估、智能合约优化不足的漏洞	敏感数据暴露，隐私泄露	日志记录不足 监控、安全配置错误

O2013年4月3日，黑客入侵钱包，窃取了35000 BTC，导致钱包无限期暂停运营。

O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。

O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。

O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]。

.2.4.5.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165.38 ETH [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]。

.2.6.5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。

.2.7.5次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。

表7
攻击、年份、类别、利用价值和根本原因。

攻击	年 类别	利用价值	根本原因
山。戈克斯	2011 C1	几个 千BTC	网络中的缺陷 礼仪
位地板	2012 C2	24,000 BTC (250,000 极限强度设计	比特地板的服务器被黑攻击 泄漏的未加密的备份 钱包钥匙
个人钱包	2013 C4	35,000 BTC	个人钱包被黑了
点对点基于网络的匿名数字货币 基金会	2013 C6	_	一个与旧的一代错误 伪随机数
羊 市场市场	2013 C4	5400 BTC	一个网站供应商利用了一个弱点
山。戈克斯	2014 C4	65万BTC（4. 5亿美元）	一个允许用户修改事务id的软件错误
小谷 安全工程	2014 C1	83000美元	BGP劫机
大刀	2016 C4	五千万 极限强度设计	代码上的弱点：微妙的游戏理论上的弱点
比特芬尼克斯	2016 C2 & C4	119,756 BTC （6500万 极限强度设计	黑客偷了BTC。
以太坊 网络	2016 C1 & C4	_	DDoS攻击：调用 每个块大约有50,000次
金HKG	2017 C4	_	一个用合同代码读取“¼þ”而不是“þ¼”的错误
奇偶校验钱包	2017 C4	3千万 极限强度设计	地址组成（委托调用þ公开自毁）
智能数十亿	2017 C4	400 ETH (120,000 极限强度设计	陷入聪明的合同 断开的缓存机构
奇偶校验钱包	2017 C4	3亿 极限强度设计	未发现的初始化错误（委托调用þ未指定的修改器）
加密劫持	2017－2018 C2 & C4	_	被破解并插入的加密数据挖掘脚本或加密劫持代码
PoWH	2018 C4	888 ETH	整数溢出
跨链	2018 C4	165.38 ETH	再入攻击
希腊文的第九个字母	2019 C2	394万 极限强度设计	一种收集用户隐私密钥的网络钓鱼攻击
希腊文的第九个字母	2020 C4	_	自定义哈希函数 被打破了
现金a	2020 C2	超过336 BTC	怀疑该系统上安装了一块恶意软件
2gether	2020 C2	.3一百万 极限强度设计	2gether的服务器被黑了

注：C1：网络攻击，C2：端点安全，C3：故意误用，C4：代码漏洞，C5：数据保护，C6：人为疏忽；DAO：分散的自主组织；PoWH：弱手的证明。

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。

.2.6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

表8
智能契约字节码漏洞分析工具和特性比较。

智能合同分析工具	分析领域	脆弱性检测到	已分析的智能合同的数量	脆弱的智能合同的数量	备注：
Oyente [92]	符号的实行	时间戳依赖，事务顺序依赖，错误处理的异常，重入性	19，366	8，833	第一个基于符号执行的工具
Mythril [93]	符号的实行	整数欠流，所有者覆盖到以太的退出，以及其他	未知的	有，但没有给定的数字	
teEther [94]	符号的实行	错误的可见性、错误的构造函数、语义混淆、逻辑缺陷、契约间的利用	38,757	815	
洋蓟[95]	符号的实行	未受保护的函数，整数溢出，未定义的行为，错误配置，数字，定时，业务逻辑。	100	有，但没有给定的数字	
宙斯[91]	摘要解释	重入性、发送失败、未检查发送、整数溢出/下流、事务状态依赖性、不正确的逻辑、无逻辑、块状态依赖性、逻辑正确但不公平、事务顺序依赖性	22，493	21，281 (94.6%)	检查智能合约 针对用户定义的策略编写
M艾安[96]	符号的实行	整个合同的执行轨迹，i。e.，漏水的合同，挥霍的合同，自杀的合同，贪婪的合同	970,898	34,200	通过长调用序列检测智能契约
Securify [90]	数据流分析	以太流动性，不受限制的写，不写后的呼叫，限制转移，处理不当的异常，交易顺序依赖，意外的参数	以太坊虚拟机（EVM）：24594；固体数据集： 100	6.50%	探索所有合同 行为
破坏性[71]	摘要解释	重新入，无担保余额，使用原产地，可破坏的合同，未检查发送	141,000	有，但没有给定的数字	将字节码转换为语义逻辑关系
MadMax [97]	摘要解释	无界批量操作，整数溢出，钱包中的非孤立外部调用，激励攻击	633万	5.42%	寻找气体的工具 脆弱点
奥西里斯[98]	符号的实行	整数错误：截断错误、算术错误和信号相关的错误	.2一百万	42,108	
EthBMC [94]	符号的实行	提取乙醚，重定向控制流，自毁契约，奇偶校验漏洞，更多的利用	大约一 2.2百万	5905	更精确的EVM内部推理

