区块链技术在投票系统中的应用：一个回顾

中国武汉大学网络科学与工程学院黄俊俊和DEBIAO先生，中国彭成实验室网络安全研究中心
MohammedS.OBAIDAT，IEEE研究员，SCS研究员，学院创始院长和教授
阿联酋沙迦大学计算与信息学、阿卜杜拉二世国王、约旦大学信息技术学院和中国北京科技大学
PANDI VIJAYAKUMAR，美国大学环境学院计算机科学与工程系
工程丁迪瓦南，印度
中国武汉大学网络科学与工程学院、山东计算机科学中心（济南国家超级计算机中心）、齐鲁理工大学（山东科学院）
KIM-KWANG雷蒙德赵，信息系统和网络安全部，大学-
美国德克萨斯州的圣安东尼奥大学

投票是个人或一组个人的意见或选择，无论是积极的还是消极的。然而，传统的投票系统往往是集中化的，已知它们受到安全和效率的限制。因此，出现了一种转向分散的投票系统的趋势，比如那些基于区块链的投票系统。后者是点对点网络中的一个分散的数字分类帐，其中由每个参与者维护数字签名和加密事务的只附加分类帐的副本。因此，在本文中，我们对基于区块链的投票系统进行了全面的回顾，并根据许多特征（如所使用的区块链的类型、所使用的共识方法和参与者的规模）对其进行分类。通过系统地分析和比较不同的基于区块链的投票系统，我们也确定了一些局限性和研究机会。希望这是这次调查

这项工作得到了中国国家自然科学基金会的支持。61972294和61932016)，湖北可行性科技项目专项项目(号。2020年AEA013)，湖北省自然科学基金会(没有。2020CFA052)和武汉科技项目。 2020010601012187).k。赵的工作只得到了云技术授权教授的支持。

作者地址：J.Huang和D。中国武汉大学网络科学与工程学院，430072，中国深圳彭成实验室网络空间安全研究中心，518000；电子邮件：hj10007@whu.edu.cn，hedebiao@163.com；M.S.Obaadat，阿联酋沙迦大学计算机与信息学院，27272，约旦大学阿卜杜拉二世信息技术学院，11942，北京科技大学，100083；电子邮件：msobaidat@gmail.com；印度大学工程学院计算机科学与工程系，604001；电子邮件：vijibond2000@gmail.com；M。罗，中国武汉大学网络科学与工程学院，430072，山东省计算机网络重点实验室，山东计算机科学中心（济南国家超级计算机中心），齐鲁理工大学（山东科学院），中国济南，250014；电子邮箱：mluo@whu.edu.cn；K.-K。R.赵，德克萨斯大学圣安东尼奥分校信息系统和网络安全系，美国圣安东尼奥，德克萨斯州78249；电子邮件：raymond.choo@fulbrightmail.org.

art60$15.00
https://doi.org/10.1145/3439725

将深入了解区块链在投票系统和设备未来研究议程中的潜在效用。

中国化学会概念：安全和隐私→加密；特定于领域的安全和隐私架构；隐私保护协议；

其他关键字和短语：区块链、基于区块链的投票系统、电子投票、隐私保护

ACM参考格式：

黄俊、德彪、欧伟达、维光光、罗敏、赵金光等。 2021.区块链技术在投票系统中的应用：一个综述。*ACM组合。冲浪。*第54、3、第60条（2021年4月），28页。

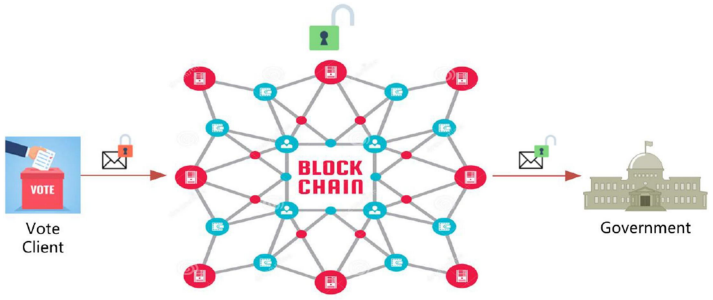
https://doi.org/10.1145/3439725

1 产品简介

投票系统已经逐渐远离纸质选票和投票站。[1] 近年来，人们已经逐渐转向使用电子投票系统。在这样的系统中，选民（包括海外选民）可以在线投票，投票可以实时处理。最后，投票记录和结果将存储和管理在一些数据库中，这些数据库通常是集中（例如，由国家选举委员会控制）。传统的基于纸质的投票系统仍然在许多情况中使用。众所周知，他们有许多缺点。首先，纸质选票由staf进行处理，因此有可能会意外或有意地修改选票内容。此外，根据实际设置（例如，在独裁国家），选民可能会受到身体胁迫。由于投票记录和结果是集中存储和管理的，选民很难验证他们的选票计算正确。由于某些自然或人为因素（如洪水、地震或纵火等自然灾害），投票记录和结果总是有被破坏的风险。虽然电子投票系统在理论上可以潜在地提高投票过程的安全性和效率，但这些好处并没有真正转化为实践。除了目前对美国使用电子投票系统的担忧之外。选举时，集中存储和管理投票记录和结果[18,20]存在限制。因此，最近有人努力设计分散的电子投票系统，比如那些基于区块链的系统。区块链是点对点(P2P)网络中分散的数字账本，由每个参与者维护数字签名和加密交易的附加账本的副本。区块链是比特币等加密货币的基础如以太坊等合同。

区块链具有许多特性（例如，分散化、透明度和不变性），这使得它在设计分散化的电子投票系统方面具有吸引力。例如，参与者可以使用区块链地址来表示他们的身份；因此，实现了伪匿名性。传统投票系统中的所有操作都可以定义为选民和候选人之间虚拟资产的交易或转移。此外，交易的内容可以被加密，以保护参与者的隐私。候选人获得的投票次数是候选人的地址收到的事务处理或虚拟资产的数量。投票过程结束后，与投票事件相关的所有交易将永久不可可逆地存储在分布式区块链中，确保投票过程的完整性。利益相关者

[1]在传统的纸质投票系统中，选民们会到最近的投票站去投票。在投票截止日期后，所有的选票都将由一些受信任的实体手动清点，如国家的选举委员会。最终，铸造的选票和投票结果将被安全地储存和管理在一些档案场所，在预定的一段时间内。



图中示。1. Ã基于区块链的电子投票的逻辑。

参与者可以随时随地查看和核实投票记录。基于区块链的电子投票[34]的逻辑如图1所示。

理论上，基于区块链的投票系统比传统的投票系统有许多优势，如分散化、透明度和不变性。

(1) *分散化*。区块链网络中的每个节点都有对所有事务的完整备份。因此，单个节点的故障或不可用性不会影响整个区块链网络。这使得基于区块链的投票系统更加健壮。
(2) *透明度*。一旦投票记录作为交易存储在区块链中，就可以以最小的修改风险进行审查和验证。因此，基于区块链的投票系统更为可信。
(3) *不变性*。一旦事务被验证并附加到区块链上，结果就不能再被修改了，这可以通过使用安全的哈希函数来保证。对单个节点中的区块链的修改不会影响整个区块链网络的一致性。

尽管有承诺，现有的区块链平台仍然有许多挑战，比如与吞吐量、隐私和身份验证相关的挑战。

(1) *吞吐量*。吞吐量用每秒成功的事务数来衡量。在全国选举活动中，将在短时间内产生大量的投票交易，这需要区块链网络中的高吞吐量。然而，现有的区块链平台，特别是公共区块链平台，通常没有高吞吐量。例如，比特币网络具有每秒约7[16]的交易(TPS)，以太坊平台具有约8[15]的TPS，而超分类帐结构平台具有40到500[44]之间的TPS。
(2) *隐私权*。区块链地址是随机生成的，这对选民匿名投票有部分帮助。然而，对参考文献[4,22]的研究表明，用户的比特币交易可以被链接起来，以揭示用户的信息。Bir尤科夫等人。[5]还提出了一种将用户假名链接到IP地址的方法，即使用户是在网络地址转换或防火墙后面。这给选民带来了个人安全风险，特别是在独权国家。
(3) *正在进行身份验证*。在计算系统中，目前的认证方案需要人类的认知能力来记住许多复杂的标识和密码，或依赖于一个受信任的第三方(TTP)，从而有一个额外的攻击向量[55]。在分布式区块链环境中，特别是那些不依赖TTP的环境中，实现安全验证方法可能一个挑战。