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。

.5.6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。

.8.6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。[3,27].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。[44].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。

.1.7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0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10 TPS。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。

.2.7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。

.3.7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。

.5.7.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，

表9
对各种调查工作的总结。

工作	区块链类别	共识协议		应用程序	可扩展性	区块链安全	量子计算	未来方向
		定性比较	定量的比较					
[26]	是	是						
[27]	是	是			是	部分的		是
[55]						部分的		
[2,28]	是	是		是	是	部分的		
[3]	是	是	部分的	是	是	部分的		是
[150]				是				
[29]		是				部分的		是
[30]		是						
[31]	是	是	部分的		是	部分的		
[32]				是				
[45]	是	是	部分的	是	是			是
[44]				是		部分的		是
[146]	是	是		是		部分的		
[147]		是	部分的			部分的		是
[148]				是	是	对漏洞进行调查	是	是
[149]		是		是	是	检查了流程、数据和基础设施级别中的安全性	是	是
这个纸	是	是	尽可能多的做得到的	是	是	综合区块链安全风险类别，真实的攻击，错误和根本原因，最近的安全措施	是	是

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。[31].在2020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。

参考文献

[1] M.S.阿里，M。维奇奥，M。等人，区块链的应用
物联网：一项全面的调查，IEEE通信调查和教程21(2)（2019）1676-1717。
[2] IC.-林，TC。.-廖，一个关于区块链安全问题和挑战的调查，Int。J.
网络。安全。19 (5) (2017) 653 - 659.
[3] Z.郑，S。谢，HN。.-戴，X。陈，H。王，区块链挑战和
机会：一项调查。J.网络网格服务。14 (4) (2018) 352 - 375.
[4] D.周姆，由相互建立、维护和信任的计算机系统
可疑的团体，博士。D论文，加州大学伯克利分校，美国，1982年。
[5] S.哈伯，W。S.例如，如何对一个数字文档进行时间戳，J。密码。3 (2)
(1991) 99 - 111.
[6] D.拜耳。哈伯，W。S.提高效率和可靠性
数字时间戳，in: R。卡波塞利。德桑蒂斯，美国。Vaccaro（电子版），序列二，施
普林格，纽约，纽约，美国，1993年。
[7] R.夏尔玛，有点金，投资百科全书，2021年。在线可用： https://www。investop
edia.com/条款/b/b-gold。asp.（2021年10月24日通过）。
[8] S.中本聪，比特币：一个点对点的电子现金系统。https://bitcoi
n.org/bitcoin.pdf，2008年10月。
[9] R.作者，区块链技术的时间轴和历史。https://whatis.techt arget.com/feature/A
-timeline-and-history-of-blockchain-technology, 2021.
[10] V.丁灵，以太坊白皮书。https://ethereum.org/en/whitepaper/, 2013.[11]
A.Groetsema。Groetsema，N.Sahdev，N。萨拉米，R。Schwentker，F.Cioanca，
区块链为商业：超分类帐技术导论，Linux基金会，2019年。
[12] P.Vasin，黑币的股份证明协议v2。https://blackcoin.组织/黑色公司在邮政协议-
v2白皮书。pdf.2021年3月21日通过。
[13]加密，什么是委托的证据？Crushcrypto (2018).可在网上获得。什么是委托的股权
证明。（2021年3月21日通过）。
[14]英特尔公司，PoET 1.0规范，2016年。可在网上获得：https://锯齿形的照片。
hyperledger.org/docs/core/releases/1.0/architecture/poet.html.（2021年3
月21日通过）。
[15] M.卡斯特罗，B。Liskov，实用拜占庭容错，在：论文集