人们对基于区块链的电子投票系统的兴趣部分体现在少量关于该主题的文献综述和调查文章中。例如，在参考文献[50]中，作者调查了基于区块链的投票系统的特征。然而，用例和技术分析的深度都不够充分。参考[32]的作者分析了将区块链应用于在线投票系统时可能发生的制度和技术问题。然而，用例是独立分析的，这些用例之间没有比较。在参考[31]中，提出了一些现有建议的文献综述，以及它们提出的方法和局限性。然而，该审查缺乏技术分析。在参考[1]中，对不同基于区块链的投票系统进行了系统调查，重点关注区块链的可行性和适宜性。但是，并没有讨论任何用例。

为了为文献空白做出贡献，在本文中，我们首先重新审视区块链，然后对不同基于区块链的投票系统进行系统的分析和比较。基于综述，我们然后确定了一些未来的方向。

本文的其余部分组织如下。下一节介绍了传统的投票制度及其缺点。接下来的两个部分概述了区块链技术和基于区块链的投票系统所面临的挑战。在第5节和第6节中，我们将回顾一些用作投票系统的基于区块链的投票系统。在第7节中，我们对经过审查的投票系统进行了比较和分析。在第8节中，我们为基于区块链的投票系统提供了一些更广泛的观点。最后，我们在最后一节中结束本文。

2 常规的投票制度

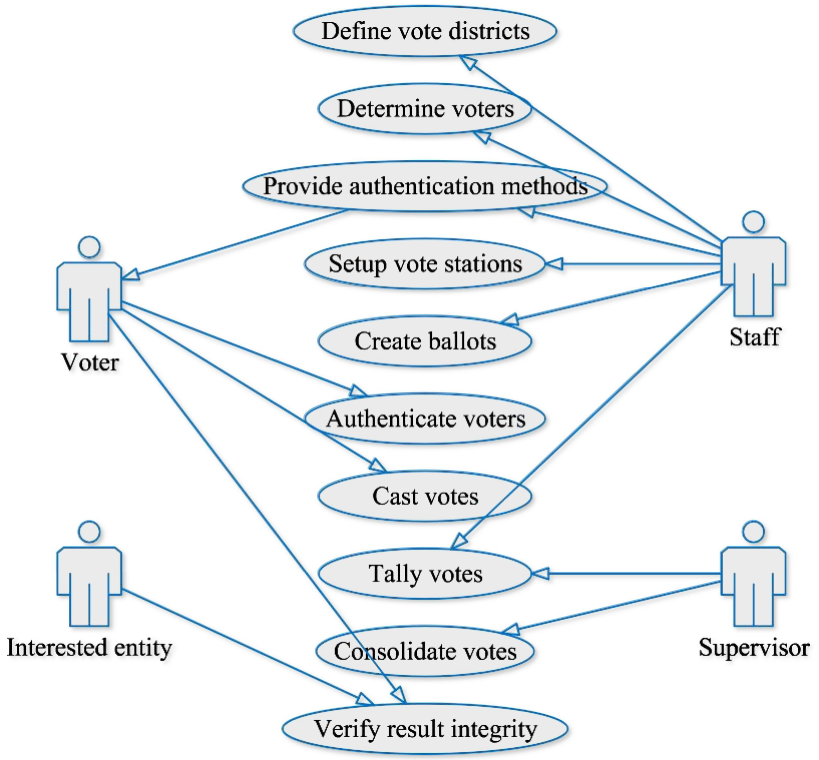
在本文中，我们广泛地将手动（或基于纸张的）投票系统和现在的电子投票系统定义为传统的投票系统，因为它们具有相同的设计原则和安全级别。接下来，我们将介绍这样一个普遍的传统投票模式和相关的挑战。

2.1 常规的投票模式

投票系统在我们的日常生活中很常见，因为它们被用来帮助集体表达我们的意见。在一个国家、州、省或县，公民可以投票决定一个提案是否可以通过。在一家公司中，董事会成员会对重要的决定进行投票。在学校里，学生和老师会投票决定谁将担任一个职位。

投票系统的组织方式不同，并针对不同的群体。然而，他们通常遵循相同的投票原则，并尽可能尽可能反映选民的意愿。以下是投票系统[25]的共同原则。

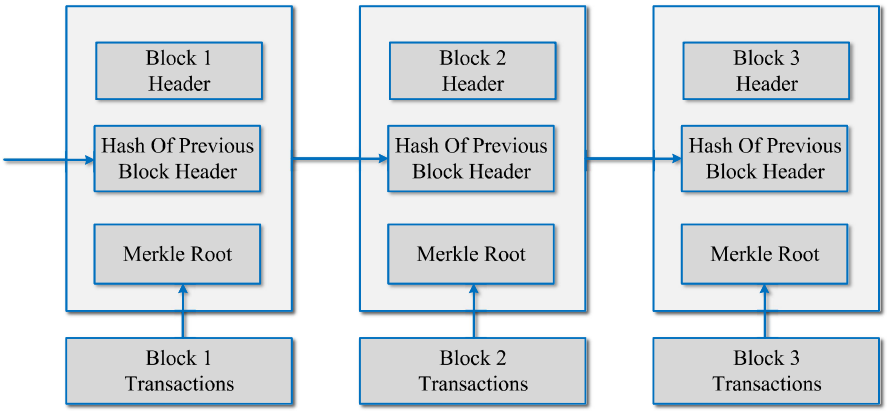
(1) *无记名投票的原则*。选民的真实身份不应记录在选票中。
(2) *平等的投票权*。每个选民都有同样的投票权，除非在某些情况下考虑了投票的分量。
(3) *填写选票的自由*。不得以任何理由强迫或引诱选民。
(4) *候选人不需要出席*。候选人可能不出席投票。
(5) *投票结果是最终的结果*。投票结束后，选举结果必须同意投票结果。
(6) *投票结果无法修改投票结果*。投票结果确定后，不得进行任何变更。



图中示。2. A大选投票模式的用例。

格里兹利斯[25]为传统投票系统提供了一般模型，大选投票模型的用例如图2所示。该模型中有10个一般步骤，如下所述：

(1) *定义投票区*。在投票前，所有参与者可以根据自己的实际位置分成几部分，这样可以到相应的地区投票。此外，候选人将在这一时期被确定。
(2) *确定选民人数*。这个阶段决定了谁可以投票或谁不能投票。一般来说，所有的成年人都有权在全国选举中投票。
(3) *提供身份验证方法*。执行对选民身份验证。身份验证方法应该足够，因此选民可以选择适当的方法来验证他们的身份。
(4) *设置投票站*。在确定了投票区后，应在一个地区设立至少一个投票站作为基础设施。
(5) *创建选票*。这些选票将在此期间创建。投票的内容应包括所有候选人的信息，以便选民可以在投票过程开始时选择相应的候选人。
(6) *通过身份验证投票者*。在选民投票前，必须核实选民的身份。
(7) *由演员进行投票决定*。选民们会到相应的投票站去投票。此过程应秘密进行。



图中示。3.A区块链插图。

(8) *投票投票*。执行以验证演员投票，并计算每个候选人获得的票数。这个过程将在每个地区进行。在所有选民完成投票后，将总结所有选区的投票结果。
(9) *合并投票结果*。投票结束后，应对投票结果进行妥善的保存和管理。没有人可以以任何理由修改投票结果。
(10) *验证结果的完整性*。如果任何感兴趣的实体想要证明投票程序已经正确进行，那么该组织可以出示证据。

2.2 传统的投票制度所面临的挑战

传统的投票系统主要基于纸质选票和手动操作，或来自电子投票系统的集中数据库。很难保证整个投票程序的安全。传统的投票在许多方面都有缺点。首先，很难保证选民的匿名性。在传统的投票系统中，选民可以通过使用身份证等真实身份来获得选票。在某些情况下，选民甚至被要求在纸质选票中填写个人信息，这将导致选民隐私的披露。然后，在投票过程结束时，基于纸质的投票系统会手动计票。一方面，人为的错误很难避免，这使得投票结果很难反映选民的意愿。最后，大多数传统的投票系统会将投票结果保存在一个集中的数据库或纸质档案中。集中数据库或纸质档案一旦遭受自然灾害，就会导致投票记录的丢失。这种方法也使选民很难核实他们的选票是否被正确地计算出来。