第三届操作系统设计与实施研讨会：1999年2月22-25日；美国洛杉矶新奥尔良，
USENIX协会，加州伯克利，美国，1999年，页。173 - 186.
[16] S.波波夫，缠结。https://whitepaper.io/document/3/iota-whitepaper,
2018.2021年3月21日通过。
[17]学院绑定，什么是加密货币中的有向无环图（DAG）？学院约束力，2020年。可在线获得
：https://学院。约束力。com/en/艺术les/what-is-a-directed-acyclic-graph-dag-
in-cryptocurrency.（2021年4月29日通过）。
[18]开放以太坊，权威链的证明。https://openethereum.吉图布。io/权威链的证明。2021
年3月21日通过。
[19] J.天创之权：没有采矿的共识。https://tendermint.com/static/
docs/tendermint.pdf, 2014.2021年3月21日通过。
[20] B.蔡斯。《XRP账本共识协议的分析》，arXiv，
2018年，预印本。
[21] L.Luu，V.纳拉亚南，K。Baweja等人，SCP：一种可计算扩展的拜占庭图
区块链的共识协议，IACR密码学电子打印存档，2015年，p。1168.
[22] M.GhoshM。理查森，B。福特，R。詹森，《到乌龟的环形路径：补偿继电器的带宽
证明》，2021年。https://dedis.cs.耶鲁。edu/dissent/papers/hotpets14-
torpath.pdf.2021年3月21日通过。
[23] NEM，NEM技术参考书。https://nemplatform.com/wp-content/uploads/
2020/05/NEM_techRef.pdf, 2018.2021年3月21日通过。
[24] K.卡兰提亚斯。Kiayias，D.Zindros，燃烧证据，在：J。波诺，N。赫宁格
(Eds.),金融加密和数据安全。FC 2020.《计算机科学》上的课堂讲稿》，第1卷
。12059，施普林格，图章，2020，页。523 - 540.
[25] A.海耶斯，《能力证明》（加密货币），投资出版社，2020年。在线可用：
https://www.投资百科全书。能证明容量的加密货币。asp.（2021年3月21日通过
）。
[26] L.S.桑卡，S。M，M.塞苏马达万，共识协议的调查
区块链应用，在： 2017年高级计算和通信系统国际会议（ICACCS -2017）：
2017年1月6-7日：哥印拜陀，印度，IEEE，皮斯卡塔韦，新泽西州，美国，
2017年，页。1 - 5.
[27] Z.郑，S。谢，H。Dai等人，区块链技术的概述：架构，
共识和未来趋势，见： IEEE第六届国际大数据代表大会：2017年6月25-30日：檀香
山，嗨，美国，IEEE，皮斯卡塔韦，新泽西州，美国： IEEE，2017，pp。557 - 564.
[28] A.P.JoshiM。韩，Y。王，一个关于区块链的安全与隐私问题的调查
技术，计算的数学基础1(2)（2018年5月）121-147。
[29] X.李，P。江，T。陈，X。罗，问。温家，区块链的安全性调查
系统，未来的发电机。压缩。西斯特。107（2020年6月）841-853。
[30] E.J.De Aguiar，B。S.Faical，B.Krishnamachari，J.Ueyama，对区块链的调查-
基于医疗保健的战略，ACM Comput。服务。53 (2) (2021) 1 - 27.
[31] H.T.M.游戏，H。D.Weerasinghe，N.G.J.Dias，一个关于区块链的调查
技术概念、应用和问题，SN计算机科学1（114）
(2020).
[32] D.Berdik，S.Otoum，N.施密特，D。波特，Y。一个关于区块链的调查
对于信息系统的管理和安全，Inf。过程。马纳格。58 (1)
（2021年1月）。
[33] S.国王，S。纳达尔，PPCoin：带有股权证明的点对点加密货币。
https://decred.org/research/king2012.pdf2012年8月。
[34] D.施密特，被委托的股权证明。https://www.benzinga.授权股权证明/，2020年7月
。
[35] J.弗兰肯菲尔德，《时间流逝的证明》（PoET）（加密货币），投资出版社，2020年
10月16日。在线可用： https://www。投资百科全书。证明经过的d-时间-加密货币。
asp.（2021年3月21日通过）。
[36]日耳曼。https://www.希腊文的第九个字母org/.2021年3月23日通过。
[37] T.Kozak，《满足不同商业需求的共识协议》，第一部分，智力软件，2018年。可
获得：https://区块链。intellectsoft.净/blo g/consensus-protocols-that-
meet-different-business-demands/.（2021年3月21日通过）。
[38]破解密码，什么是工作的证明？。https://crushcrypto.什么是工作的证明/，2021年。
[39]破解密码，什么是实用的拜占庭容错（PBFT）？Crushcrypto，2018.可在网上获得。
拜占庭容错。（2021年3月21日通过）。
[40] S.张，JH。.-Lee，区块链的主要共识协议分析，ICT
特快6（2020）93-97。