3 区块链技术

区块链是P2P网络中的一个分散的数字账本，由每个参与者维护数字签名和加密事务的附加账本的副本（如图3）。它是比特币等加密货币的核心技术。2008年10月，中本公司在比特币白皮书[43]中首次提出了区块链的概念。在接下来的几年里，比特币成为了加密货币的核心组成部分。区块链技术被认为是继蒸汽机、电力和互联网[13]之后的下一代颠覆性核心技术。如果蒸汽机释放了人们的生产力，那么电力就解决了人们的基本生活需求，互联网完全改变了信息的传递方式，那么区块链，作为一种构建信任的机器，将完全改变人类价值的传递方式。

区块链主要解决交易的信任和安全问题。针对这两个问题，提出了以下技术创新方案。

(1) *分布式分类帐*。整个区块链网络由对等者网络[51]中的多个节点组成，以维护分布式账本。每个节点都有对分布式分类帐的完整备份，通过对等网络和共识机制来维护所有备份的一致性。不同的节点互相监督以验证事务，并同时互相作证。这些节点保持着整个区块链网络的顺序。
(2) *不对称的加密和授权*。区块链中存储的数据是公开的，但与账户相关的数据，如地址、公钥、私钥等，都使用非对称加密技术进行加密。数据访问只有在数据所有者的授权后才能进行，这样可以将公共数据和私有数据分开，便于管理，保护用户的隐私。
(3) *共识机制*。整个区块链网络中的节点如何达成一致以确定交易的有效性，这既是确定交易有效性的手段，也是防止数据篡改的手段。区块链有许多共识机制。它们适用于不同的应用程序场景，并在效率和安全性之间取得平衡。比特币使用工作证明(PoW)，只有在有人控制了网络中超过51%[37]的节点时，才能创建一个不存在的交易。如果整个区块链网络中有足够的节点，这基本上不会发生，从而消除了欺诈的可能性。

综上所述，区块链技术具有以下重要特征。

(1) *分散化*。整个网络都没有中央统治者。该系统依赖于网络上多个参与者的公平约束，因此每个节点具有平等的权利和义务，每个节点存储块链上的所有数据。即使节点被损坏或攻击，对分类帐也不会存在威胁。区块链上生成的数据是建立在加密和数学算法的信任上，而不是集中机构。一种分布式的点对点交易系统，其中双方都可以直接进行交易，而不需要第三方的可信背书。
(2) *不变性*。如果分类帐由一个或几个人控制，那么欺诈的可能性非常高，但如果每个人都有分类帐的副本，那么除非想要更改特定记录的超过51%的参与者，否则任何篡改是不有效的。这是集体维护和监督的优势。当节点生成一组数据并被大多数节点识别时，数据写入区块链，每个节点复制并保存。因此，区块链数据难以改变。这些条件非常严格，几乎不可能被篡改，从而确保了数据的真实性。
(3) *不否定*。在发送事务时，发送方需要使用其私钥签名事务数据。此签名始终可以使用签名者的公钥进行验证。根据签名的特征，交易发送人不能否认自己发送了某一交易，从而实现了不否定
(4) *透明度*。在公共区块链中，除加密的交易主体身份信息外，其他信息打开，任何参与者都可以通过公共端口查询相关记录。区块链网络中的任何参与者都是平等的，并且可以与任何人交互。参与者发送的任何事务都具有被网络中的其他节点处理和验证的相同概率。

(5) *假名词*。虽然区块链上的数据都是公开的，但区块链可以通过随机化区块链地址，在一定程度上保护用户的隐私。例如，在参考[56]中，一个应用程序旨在利用区块链地址的伪匿名性来保护用户的私有数据。然而，区块链地址的伪匿名性不能完全保护用户的隐私，并且可以在多个事务[2]后推断出用户的真实身份。

(6) *可追溯性*。简而言之，区块链是一个分散的数据库，数据由节点存储，节点将数据分散到连接到网络的每台计算机上，不受集中服务器的控制。由于存在大量节点，区块链的数据存储可以防篡改。我们可以跟踪区块链中的数据。我们日常生活中生成的任何数据都可以通过区块链记录，交易编号和时间戳是唯一的，所以我们的交易也可以跟踪，方便一些机构和部门管理。

3.1 智能合同

智能合约并不是完全“全新的”。计算机科学家和密码学家尼博在1994年首次提出了“智能合约”的概念。所谓的智能合同是自动程序合同，满足预设条件后可以自动触发。例如，当付款的条件得到满足时，保险公司会自动偿还客户。

区块链使智能契约成为可能，因为区块链提供了一个可靠的代码执行环境。智能合约以数字形式写入区块链，区块链技术的特点确保整个存储、读取和执行过程透明、可追溯，不被篡改。同时，利用区块链的共识算法构建了一组状态机系统，使智能契约能够有效地执行。智能合同允许在没有第三方的情况下进行可信的交易，这是可跟踪的和不可逆转的。智能合约的出现可能会对业务合作造成重大中断。例如，以往的业务合作需要第三方公共信托机构的参与或第三方的担保。基于区块链的智能合约的出现已经大大减少了人类的参与。智能合同适用于所有情况。它们可能是金融服务、众筹协议、保险费、违约合同、信贷执行等等。

3.2 区块链系统的分类法

区块链技术可分为三类：公共区块链、私有区块链和联盟区块链。它们都有自己的特点和不同的应用程序，如表1所示。

公共区块链。公共区块链是最早和使用最广泛的区块链。它是指
到一个完全分散的区块链，比如比特币区块链。世界上任何个人或群体都可以发送交易，交易可以获得区块链的有效确认，任何人都可以参与其共识过程。共识过程的参与者通过加密技术和内置的经济激励措施来维护数据库安全。最常见的共识机制包括PoW、堆栈证明(PoS)和堆栈委托证明(DPoS)。世界上的每个人都通过一个P2P网络参与了达成共识的过程。

那么，如何让人们积极参与，维护公共区块链的稳定呢？硬币作为一种激励机制被引入，这意味着公共区块链必须

具体情况详见表1。区块链的分类法

	公共区块链	专用区块链	联盟区块链
参与者	任何人	个人/公司	联合体成员
共识机制	工作俘	分布式一致的算法。	分布式一致的算法。
簿记员	任何人	自定义的	联合体谈判
激励机制	需要的	不需要的	可选的
分散化	分散化	集中化的	多中心的
验证速度	缓慢的	快速的	中等
交易记录数据	公共	半公开的	私人的
“网络”	P2P网络	快速的网络	快速的网络
典型的应用程序	加密货币种	审核内容	支付/结算

发行像比特币这样的硬币。一旦公共区块链无法保持其稳定，硬币将一文无值。

私有的区块链。私有区块链是指具有某种集中控制方式的区块链小跑。只要使用区块链分类帐技术进行簿记，簿记员就可以是一家公司或一个个人，而私有链与其他分布式存储方案并没有太大的不同。唯一参与的节点是用户本身，对数据的访问和使用有严格的权限管理。

私有区块链不对公众开放，只有授权节点可以参与和查看区块链数据。采用私有区块链的主要群体是金融机构、大型企业和政府部门。私有区块链的典型应用是由央行开发的发行数字货币的区块链。这个私有的区块链只能由中央银行保存，而且个人不可能参与其中。还有一些大公司在开发私有区块链，如阿里巴巴、百度、jd.com，主要关注区块链在数据安全、供应链等行业困境中的作用。

联盟区块链。联盟区块链通常仅限于一个特定的成员集团和有限数量的第三方。在内部，多个预先选择的节点被指定为簿记员，新块的生成由所有预先选择的节点决定。其他后期加入的节点可以参与事务，但不打扰簿记。

联盟区块链是公司和组织之间的联盟模式。在区块链上维护数据的节点都来自联合体的公司或组织，记录和维护数据的权利掌握在联合体成员手中。采用联盟区块链的主要集团有银行、证券、保险、集团企业等。联盟区块链不像公共区块链那么开放，这削弱了分散化，这是它的一个缺点。目前，联盟区块链的典型项目是超分类帐项目。目前，有十多个不同的利益相关者，如ABNAMRO、埃森哲等，可以满足各自行业的需求，简化业务流程[9,26,52]。

4 基于区块链的投票系统所面临的挑战

将区块链技术应用于投票系统还有很长的路要走。与传统的投票系统相比，区块链投票系统在认证、匿名性、强制自由性和可审核性方面更为严格。应在实际生产的投票系统中满足这些要求。一个基于区块链的投票系统的建议需要付出一些努力来解决这些问题。