[41] R.桑托斯，K。贝内特，E。Lee，《区块链：理解其用途和含义》，Linux基金会，
2021年。在线可用： https://www。edx.组织/课程/b lockchain-understanding-its-
uses-and-implications.（2021年10月5日通过）。
[42] A.M.安东诺普洛斯，掌握比特币，第二版，奥莱利媒体公司。，
2017年6月，美国加州塞瓦斯托波尔市。
[43] W.陈，Z。徐，S。石，Y。赵，J。赵，区块链应用的调查
不同领域，见：区块链技术与应用国际会议（ICBTA）：12月10-12日：西安，中国，
ACM，纽约，纽约，美国，2018年，页。17 - 21.
[44] D.戴夫，S。帕里克，R。Patel等人，区块链技术及其调查
建议的解决方案，程序。科学。160 (2019) 740 - 745.
[45] A.A.Monrat，O.Schelen，K.安德森，对区块链的调查来自
应用程序、挑战和机遇的观点，IEEEAccess7（2019）117134-117151。
[46] W.孟，E。W.Tischhauser，Q.王，Y。王，J。汉，入侵检测时
满足区块链技术：一篇综述，IEEEAccess6（2018）10179-10188。[47]加密石板，硬
币排名。https://cryptoslate.com/硬币/，2021年2月28日。[48] L.康威，除比特币之
外最重要的10种加密货币，投资
（2021年6月1日）。
[49] S.特斯拉购买了15亿美元的比特币，计划接受它作为支付，2021年2月8日。在线可用
： https://www。cnbc.比特币-1点50亿比特币。html.（2021年3月23日通过）。
[50] J.冷，P。江，K。徐，问。刘，J。L.赵，Y。边，R。Shi，MakerChin：区块链
具有社会制造中自组织过程的化学签名。清洁。刺针234 (2019) 767 - 778.
[51] J.冷，S。是的，我。周，J。L.赵，问。刘，W。郭，W。曹，L。富，区块链
工业安全智能制造4.0：一项调查，IEEE交易。西斯特。男人
网络网。：系统51(1)（2021）237-252。
[52] J.冷，G。阮，P。江，K。徐，问。刘，X。周，区块链授权
行业中的可持续制造和产品生命周期管理4.0：一个调查，更新。维持。能量Rev。
132 (2020), 110112.
[53] J.冷，D。Yan，问。刘，K。徐，J。L.赵，R。石，L。魏，D。张，X。陈，
手动链：将允许的区块链与整体优化模型相结合，作为智能制造的两级智能，IEEE交易
。西斯特。人的网络网。：系统50(1)（2020）182-192。
[54] H.邮政邮政，将OWASP前十映射到区块链，收益计算。科学。177
(2020) 613 - 617.
[55]吉。H.公园，乔。H.云计算中的区块链安全：用例，
挑战和解决方案，对称性9 (8)（2017）164。
[56] J.Frankenfield，Mt.Gox，投资百科全书，2021年。在线可用： https://
www.投资百科全书。com/terms/m/mt-gox.asp.（2021年3月26日通过）。
[57] E.匿名网站以1亿美元的比特币消失，ZDNet，2013年12月5日。在线可用：
https://www。zdnet.用10亿比特币消失。（2021年3月26日通过）。
[58] J.霍维茨，我。2016年8月3日，全球最大的比特币交易所之一Kar在一次石英”黑客
交易中损失了6500万美元。在线可用： https://qz。com/748995 /one-of-the-worlds
-largest-bitcoin-exchanges-lost-65-million-in-a-hack/.（2021年3月26日通过）
。
[59] F.Erazo，黑客从欧洲加密货币交易平台窃取了超过130万美元，2020年8月3日。可在
网上获得：https://图表。com/ne ws/hackers-steal-over-13m-from-european-
crypto-trading-platform.（2021年3月26日通过）。
[60] V.布特林，比特地板被黑客攻击，25万美元失踪，比特币杂志，2012年9月5日。可
在线获得：https://bitcoin杂志。地址-250000-缺失-1346821046。（2021年3月
26日通过）。
[61] C.K.Elwell，M。M.墨菲，M。V.塞特辛格，《比特币：问题、答案和法律问题分析》
，国会研究服务部，2014年7月15日。在线可用： https://www。
everycrsreport.com/reports/R43339.html.（2021年3月26日通过）。
[62] R.比特币钱包，注册器，2013年8月12日。在线可用： https://www。theregister.
安卓_bug_beteh s_bitcoin_wallets/。（2021年3月26日通过）。
[63] B.澳大利亚比特币银行被黑客攻击：$1mþ被盗，布里斯班时报，2013年11月8日。
在线可用： https://www。brisbanetimes.com.非盟/科技公司nology/australian-
bitcoin-bank-hacked-1m-stolen-20131108-hv2iv.html.（2021年3月26日通过）。
[64] W.赵，3000万美元：以太因平价钱包被盗被盗，币台，2017年7月20日。在线可
用： https://www。coindesk.com/marke

ts/2017/07/19/30-million-ether-reported-stolen-due-to-parity-wallet-breach/.[92] L.Luu, DH..-楚，H。Olickel等人，使智能合同更智能，在：2016年
（2021年3月26日通过）。ACM SIGSAC计算机和通信安全会议（CCS '16）；
[65]奇偶校验技术，安全警报。https://www.平价io/安全警报-2016年10月24日至28日；奥地利维也纳，ACM，纽约，纽约，美国，2016年。
2017年11月8日。已于2021年4月11日通过。[93] Mythril.https://github.com/ConsenSys/mythril, 2018.2021年4月7日通过。
[66] N.波普尔，一个超过5000万美元的黑客攻击，希望在[94] J。弗兰克，C。阿谢尔曼，T。Holz，EthBMC：一个有界的模型检查器的智能
虚拟货币，N。Y.时报，2016年6月17日。合同，截止日期：第29届USENIX安全研讨会；2020年8月12-14日；在线，USENIX
[67] A.刘易斯，《以太坊的温和介绍，《街区》，2016年10月2日。协会，伯克利，美国，2020年，页。2757－2774.
[68] V.布特林，思考智能合同安全，以太坊基金会博客，[95] M。莫斯伯格，F。曼扎诺。亨宁芬特等人，手册：用户友好
2016年6月19日。在线提供： https://blog。以太坊。请思考二进制文件和智能契约的符号执行框架， 见： 第34期
智能合同安全/。（2021年4月11日通过）。ACM自动化软件工程国际会议（ASE）：11-15
香港黑客金科技公司（[69]Spartak_t）有一个严重的漏洞。https://bitcointalk.org/ind2019年11月；圣地亚哥，美国，IEEE，皮斯卡塔韦，美国新泽西州，2019年，页。1186－1189.
ex.php?topic¼1744115.0,2017年1月08日。2021年4月11日通过。[96] I.尼古拉，A。科卢里，我。谢尔盖等人，发现贪婪，浪子和自杀
[70] J.区块链彩票智能数十亿美元，大规模合同，在：第34届年度计算机安全应用程序
可在线获得：https://卡尔维纳耶尔。比特币/10月13日/50万k黑客会议（ACSAC）；2018年12月3-7日。圣胡安，美国，ACM，纽约，美国，
enge-backfires-blockchain-lottery-smartbillions/, 2017.（2021年4月11日通过）。2018，pp.653－663.
[71] L.布伦特。Jurisevic，M.一种可伸缩的安全分析，[97] N。Grech，M。香港，A。MadMax：在天然气条件下生存
智能合同框架，arXiv，2018年预印本。以太坊智能合约，在：关于编程语言的ACM诉讼程序
[72] A.罗恩，屁股链是如何被黑客攻击的。https://medium.com/swlh/how-spankch 2, 2018, pp.1－27.
-65b933393c，2020年3月27日。2021年4月9日通过。[98] C.F.托雷斯，J。舒特，R。状态，奥西里斯：在以太坊智能中寻找整数错误
[73] P.利特克，J。斯图尔特，BGP劫持加密货币利润，安全工作，7份合同，在：第34届年度计算机安全应用会议（ACSAC）；
2014年8月。在线可用： https://www。secureworks.com/研究/bgp-h3-2018年12月7日；圣胡安，美国，ACM，纽约，美国，2018，页。664－676.
劫持加密货币的利润。（2021年4月9日通过）。[99] M.张，X。张，Y。张，Z。揭露以太坊的攻击
[74] J.Wilcke，以太坊网络目前正在遭受DoS攻击，来自交易，在：第29届USENIX安全研讨会；2020年8月12-14日；在线，
以太坊基金会博客，2016年9月22日。在线提供： https://blog。e USENIX协会，伯克利，美国，2020，页。2775－2792.
thereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/.[100] S.周，Z。杨，J。翔，一个不断发展的游戏：对现实世界的评价
（2021年4月9日通过）。以太坊生态系统中的攻击和防御，见：第29届USENIX安全版
[75] Aruba，10区块链和新时代安全攻击你应该知道，1月研讨会；2020年8月12-14日；在线，USENIX协会，伯克利，加州，美国，
22， 2019.在线可用：https://博客。arubanetworks.2020年第10号集团版，第1页。2793－2810.
kchain-and-new-age-security-attacks-you-should-know/.（2021年4月9日通过）。[101] C.F.托雷斯，M。史泰琴，骗局的艺术：揭开以太坊中的蜜罐的神秘面纱
[76] Waqas，海盗湾捕获运行加密货币挖掘脚本，黑客读取，智能合同，在：第28届USENIX安全研讨会；2019年8月14-16日；圣诞老人
2017年9月17日。在线可用： https://www。hackread.美国加州克拉拉，USENIX协会，加州伯克利，美国，2019年，页。1591－1607.
bay-caught-running-cryptocurrency-mining-script/.（2021年4月9日通过）。[102] A.GervaisG。O.卡拉姆，K。Wust，等人，关于证明的安全性和性能
[77] K.麦卡锡，哥伦比亚广播公司的展示时间在观众的工作网络中挖掘加密硬币，在： 2016 ACM SIGSAC会议的计算机和
浏览器，寄存器，2017年9月25日。在线可用： https://www。其他通信安全，2016年10月24日至28日；维也纳，奥地利，ACM，纽约，纽约，
egister.com/2017/09/25/showtime_hit_with_coinmining_script/.(访问美国9号，2016年，页。3－16.
2021年4月)。[103] R.张，B。普雷内尔，制定一些常见的指标：评估工作证明
[78] M.黑客们秘密运行了关于印度共识协议安全的加密货币挖掘恶意软件，发表在： 2019年IEEE安全与隐私研讨会上；
政府网站，2018年9月17日。可在线获得：https://textweb。com/n2019年5月19-23日；美国加利福尼亚州旧金山，IEEE，皮斯卡塔韦，美国新泽西州，2019年，
ews/indian-government-cryptocurrency-coinhive.访问时间：2021年4月9日。pp.175－192.
[79] T.加密货币黑客招募谷歌标签经理来走私银币矿工，[104] B。江，Y。刘，W。《合约模糊器：模糊了针对脆弱性的智能合约》
登记册，2017年11月22日。在线可用： https://www。登记册检测，见：第33届ACM/IEEE国际会议记录
.com/2017/11/22/cryptojackers_google_tag_manager_coin_hive/.(访问了9个自动化软件工程：2018年9月3-7日；法国蒙彼利埃，IEEE，