具体详见表2。建议书的覆盖范围

	身份验证	匿名性	胁迫自由	可审计性
[40]	是的	是的	否	否
[36]	是的	是的	否	是的
[3]	是的	部分的	否	否
[6]	否	是的	否	是的
[41]	是的	是的	是的	是的
[53]	未提及	是的	否	否
[29]	是的	是的	部分的	未提及

如上所述，一个良好的基于区块链的投票系统应该涵盖所有方面，包括但不限于身份验证、匿名性、强制自由性和可审核性。我们研究了近年来提出的几种方案，并列出了它们的覆盖范围；结果总结在表2中。

4.1 身份验证

在基于区块链的投票系统中，参与者使用区块链地址等虚拟身份进行投票。然而，在现实生活中，只有个人才有投票权。因此，虚拟身份必须绑定到现实生活中的身份，如社会安全号(SSN)，以确保每个参与者都是合法的。

身份验证并不困难，而且有许多成熟的解决方案。然而，在不揭示真实身份的情况下进行身份验证是很复杂的，特别是在没有TTP的环境中。在在线投票的情况下，都应考虑到安全和便利性。在大多数方案[45]中都使用了远程身份验证。然而，个人电脑和开放的互联网并不完全安全。在线系统中总是存在一些漏洞。在全国选举的情况下，应该首先把安全放在首位；大多数投票站，是专门供选民投票的终端。在此场景中可以使用远程身份验证，除非有针对远程环境的安全远程身份验证方案。

4.2 匿名性

为避免外部环境的干扰，所有参与者应在投票结束前保持匿名。匿名性是任何投票系统的一个重要方面。选民的意见可以在一个匿名的环境中自由地表达。因此，保持匿名是保护选民隐私的最基本的原则。

已经有一些方法可以实现匿名性，比如Rivest、Shamir和Tauman在2001年[49]发明的戒指签名，Chaum和Heyst在1991年[12]引入的团体签名，以及Chaum在1981年[11]描述的混合网络概念。一些现有的建议使用上述一种或多个技术来实现匿名性。此外，还有一些其他的方案通过设计一个特殊的区块链或交易结构来实现匿名性。例如，H贾尔马森[29]在他的提议中设计了一个特殊的结构，即事务不记录发送人。

4.3 胁迫自由

投票系统中的胁迫意味着某人被迫投票给候选人。基于区块链的投票系统必须没有强制性，这不是一个容易解决的问题。因为一个基于虚拟互联网的投票系统很难区分一个现实生活中的选民是否受到威胁。有许多建议已经解决了胁迫的问题。我们相信这一点很好

基于区块链的投票系统的方案应涵盖从投票开始到结束的各个方面。虽然强制问题不能完全解决，但我们至少应该提出一些方法来减少它。

一些现代的电子投票系统允许在其政策中进行多次投票，以减少胁迫。这样，选民就可以放置一张新的选票来撤销旧的选票。这种系统应该易于使用和理解，以防止胁迫。

Civitas[14]是一个电子投票系统的开源解决方案。它被设计成完全分布的，是少数为数不多的系统之一，证明自己是强制系统自由。西维塔人通过使用假证件来避免胁迫。要创建假凭据，选民需要其专用指定密钥，然后运行一个本地算法。这些虚假的私人证件与奇维塔斯提供的官方证件没有区别，但用它们加密的选票将不会在选举的最后阶段进行统计。使用这种机制对密码器进行攻击是不可能的，因为编码器永远无法确定使用了真实凭证还是假凭证。

4.4 可审计性

可审计性对投票系统的安全至关重要。要审核整个投票过程产生的数据，从投票开始到结束，所有与投票相关的数据都应进行详细记录。它对检查基于区块链的投票系统的安全状态非常有帮助。

区块链是可审核的，因为事务中包含的所有数据永久不可可逆地存储在区块链中。我们可以通过验证交易发送人和分类帐提交人签署的签名来检查交易的有效性。类似地，在基于区块链的投票系统中，由整个投票过程生成的数据可以包含在相应的交易中。然而，有一件事应该在我们心中记住，参与者的隐私不容忽视。选民应该在整个选举过程中保持匿名。没有人，甚至是审计员，能得到与选民有关的信息。此外，审计权限不能由一个实体控制，它可以由如参考[21]中报告的多方协议授权来分散权限。

5 对基于区块链的投票系统的审查

我们研究了一些最近与基于区块链的投票系统有关的论文。这里我们简要描述一些典型的情况。

5.1 具有最大选民隐私的董事会投票的明智合同

Patric等人。[40]展示了第一个使用区块链技术实现的分散和自统计的投票协议。这是一个小规模的董事会投票方案，具有最大的选民隐私。

在上述场景中，选民只有两个选择：二进制1表示是，二进制0表示不是。如果在一次投票中有两个以上的选择，则该协议可以扩展到三个或三个以上的选择，但在建议书中只描述了最简单的方案。

在协议运行前，应选择G组和д组的生成器等现场参数。此外，还将其设置为P_1，P_2，，$P...n$代表所有选民；每个选民秘密选择一个投票键x_i。该协议的左侧可以分为两个步骤。

第1步。P_i广播д^{x_i}以及x的零知识证明$_i$(菲亚特-Shamir启发式[23])。然后所有的选民都可以计算出$Y_i=\prod_{j=1}^{i-1} д^{-J}/\prod_{j=i+1}^{n} д^{-J}$，让$Y_i=д^{-J}$。以上计算可以满足

$$\sum_i x_i y_i = 0.$$

第2步。每个投票人P_i广播д$^{i\,i}$д^i，其中，v_i是选民的选择（0或1）和两个零知识证明（CDS技术）吗$_i$以证明该v_i可以为0或1。然后是任何人

（包括非选民）可以计算Π д $^{x_i y_i}$ д ^{v_i}和$y = д^{V_i}$。在了解了y的值后，我们可以得到v=的值$_i V_i$通过从零遍历所有可能的指数（这是该协议是小规模董事会投票的原因之一）。v的值是投赞成票的选民人数，我们可以通过从总数中减去v来获得投反对票的选民总数 选民们。

上述两个步骤是基于开放投票网络协议[17]。在最初的协议中，最后一个选民可以在广播他或她的投票之前计算结果，并且根据结果，最后一个选民可以改变投票。为了解决问题，以太坊的实现使智能契约首先收集所有选票，然后管理员计算结果并将其发布给所有选民。

5.2 使用区块链的电子投票服务

Lee等人。[36]提出了一种使用区块链技术的国家级选择方案。该计划参与了三个实体：举办投票活动的组织(表示Or д)，它拥有所有选民的真实身份(ID)、TTP(他们不知道有关ID的信息)和选民。投票活动可分为四个步骤。

第1步。准备工作。在投票开始前，每个选民和候选人应该有一对公钥和私钥以及相应的区块链地址。密钥对用于签名事务并验证签名的有效性。区块链地址用于发送事务。**第2步。注册。**每个投票者秘密地选择一个消息m，然后计算消息的哈希值H(m)，并将其发送到Or д以注册选民(假设每个投票者都有一个帐户链接到他的身份证来登录注册系统)。

第3步。获得正确的投票权。选民将他们秘密选择的消息的哈希值H(m)发送给TTP，然后TTP将接收到的H(m)发送给Or д，询问H(m)是否由相应的选民在Or д中注册。Or д答案是表示投票人已经在Or д中注册；否则，中止接收的H(m)如果答案是是，则TTP记录H(m)和H(pubkey)表。.