2021年4月)。皮斯卡塔韦，新泽西州，美国，2018年，页。259－269.
[80] M.加密挖掘，11月[105] C。刘，H。刘，Z。《防范：在智能合同中发现再入性漏洞》，
8， 2017.在线可用： https://www。theregister.第40届软件工程国际会议：同伴：27岁
kers_google_tag_manager_coin_hive /.（2021年4月9日通过）。2018年5月-6月3日；瑞典哥德堡，IEEE，皮斯卡塔韦，美国新泽西州，2018年，
[81] T.超过10万个Drupal网站很容易受到毒品分子的攻击。65－68.
（CVE-2018-7600），《坏数据包》，2018年6月4日。可在线获得：https://标记包[106] Y。傅，M。任，F。Ma等人：通过模糊测试检测EVM漏洞，
等。net/over-100000-drupal-websites-vulnerable-to-drupalgeddon-2-cve-2018-在：第27届ACM欧洲软件工程会议和会议联席会议
7600/.（2021年4月9日通过）。软件工程基础研讨会；2019年8月26-30日。
[82] T.坎蒂萨诺，YouTube广告劫持访客计算机挖掘加密货币，塔林，爱沙尼亚，ACM，纽约，纽约，美国，2019年，页。1110－1114.
纽温，2018年1月26日。在线可用： https://www。neowin.net/news/yout [107] V.Wustholz, M.哈维：智能合约的一个灰盒模糊器
ube-ads-hijacked-visitors-computers-to-mine-cryptocurrency/.(4月9日通过28日ACM欧洲软件工程联席会议
2021).软件工程基础研讨会；2020年11月8-13日；虚拟的
[83] C.奥斯本，密克洛蒂克路由器在大规模共抑制密码劫持事件，ACM，纽约，纽约，美国，2020年，pp。1398－1409.
竞选活动，ZDNet，2018年8月3日。在线可用： https://www。zdnet.com/arti [108] L.Luu, Y.Velner, J.特乌奇，P。Saxena，智能池：实用的去中心化
cle/mikrotik-routers-enslaved-in-massive-coinhive-cryptojacking-campaign/.集中采矿，在：第26届USENIX安全研讨会，温哥华，BC，加拿大；
（2021年4月9日通过）。2017年8月16日至18日。加拿大温哥华，美国加州伯克利，USENIX协会，
[84] L.Kelion，星巴克咖啡馆的Wi-Fi制造的电脑挖掘加密货币，BBC 2017，页。1409－1426.
新闻，2017年12月13日。[109] M.驱动器，K。Edalatnejad, B.福特等人，关于两轮多轮车的安全性
[85] C.IOTA加密货币用户损失了400万美元的聪明的网络钓鱼签名，在：第40届IEEE安全与隐私研讨会；2019年5月19-23日；
攻击，流血电脑，2018。在线提供，https://www。美国旧金山，加州，IEEE，皮斯卡塔韦，美国新泽西州，2019年，页。1084－ 1101.
r.com/news/security/iota-cryptocurrency-users-lose-4-million-in-clever-phishin [110] M.Drijvers。Gorbunov。Neven，Pixel：多签名的共识，在：第29位
（访问日期：2021年4月9日）。USENIX安全研讨会；2020年8月12-14日；在线，USENIX协会，
[86] L.《被关闭》是荒谬历史的最新一章，伯克利，美国，2020年，页。2093－2110.
CoinDesk，2020年2月26日。在线可用： https://www。coindesk.com/bus [111] Y.太阳，A。Edmundson, N.Feamster, M.蒋介石。反强奸犯米塔尔：
iness/2020/02/25/iota-being-shut-off-is-the-latest-chapter-in-an-absurdist-histo保护tor抵御主动路由攻击，见： IEEE安全研讨会
ry/.（2021年4月9日通过）。和隐私；2017年5月22-26日；美国加州圣何塞，美国新泽西州皮卡塔韦皮斯塔韦，
[87] L.布莱登巴赫，P。戴安，F。Tramer。朱尔斯，进入九头蛇：走向原则2017，页。977－992.
漏洞奖励和抗漏洞智能合约，在：27 USENIX安全[112] F。张，E。塞切蒂，K。克罗曼，A。尤尔斯，E。石，经认证的人
研讨会；2018年8月15-17日；美国马里兰州，USENIX协会，智能合同数据源，在： 2016年ACM SIGSAC计算机和计算机会议
美国加州伯克利分校，2018年，第3页。1335－1352.通信安全（中国化学会'16）；2016年10月24-28日；维也纳，奥地利，ACM，新的
[88] E.Hildenbrandt, M.萨克森纳，N。罗德里格斯等人，KEVM：一个完整的正式约克，纽约，美国，2016，页。270－282.
以太坊虚拟机的语义，在： 2018年IEEE31日计算机安全[113] A。马夫里多，A。Laszka，工具演示： FSolidM设计安全
基金会研讨会（脑脊液）；2018年7月9-12日；牛津，英国，IEEE，皮斯卡塔韦，新泽西州，以太坊智能合同，在：国际安全原则会议
美国，2018年，页。204－217.和信任；2018年4月14日至20日；塞萨洛尼基，希腊，施普林格，中国，瑞士，
[89] L.一个用于智能合同的分析工具。https://loiluu.com/oyente.h 2018, pp.270－277.
tml, 2016.2021年4月5日通过。[114] H.卡洛德纳，S。戈德费德，X。陈等人，仲裁者：可扩展的，私人的智能
[90] P.特桑科夫，A。丹，D。安全化：实际安全分析合同，在：第27届USENIX安全研讨会；2018年8月15-17日；巴尔的摩，马里兰州，
智能合约，见：2018年ACM SIGSAC会议论文集，USENIX协会，伯克利，美国，2018年，页。1353－1370.
计算机和通信安全（CCS '18）；2018年10月15-19日；多伦多，[115] S。所以，M。李，J。这是一个高度精确的安全验证者
加拿大，ACM，纽约，纽约，美国，2018，pp。67－82.以太坊智能合约，发表在： 2020年IEEE安全与隐私研讨会；
[91] S.卡拉，S。Goel，M。Dhawan等人，宙斯：分析智能合同的安全性，2020年5月17-21日；旧金山，加州，IEEE，皮斯卡塔韦，美国新泽西州，2020年，
网络和分布式系统安全（NDSS）研讨会，圣地亚哥，CA，pp。1678－1694.
美国，NDSS，莱斯顿，弗吉尼亚州，美国，2018年。[116] S.阿马尼，M。Bgel, M.Bortin, M.史泰博，以验证以太坊智能
合同字节码在伊莎贝尔/HOL，在：第七届ACM签署计划国际