第4步。投投票表决。在投票过程中，任何人（包括没有投票权的选民）可以将交易发送到相应候选人的区块链地址。投票结束后，只有登记选民的交易将计算，新的交易将涵盖旧的交易。

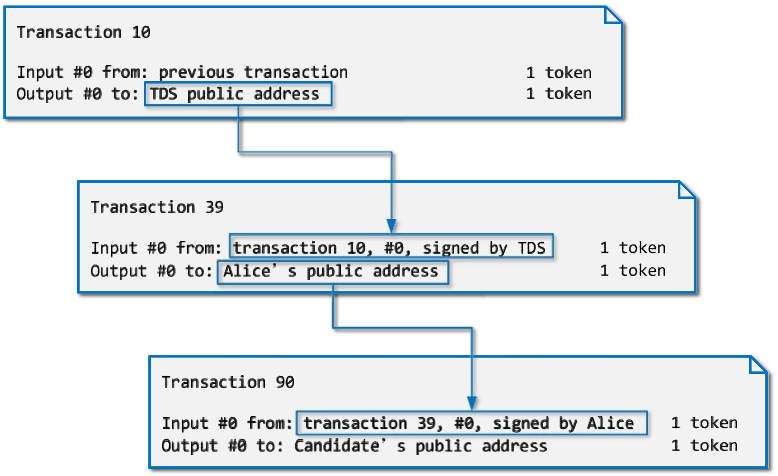
该方案独立于平台无关。可以使用自构建的区块链网络，但计算能力应均匀分布，否则，一个节点就有作弊的能力。目前的比特币区块链网络也可以使用。其优点是，我们不必担心计算能力的分布不均匀，但缺点是发送交易会花费比特币。

该方案是安全的，因为Or д和TTP都只有关于投票的部分信息。选民选择了一个秘密信息m作为他的临时身份。Or д拥有所有选民的真实ID和H(m)，但是公钥和相应的区块链地址，所以Or д不知道是谁投票给了谁。TTP知道H(m)和公钥，但都是真实的身份，所以TTP也不知道谁投票给了谁。

5.3 一种基于比特币的端到端投票系统

[6]提出了一种基于比特币的端到端投票系统。本文的主要思想是使用区块链来存储投票，并将投票与比特币代币联系起来。

投票过程大致分为三个阶段：投票前阶段、投票阶段和投票后阶段。



图中示。4. A投票的审核路径。

预投票阶段。候选人使用他们的比特币地址来进行候选人提名。被提名的候选人的地址将被公布给所有选民。在投票开始前，所有的选民都需要进行登记。选民会生成一对可供注册的公钥和私钥。成功注册的选民将收到一定数量的比特币作为后续投票的标志。应注意，令牌的发出是一个匿名的过程。选民的真实身份不能与他的公共比特币地址联系起来。为了实现这一点，作者引入了匿名内核系统(RFC8062[42])和盲签名[10]。只有通过匿名内核服务器进行身份验证的选民才能从令牌分发服务器(TDS)接收该令牌。

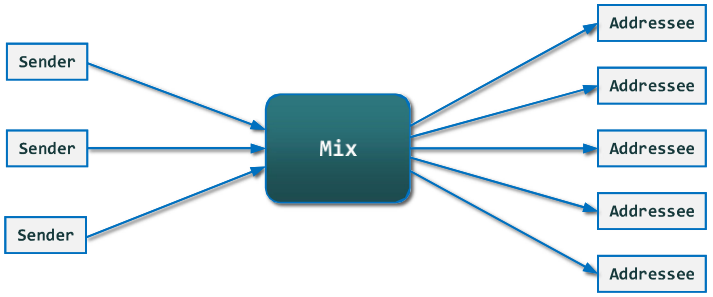
投票阶段。有投票权的选民是那些有标记的人。合法选民
可以很容易地通过该标记来标识。投票铸造只是通过将代币发送到相应的候选比特币地址来完成的。投票的传输和验证对应于比特币网络中的交易发送和块挖掘。

投票后的阶段。投票结束后，需要进行计票。的
候选人所获得的票数是相应的比特币地址所收到的令牌数。审计投票结果对选民来说也很重要。比特币使用的未用交易输出模型使所有参与者都很容易审计投票事件的整个过程。例如，Alice发送进行投票的交易必须包括由TDS签名的TDS交易的输入和相应候选人公共地址的输出。审核路径，如图4所示。

5.4 分布式投票系统的设计

克里斯蒂安·[41]提出了一种使用区块链技术的分布式投票系统方案。该方案假设每个人都有一个电子ID(eID)，以及由政府生成的一对公钥和私钥。作者定义了一项投票方案。该协议有自己的加密货币，称为气球币。在投票期间，选民们用他们的电子身份证进行登记。经该系统授权的选民将获得一张气球硬币。在投票时，选民只需将他们的气球硬币转移到候选人的地址。计票是为了计算候选人地址中的气球硬币的号码。

就像比斯塔雷利之前提出的方案一样，投票和计票都是相同的操作。然而，实现安全性和协议细节的方法是不同的。



图中示。5.关于混合网络是如何工作的的说明。

克里斯蒂安的计划使用了修改后的宣誓证据来达成共识。该共识算法将从所有完整的节点中选择提交节点，这使手机和平板电脑能够成为节点。只要在投票期间有足够的节点运行，计算能力就会均匀分配。因此，安全将得到保障。

要记录选民和投票服务器的数据，系统引入日志服务器。它对审计活动很有帮助。但是，该日志服务器并不是对所有参与者都是公开的。选民与投票服务器之间通过专用通道的交互，与普通通道没有区别，否则会引起攻击者的注意。

投票内容采用非对称加密算法加密，私钥采用阈值加密分离。必须涉及到多个权威机构，才能获得投票的内容。这是一种防止腐败和攻击的有效方法。

选民可以投票不止一次，新的投票将涵盖旧的投票。最近的投票是最后的投票，之前的投票将被放弃。它有助于防止投票胁迫。

为了提高投票系统的匿名性，将混合网络引入了系统中。当选民投票时，混合网络会使选民和投票服务器之间的通信难以追踪。混合网络洗牌发送人地址并按随机顺序发送，图5显示混合网络的工作方式。

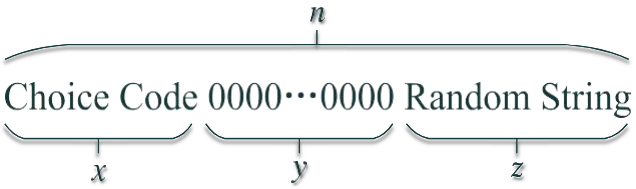
5.5 一种基于区块链的电子投票协议

Liu和[38]和Wang[38]提出了一种基于区块链技术的电子投票协议。这是一个通用的投票协议；它不依赖于任何区块链平台，也不需要一个值得信任的第三方。本协议要求每个选民拥有两对公钥和私钥，一对是签名，它的公钥可以知道。另一个是通过区块链投票；它的公钥应该保密，让选民匿名。

此协议涉及三个角色：投票人、组织者和检查员。组织者是举办投票活动的实体。组织者需要核实合格选民，记录投票信息，并在投票过程中与合格选民进行互动。检查员的存在是为了限制组织者的权力，并监督组织者的行为。该协议大致分为四个步骤。

注册阶段。所有潜在的选民都需要登记在他们的个人信息中
以及他们签署的公钥。组织者将根据合格选民的个人信息来记录他们。

预投票阶段。选民需要通过生成一个投票字符串来准备他们的选票
如V)，投票字符串中包含三部分：x位选择代码，代表选民的选择；y位零，表示格式良好的投票；以及z位随机字符串，它不同于包含相同选择代码的不同投票；参见图6。在投票字符串之后



图中示。6.Ã投票字符串公式。

准备好了，选民与组织者和检查员互动，让他们在V的点击上盲目签名。最后，投票串V和收集的V签名形成一个完整的投票。

投票阶段。选民构建一个交易，其中包含完整的投票。然后，他们使用他们的秘密公钥将事务发送到区块链网络。

投票后的阶段。计票只是在收集所包含的投票字符串
通过所有的交易记录。

应注意，发送事务时无法跟踪的IP的信息。因此，建议选民通过代理或TOR网络发送他们的交易。另一个问题是，投票的中间结果对所有参与者都是公开的，这可能会对最终结果产生影响，因此建议使用允许的区块链。另外，我们可以用组织者的密钥加密选票；只有当投票过程关闭时，组织者才能解密结果。

6 正在使用的投票系统

随着区块链技术的发展，世界上一些地方已经使用区块链进行投票。接下来，我们将介绍一些正在使用的投票系统。

6.1 筑波公司在日本首次部署了在线投票系统

2018年8月，日本使用区块链和我的号码卡进行了第一个在线投票验证测试[30]。该测试是在茨城县的筑波市进行的。政府鼓励其公民充分利用其智力和创新技术，提出新的思想，为社会服务。这些新技术包括物联网、人工智能和大数据分析。政府通过审查阶段支持优秀的工作。在最后的投票阶段，他们使用基于区块链的投票系统从候选人中选择最终支持的作品。我的号码卡被用来识别有效的选民。

公平投票制度一般需要满足以下四个基本条件：(a)区分合法选民和非法选民，(b)投票程序应保密，(c)应阻止选民多次投票，(d)投票结果不得被篡改。

本次投票的基本思想是利用区块链的特征，安全地记录选民的投票，以确保投票记录不被篡改。将区块链与投票相结合，利用现有的我号码卡认证机制，可以实现基于区块链并满足这四个条件的在线投票系统。

虽然这次投票要求互联网用户使用投票站的终端进行投票，但最终的目标是让人们能够在家里或其他地方使用手机或个人电脑进行投票。随着技术的成熟，我们可以在家里或任何地方投票；否则通过互联网。

6.2 祖格加密镇进行瑞士第一次基于区块链的市政调查

据swissinfo.ch网站称，2018年6月8日，瑞士的小镇Zug在夏季[7]举行了一次基于区块链的市政投票。该活动是瑞士第一次使用区块链进行的市政投票。

根据该报告，测试投票测试了该市于2017年11月推出的数字身份证(eID)系统。该系统允许公民对其移动设备进行投票。

除了就小市政问题投票，公民还被问及是否应该使用基于区块链的eID系统投票。由于即将到来的投票是一项实验，选举结果对市政当局没有约束力。

在建立了全球加密货币和区块链开发中心“加密谷”之后，Zug已经成为整合了加密货币、区块链和分布式账本技术的全球领先的生态系统之一。2016年，Zug推出了一项接受比特币(区块链技术公司(BTC))作为支付某些市政服务的项目。

由于“加密谷”的存在和该国对加密货币投资者的免税政策，瑞士已成为欧洲最大的区块链友好型国家。

2018年6月6日，伦茨堡超级银行私人银行成为第一家向区块链和加密货币公司提供商业账户的瑞士银行。

6.3 莫斯科的积极公民项目引入了区块链技术，以提高投票的可信度

2014年，莫斯科启动了“积极公民”项目，允许公民就公共照明的颜色、地铁列车的命名和体育场座位的颜色进行投票。现在，莫斯科已经将区块链技术应用于活跃公民的投票，以使[27]项目更加可信。根据2018年3月发布的一份新闻稿，莫斯科居民每年会就这些问题举行5000至7000名活跃公民的面对面会议，但在繁忙的城市环境中，这种会议越来越难以安排。此外，居民们有时会质疑调查结果的结果投票结果。

莫斯科首席信息官的顾问安德烈·贝泽洛夫说：“有时我们听说不是所有的选票都可信，所以我们决定在积极公民项目中使用区块链技术作为建立电子信任的平台。”

2017年12月，活跃公民项目开始使用区块链技术进行投票。一旦投票获得批准，它将被列在包含所有投票的分类账中。这确保了在投票后，数据不会被一人丢失或更改，因此不会存在欺诈或第三方干涉。

7 比较与分析

从比特币一开始，区块链已经发展成各种类型，如公共区块链、私有区块链和混合区块链。一般根据权限管理分为允许区块链和无许可区块链。不同的区块链也采用不同的方法来达成共识，包括但不限于PoW和PoS[33]。这些共识机制首先有它们自己的特点，它们可以分别用于不同的投票场景。

我们根据区块链的分类、共识的分类和匿名的分类等不同的原则对这些基于区块链的投票系统进行了分类。然后对这些方案进行了分析，并进行了比较。这些方案的分类情况见表3。

具体详见表3。基于区块链的投票系统的分类

各小节	分类原则	分类项目	现有的建议书
7.1	区块链的分类法	允许的区块链	[29][38]
		无允许的区块链	[6]
7.2	达成共识的方法	战俘俘	[6]
		职位	[41][53]
7.3	实现匿名性的方法	环签名	[53][39]
		混合式网络	[41]
7.4	隐藏信息的方法	零知识证明	[29][40][53][46]
		盲签：	[6][38]
		同态加密	[41]
7.5	对平台的依赖性	独立于平台的信息	[40][38]
		与平台相关的信息	[29][3]
7.6	对TTP的依赖性	TTP独立于自动控制系统	[40][38]
		与TTP相关的	[36]
7.7	参与者的比例表	大规模的	[36][53]
		小规模的	[40]
7.8	安全级别	全国选举水平	[36]
		在线投票水平	[48]

7.1 区块链的分类法

允许的区块链。私有区块链和混合区块链都是允许的区块链。因为他们的读权限或写权限或多或少受到限制。在一些基于区块链的投票系统中，特别是那些涉及到TTP的投票系统中，允许的区块链被用于避免不必要的信息泄漏。只有特定的实体，如TTP或投票组织者才拥有读写权限，而选民可以通过提供其凭证来读取区块链。

在其提案[29]中使用了允许的区块链来实现流动民主，这是一种新的集体决策形式，给予选民充分的决策控制。在该系统中，区域节点可以与相应的智能契约进行交互。当一个个人选民投票时，投票数据将由所有相应的地区节点进行验证，当到达区块时间时，他们同意的每个投票都将附加到区块链上，选民将收到一个交易ID作为反馈。投票结束后，选民可以通过向授权节点提供其交易ID来验证其选票是否已被正确清点在内。

无允许的区块链。无允许的区块链被称为公共区块链，
因为它们是为所有的互联网用户准备的。任何人都可以拥有区块链的读写权限，并且任何人都可以成为分类账提交者。最著名的公共区块链是比特币区块链和以太坊区块链[54]。大多数使用无许可区块链的建议都是基于比特币网络或以太坊平台。

比斯塔雷利的提议是，[6]是基于比特币的。在预选阶段，所有合法选民都将被授权作为投票权。此外，在投票阶段，他们所需要做的就是将令牌直接发送到相应候选人的区块链地址。选民和候选人之间没有中间人，注册后也不需要TTP。

其优点之一是基于无允许区块链的投票系统是独立于平台的。投票过程被认为是虚拟资产如代币的转换，比特币，或以太坊，这很容易实现。

具体详见表4。允许区块和无许可区块链的比较

	已许可的	无许可的文件
分散化	部分部分	是的
吨	高的	低的
隐私保护	良好	缺乏
节点安全	高的	低的

可进行比较。允许的区块链和无允许的区块链在许多方面都是不同的，包括但不限于非集中化、TPS、隐私保护和节点安全。表4显示了定性比较。

(1) *分散化。*允许的区块链由一个组织或一个联盟控制，其中包括几个组织，这会危及区块链的分散化，而无许可的区块链则面向所有用户，从而实现完全分散化。
(2) *标签。*通常，允许的区块链网络中包含少量节点，在参与授权后都受信任。不需要通过所有节点来验证事务，这对于提高事务速度至关重要，而无许可区块链的不可信任的网络环境使得事务必须由网络之间的所有节点来验证，这是一个非常缓慢的过程。
(3) *隐私保护。*存储在允许的区块链中的数据受到访问控制法规的保护。只有授权实体才能访问数据，这使得更难泄露与参与者隐私相关的信息。相比之下，存储在无许可区块链中的数据则对所有互联网用户开放。强烈建议不要在无许可的区块链中存储任何敏感的内容。
(4) *节点的安全性。*如上所述，组织或联盟中允许的区块链得到了良好的控制。在接受节点作为许可区块链的一部分之前，需要进行严格的授权认证。虽然无允许区块链中的节点可以自由参与，但其中可能会有一些邪恶的节点。因此，节点在被允许的区块链中比在无允许的区块链中更安全、更受信任。

7.2 达成共识的方法

战俘俘。战俘是工作证明的缩写。它是第一代共识机制，也是比特币系统的基础。网络中的所有节点都通过解决一些计算密集型的难题来相互竞争，成为账本的提交者。此外，采矿的困难也可以动态调整。要解决这些谜题，需要有大量的计算能力。这既是有利的，又是缺点。一方面，如果这个网络中有足够的参与者，某人就不可能控制超过51%的计算能力，从而消除了欺诈的可能性；另一方面，计算需要大量的时间，这减少了网络的事务吞吐量。大多数使用PoW的基于区块链的投票系统都是基于比特币，或以太坊平台，或其他无许可的区块链。比斯塔雷利的提议[6]就是一个例子。该方案基于比特币系统，采用战俘共识机制。战俘的优点之一是采矿将吸引更多的参与者，这加强了基于区块链的投票的安全性

具体详见表5。战俘系统与战俘系统的比较

	工作证明	取样证明
节点的匿名性	强烈	弱
采矿成本事务处理延迟	高位	低低

系统。然而，使用PoW的系统通常无法实现高事务吞吐量，这限制了其应用场景。

职位。创建新块的机制与波完全不同。内部
每个社区成员收到的股份都由每个社区成员持有的股份决定。在珍珠币的股份证明系统[33]中，这里的股份是指硬币数量和硬币持有日的产物。你拿硬币的时间越长，持有的硬币越多，你就越有可能记好。持币时间超过30天后，节点可以参加簿记员的比赛。一旦获得了簿记权，持有天数将恢复到零，下一场比赛至少需要等待30天。持有天数不会持续增加，最长为90天，可以防止持有大量硬币的节点控制簿记权。这种共识机制可以连续产生计算能力而不消耗大量的硬币。