认证项目和证明会议：2018年1月8日至9日：洛杉矶。ca。
美国，ACM，纽约，纽约，美国，2018年，页。66–77.

[117] T.荷兰阿卜德拉蒂夫。.–智能合约的正式验证，基于
用户和区块链行为模型，见：第九届IFIP新技术、移动性和安全国际会议（NTMS）：
2018年2月26-28日：巴黎，
法国，IEEE，皮斯卡塔韦，新泽西州，美国，2018年，页。1–5.

[118] T.太阳，W。Yu，区块链安全问题的正式验证框架
智能合约，电子产品9(2)（2020年），225年。

[119] A.Permenev，D.迪米特洛夫，P。Tsankov等人，VerX：智能的安全验证
合同，在： 2020年IEEE安全与隐私研讨会：2020年5月17-21日：旧金山，加利福尼亚
州，美国，IEEE，皮斯卡塔韦，新泽西州，美国，2020年，页。1661–1677.

[120] A.科斯巴，A。米勒，E。施，Z。温，C。鹰：区块链模型
密码学和隐私保护智能合同，见： 2016年IEEE安全和隐私研讨会：2016年5月22-26日
：美国加利福尼亚州圣何塞，IEEE，皮斯卡塔韦，美国新泽西州，2016，页。839–
858.

[121] M.Tran，L。Luu，M.S.康，我。本托夫，P。《明暗对比》：一个比特币混合器，使用
可信执行环境，在：第34届计算机安全应用年会（ACSAC）：2018年12月3-7日：圣胡安
，公关，美国，ACM，纽约，纽约，美国，2018，页。692–701.

[122] T.科伯。Kiayias，M.Kohlweiss，V.Zikas，神秘的俄罗斯人：隐私-
保存股权证明，见： 2019年IEEE安全与隐私研讨会：2019年5月19日至23日：旧金
山，加州，美国，IEEE，皮斯卡塔韦，美国新泽西州，2019年，页。157–174.

[123] S.致密的，K。温斯特，M。施耐德等人，Bite：比特币轻量级客户端隐私
使用可信执行，见：第28届USENIX安全研讨会：2019年8月14-16日：美国加州圣克拉拉
，USENIX协会，美国加州伯克利，2019年，页。783–800.

[124] S.鲍，A。Chiesa。Green，等人，Zexe：实现分散的私有
计算，见： 2020年IEEE安全与隐私研讨会：2020年5月18-21日：
旧金山，加州，美国，IEEE，皮斯卡塔韦，新泽西州，美国，2020，pp。947–964.

[125] F.Tramr，D.BonehK。帕特森，远程侧通道攻击匿名者
交易，在：第29届USENIX安全研讨会：2020年8月12-14日：在线，USENIX协会，伯
克利，加州，美国，2020年，页。2739–2756.

[126] T.赖特，比特币黑客四周年，和1200万美元的被盗BTC移动，联合图表，2020年8月4
日。可在网上获得：https://图表。com/ news/four-year-anniversary-of-bitfinex-
hack-and-12m-of-stolen-btc-moved.（2021年4月7日通过）。

[127]以太坊，将以太坊提升到全新的高度。https://ethereum.2021年3月1日。

[128] S.Dziembowski，L.Eckey，S.Fausd等人，Perun：虚拟支付中心结束
加密货币，见： 2019年第40届IEEE安全与隐私研讨会：19-23
2019年5月：旧金山，加州，美国，IEEE，皮斯卡塔韦，新泽西州，美国，
2019年，页。106–123.

[129] P.Gazi。Kiayias，D.锌，风险证明侧链，在： 2019年第40届IEEE
安全与隐私研讨会：2019年5月19-23日：美国旧金山，加州，IEEE，皮斯卡塔韦，美
国新泽西州，2019年，页。139–156.

[130] H.玉，我。NikolicR。Hou，P.Saxena，OHIE：区块链缩放变得很简单，在：
2020年第41届IEEE安全与隐私研讨会：2020年5月18-21日：圣
弗朗西斯科，美国，IEEE，皮斯卡塔韦，新泽西，美国，2020，页。90– 105.

[131] Visa，Visa简报。https://usa.签证com/dam/VCOM/download/corporate/
media/visanet-technology/aboutvisafactsheet.2021年3月1日。[132] IBM
，IBM区块链补充链解决。https://www.ibm.com/uk
-区块链、行业和供应链。2021年7月31日通过。

[133] VeChain，VeChain解决方案概述。https://vechain.com/solution/logistics.2021
年7月31日通过。

[134] X.余，H。区块链基础数据交换的系统、设备和方法，
2020年2月5日。新加坡专利申请No.10202000875X.

[135] W.Zou，D.Lo，P.S.Kochhar等人，《智能合同开发：挑战和挑战》
机会，IEEE跨。软件工程，47（10）（2019）2084-2106。

[136] E.德国，Crypto SWOT团队调查了2018年的经济数据。在线提供： https://steemit
。com/eosgermany/@eosgermany/the-crypto-swot-team-in调查-eos。

[137] P.戴安，S。戈德费德，T。Kell等人，Flash男孩2.0：去中心化的领先
交易所、矿工可提取价值和共识不稳定性，见： 2020年第41届IEEE安全与隐私研讨会
（SP）：2020年5月18-21日：旧金山，
美国，IEEE，皮斯卡塔韦，新泽西州，美国，2020年，页。910–927.

[138] Y.周，D。库马尔。Bakshi等人，错误：逆向工程以太坊的不透明
智能合同，在：第27届USENIX安全研讨会：2018年8月15-17日：巴尔的摩，美
国马里兰州，USENIX协会，伯克利，美国，2018，页。1371–1385.

[139] H.卡洛德纳，M。BMser，K.李等，《a的设计与应用
区块链分析平台，在：第29届USENIX安全研讨会：2020年8月12-14日：在线，USENIX
协会，伯克利，美国，2020，pp。2721–2738.

[140] G.徐，B。郭，C。苏，X。郑，K。梁，D。S.黄，H。王，我是不是黯然失色了？A
以太坊的日食攻击智能探测器，计算机。安全。88（2020）.

[141] P.W.嘘，量子计算的算法：离散对数和
保理，见：第35届计算机科学基础年度研讨会：1994年11月20-22日：圣达菲，美
国纳米，IEEE，皮斯卡塔韦，美国新泽西州，1994年，页。124–134.

[142] A.量子计算将如何影响区块链？同意系统（2019年12月3日）。可在线获得：
https://consensys。网络博客开发者对区块链的影响。（2021年7月31日通过）。

[143]NIST的后量子密码学项目进入了“选择轮”，国家
标准与技术研究所（NIST），2020年7月22日。在线可用：
https://www.nist.gov/news-events/news/2020/07/nists-post-
quantum-crypto图形程序进入筛选轮。（2021年7月31日通过）。

[144] I.Barmes，B。博世，量子计算机和比特币区块链，德勤，2021年3月13日。在线可用
： https://www。nist.政府/新闻-事件/新闻/202 0/07/nists-post-quantum-
cryptography-program-enters-selection-round.（2021年7月31日通过）。

[145] L.M，IOTA价格预测2021年及以后：该期待什么？学位，2021年1月25日。在线可用：
https://www。bitdegree.组织，加密，教程，价格预测。

[146] S.萨亚迪，S。B.Rejeb，Z。区块链的挑战和安全方案：a
调查，见：第七届国际通信和网络会议（ComNet）：2018年11月1日至3日：哈马梅特，
突尼斯，IEEE，皮斯卡塔韦，美国新泽西州，2018年，页。1–7.

[147] M.SaadJ。斯波尔丁，L。Njilla等人，探索区块链的攻击表面：a
系统概述，IEEE通信调查和教程22（3）（2020）
1977–2008.

[148] D.达斯古普塔，J。M.Shrein，K.D.古普塔，对区块链的安全调查
视角，银行和金融技术杂志3（2019）1-17。

[149] J.冷，M。周，J。L.赵，Y。黄，Y。边安，区块链安全：一项调查
技术与研究方向，IEEE服务计算学报，2020年。

[150] W.陈，Z。徐，S。Shi等，区块链应用的调查
领域，见：区块链技术与应用国际会议
（ICBTA）：2018年12月10-12日：西安，中国，ACM，纽约，纽约，美国，2018
，页。17–21.