还有另一种共识机制被称为DPoS[35]。DPoS系统中的社区成员不会自己提交分类帐，而是让他们选择委托一个超级代表来验证下一个块的事务。DPoS和PoS之间的主要区别在于DPoS共识系统；社区成员在网络中拥有更多的治理权。

Wang等人。提出了一种基于区块链的投票方案；该方案采用了DPoS。由于DPoS，投票系统可以获得较高的事务吞吐量；这对于一个大规模的投票系统是非常重要的。此外，DPoS使其成为一个更加分散的系统，具有民主、自治的投票程序。

可进行比较。在PoW和PoS，以及区块链网络之间有很多差异
基于它们是不同的。分析了节点的匿名性、挖掘成本和事务延迟等方面，并进行了比较。结果如下表5。

(1) *节点的匿名性。*在工作证明区块链系统中，所有节点自由加入区块链网络，无需授权。这使得所有节点在网络中保持匿名，这保护了所有用户的隐私。相反，断证明区块链网络中的节点不能自由连接。他们首先需要账户中的硬币余额。为了取得平衡，他们必须与他人打交道。这提高了参与的门槛，并削弱了匿名性。
(2) *采矿成本。*如前所述，矿工们通过解决一些计算密集型的谜题来参与簿记。它很耗时，也很耗电。然而，在基于PoS的网络中，并没有什么难题需要解决。分类帐提交者由硬币年龄决定，然后分类帐提交者只需签署一个签名来创建一个新的块。它对计算很友好。
(3) *事务处理延迟。*在基于俘的区块链网络中，如比特币，大约每10分钟就会创建一个新的块。此外，事务需要等到创建六个块才能得到其确认。因此，一个事务的平均延迟为1小时。在基于PoS的区块链网络中，可以在接收到事务后立即打包，然后进行广播。没有等待时间。因此，延迟可以保持在一个非常低的水平。与战俘战相比，这几乎可以忽略不计。

7.3 匿名的方法

戒指签名。2001年，里维斯特、沙米尔和陶曼描述了亚丙烯酸酯[49]的环签名。戒指签名是一种特殊的签名。在一个消息通过环签名签名后，我们只能知道签名者来自一个组，而不是确切签名的人。在计算上不可能知道哪一个键用于环签名。环签名和组签名之间存在一些区别：(a)没有管理员，不能公开成员的匿名性，(b)任何指定的成员都可以组成一个组。

戒指签名提供了无条件的匿名性。也就是说，即使攻击者非法获得了所有可能签名者的私钥，攻击者发现真正签名者的概率也不超过1/n，其中n是所有可能签名者的数量。环签名提供的无条件匿名性与基于区块链的投票系统中选民的要求一致。

Wang等人。提出了一种基于区块链[53]的大规模选举方案，其中选举组织者作为可信赖的第三方。在选票准备阶段，选民使用系统公钥加密他们的选票内容。然后，选民在加密的选票上签名。接下来，加密的选票和戒指签名将被发送给选举组织者。组织者通过检查戒指签名来验证投票的有效性，但不透露真实的签名者，然后用系统私钥解密选票以清点投票。

混合的网络。1981年，Chaum首次引入了混合网络[11]的概念。此后，
许多基于混合网络的应用程序已经被开发出来，如匿名转发器和洋葱路由。混合网络是一种使用代理服务器来调解用户流量的路由协议，这使得很难跟踪用户之间的流量。代理服务器混淆传入的消息，并将它们随机发送到下一个代理服务器。此混淆过程会使消息的源地址与目标地址不再匹配，这使得攻击者难以跟踪消息的源地址。

提出了一种基于区块链的电子投票系统[28]方案，建议使用混合网络和同态加密，提供了匿名投票的可靠机制。它非常容易理解，所有的步骤都可以发布为通用的可验证性。为了满足混合网络的所有加密要求，同态加密方案必须支持重新加密。在混合网络之后，所有的选票都是匿名的，仍然是加密。因此，储存的选票与选民没有任何联系。

7.4 隐藏信息的方法

零知识证明。20世纪80年代，戈德瓦瑟提出了零知识证明[24]的概念。零知识证明是一个涉及三个对象的协议：验证器、验证器和秘密。在零知识证明协议中，证明者试图证明它知道一个秘密，但不能在证明过程中透露任何关于这个秘密的信息。零知识证明协议满足以下三个属性。

(1) **其可行性。**如果Prover提供真实秘密，则验证器将以高概率接受Prover的断言；
(2) **可靠性。**如果验证程序提供了一个错误的秘密，则验证程序将拒绝验证程序的具有较高概率的断言；
(3) **零的知识。**如果验证者提供了真实的秘密，并且验证者不违反协议规则，那么无论验证者如何验证，验证者除了接受外不能获得任何与秘密相关的信息，除非接受断言。

一方面，基于区块链的投票系统需要验证某些信息的合法性，比如参与者是否有投票权；另一方面，该系统需要防止敏感信息的披露，如选民的真实身份、选票的内容和与投票相关的关键。通过零知识证明，完全满足了投票系统的这些要求。

在帕特里克等人的建议[40]中多次使用了零知识证明。在注册阶段，参与者P_i将会选择一个x吗$_i$作为它的私人投票钥匙。在投票之前，每个P_i将播放其公共投票密钥π吗^{x_i}以及x的零知识证明(菲亚特-Shamir启发式[23])$_i$。这不仅验证了P_i是合法参与者，但也防止披露其私人投票密钥。在投票阶段，选票中将包含一个三分之一的零知识证明[17]，以便让计票的人来验证选票的有效性。

盲码签名。Chaum于1983年，[10]首次提出了盲签名。盲签：
是一种特殊的数字签名，签名者签署签名而不获得签名消息的详细信息。除了满足一般数字签名的条件外，它还必须满足以下两个特性。

(1) **失明。**虽然签名人签署信息，但无法获取信息的具体内容；
(2) **不可链接性。**一旦消息的签名被公开，签名者就不能被公开
当然是当他在邮件上签名的时候。

盲签名通常用于与隐私相关的协议，其中签名者和消息作者是不同的一方。例如，包括密码选举系统和数字现金计划。盲签名不仅支持盲，而且还可以用来提供不可链接性，从而防止签名者将其签名的盲信息链接到后来可能被要求验证的非盲版本进行验证。在这种情况下，签名人的回复首先是“非盲的”，然后再进行验证，以便签名对非盲的信息仍然有效。这在需要匿名的方案中可能很有用。

刘等人。提出了一种基于区块链[38]的电子投票协议，利用盲签名来防止投票组织者和检查员的投票内容。在选票准备阶段，选民会根据自己的选择生成一个投票串。投票字符串随后被加密并发送给组织者和检查员，以检查投票格式的有效性，然后签署一个签名。盲签名后，选民解密盲签名，得到组织者和检查员的签名。组织者和检查员在上述过程中无法获得有关选民选择的任何信息。

同态加密。同态加密是一种加密方法
有一些特殊的性质属性，这个概念是Rivest等人在20世纪70年代首次提出的，与一般的加密算法相比，同态加密不仅可以实现基本的加密操作，而且可以实现密文之间的各种计算功能。即，解密后的计算相当于计算后的加密。该特性对保护信息的安全具有重要意义。同态加密技术可以用于计算多个密文，然后解密它们，而不是以很高的计算成本解密每个密文。同构加密可以不解密计算密文，不仅可以降低通信成本，而且传输计算任务，以平衡各方的计算成本。可以使用同构加密，以便解密方只知道最终的结果，而不是密文中的每个消息，这可以提高信息的安全性。由于同态加密在计算复杂度、通信复杂度和安全性方面的优势，它的理论和应用受到了越来越多的研究关注。

在基于区块链的投票系统中，通常会有一些敏感的数据，如选民的真实身份、投票内容和与投票相关的键。此外，这些敏感数据通常执行一些基本的计算，由于安全考虑，不能在明文下执行。在克里斯蒂安的提议[41]中，同态加密被用来保护选票的内容。在密码文本下统计时，组织者可以验证选票的有效性，但组织者无法获得选票内容的详细信息。

7.5 对平台的依赖性

平台独立。基于区块链的投票的平台独立协议可以应用到不同的平台上，而无需进行很大的修改，这有利于该协议的推广和实现。投票协议的数据一般作为数据部分包含在交易中。这些数据有它们自己的数据结构，并且它们包含了所有的投票内容。它们与事务中的其他数据无关。此外，区块链系统并不关心数据部分。因此，投票议定书应处理在投票过程中可能出现的所有可能的问题。

刘等人。提出了一种基于区块链[38]的电子投票协议。它是一个独立于平台的协议。在选票准备阶段，选民将根据其选择生成一个投票符串。然后投票人将加密投票字符串，并将加密结果发送给投票组织者和检查员盲签名。选民解密盲签名，并获得已签名的投票字符串。已签名的投票字符串将作为数据部分包含在事务中，并将存储在区块链中。投票结束后，组织者将收集包含签名投票字符串的所有事务，以验证签名和清点选票。

这将依赖于平台。设计了一种基于区块链的平台依赖性投票协议
对于一个特殊的平台，如比特币系统或以太坊平台。平台相关协议的设计应充分考虑平台的特点，充分利用平台的优势。例如，比特币是一种通用的支付系统，而比特币系统所使用的工作证明共识机制可以得到数学证明的安全性。为了利用比特币的专长，一些基于区块链的投票提案将投票操作转换为虚拟资产的转移，如比特币或代币。它简化了该协议。

比斯塔雷利等人。提出了一种基于比特币[6]的端到端投票系统。投票操作被定义为虚拟资产的转移。在预选阶段，已完成注册的参与者将收取一定数量的比特币作为完成注册的标志。然后，参与者需要通过具有匿名签名的匿名Kerberos身份验证协议[42]进行身份验证。完成身份验证的参与者是有效的选民，他们将收到一个投票令牌。在投票阶段，选民根据其选择将代币转移到相应候选人的账户。投票结束后，候选人账户中的代币金额是该候选人获得的总选票。

7.6 TTP的依赖性

TTP独立于TTP。受信任的第三方是一个实体，它促进了双方都信任第三方的双方之间的互动。没有TTP的基于区块链的投票系统更分散和独立。

刘等人。提出了一种基于区块链的投票系统的[38]协议，除了选民和候选人之外，只有组织者和检查员参与。组织者的职责是举行选举，核实和记录合格选民的信息，并在选举期间与选民互动。引进检查人员，限制组织者的权力，检查组织者的行为。检查员也会在选举期间与选民进行互动。在选票准备期间

在阶段，选民会根据他们的选择生成一个投票串。投票字符串随后被加密并发送给组织者和检查员，以检查投票格式的有效性，然后签署一个签名。盲签名后，选民解密盲签名，得到组织者和检查员的签名。组织者和检查员在上述过程中无法获得有关选民选择的任何信息。

它依赖于TTP。在基于区块链的投票系统中，一个受信任的第三方可以促进选民和组织者等两个实体之间的互动，以及组织者的权力可能是有限的。一些敏感数据可以由不信任的第三方没有信任的第三方处理，而不是一些基于区块链的投票系统的组织者处理。

Lee等人。提出了一个电子投票系统[36]作为区块链的应用，其中涉及一个可信的第三方。如果没有值得信任的第三方，那么投票组织者应该对选民进行认证，计数选票，并可能提供一次性挖掘的大部分内容。组织者能够找出选民投票给了谁，而且它有可能按照自己想要的方式打造区块链分类帐。这就是为什么该提案需要一个值得信赖的第三方。受信任的第三方根据投票组织者是否通过SSN进行验证。此外，受信任的第三方会在投票过程中清点选票。受信任的第三方只知道虚拟身份是否有投票权，但它无法找到虚拟身份背后的SSN。因此，组织者和受信任的第三方不能同时知道真实的身份和投票内容。

7.7 参与者人数表

大规模的。大规模的投票活动，如全国选举或在线投票，通常涉及到大量的人群，这就提高了对基于区块链的投票系统的要求。随着参与者数量的增加，需要较高的交易吞吐量来处理在短时间内大量涌入的选票。大型基于区块链的投票系统应在每个阶段有效地处理数据，存储容量也应相应增加。另一个问题是，交易费用应该保持在很低的水平，否则就会是大量的货币成本。

Wang等人。提出了一种基于区块链[53]的大规模选举方案。这个建议是基于以太坊平台，但共识算法不再是工作的证明。最初的共识机制不适合大规模的在线投票，因为战俘共识机制会消耗大量的计算能力，从而导致大量的能源浪费。它还可以导致挖掘中心和减缓交易确认。DPoS可以大大降低事务验证的频率和参与共识的节点数量，从而增加了网络的事务吞吐量。DPoS通常用于高吞吐量的区块链网络，如选择，其中的事务确认非常快。

小规模的。董事会投票等小型投票活动通常包括一个小组在有限的空间里的人。因此，小规模投票系统的设计与大规模投票系统的设计完全不同。基于小规模区块链的投票系统需要考虑的方面也有所不同。在一个大规模的投票系统中，效率和成本可能是主要考虑的因素。而在小规模投票系统中，隐私和安全可能是首要考虑因素，因为参与者在有限空间内的小规模投票活动，他们在现实生活中可能很熟悉。任何与投票内容有关的信息都很敏感。

McCorry等人。设计并实现了一个基于以太坊智能合同[40]的具有最大选民隐私的董事会投票系统。这是一个二进制选择的会议室投票系统，参与者只能选择是（记录为二进制1）或否（记录为二进制0）。选民人数

具体详见表6。大规模投票系统和小规模投票系统的比较

	大规模的	小规模的
交易处理吞吐量	高的	低的
表决成本	高无限空	有限的
参与者的分布情况	间	空间较小

他们通过广播д来投票$x_i y_i$ $д^{v_i}$，其中为x_i是一次秘密投票吗键，y_i是公共中位数，v是选民的可选择。此外，$д^{x_i y_i}$ $д^{v_i}$可在投票结束后计算出来。作为我们具有的x $y=0$，我们可以得到$д^{v_i}$。如上所述，它是一个小规模的投票系统v可以通过不断地从零开始尝试来猜出来。所以，我们得到了它的价值v_i，这是这个数字的其选择是肯定的选民。此外，我们还可以得到那些没有选择的选民的数量减去v_i从参与者的总数开始。

可进行比较。基于大规模区块链和小规模区块链的投票系统的设计在交易吞吐量、投票成本和参与者分配等许多方面都有所不同。我们进行了定性比较，结果见表6。

7.8 安全级别

全国选举水平。由于对国家的巨大影响，全国选举的安全应该达到最高水平。全国选举投票制度的设计非常严格。无法忽略系统中的任何漏洞。例如，真实名称身份验证是投票前阶段必不可少的步骤。但是，由于个人计算机不安全和不受信任的网络环境，在线真名身份验证易受攻击。因此，为了实现更高层次的安全水平，许多关于国家选举的提案损害了在线认证的便利性，代之以现场认证。

投票观察者[8]是一个基于区块链的政府投票系统，由BTC提出。为了安全起见，投票观察者系统的参与者不能远程投票。相反，他们需要到一个投票站来获得一张纸质选票，其中包括三个二维码，它们分别代表区块链地址、投票ID和投票ID。选民们通过扫描这三个二维码来投票。扫描选票后，然后投给相应的候选人。在投票结束之前，所有的投票记录都存储在一个离线的区块链中。投票结束后，离线投票站中的数据将被上传到在线区块链上。这样做的优点是可以防止在投票过程中的来自网络的远程攻击。

在线投票水平。在线投票系统通常是日常使用的系统，是一个重要的系统
其特点是，在线投票比全国选举频繁得多，黑客对在线投票结果的兴趣不如对全国选举感兴趣。因此，在一个在线投票系统中，便利性和安全性是同样重要的。在某些情况下，我们必须牺牲系统的安全性，才能获得友好的操作体验。例如，用户必须能够通过他们的智能手机或通过开放互联网的个人电脑参与投票活动，尽管有一些风险。

8 更广泛的观点

8.1 在效率和安全方面的共存

在一个大型的投票系统中，效率和安全是我们正在寻找的。然而，目前很难做到这两者。如我们所知，在众多的区块链共识算法中，战俘战的安全性应该是首屈一指的。它的安全性可以在数学上得到证明，所以它确实是如此

用于许多区块链平台。然而，其缺点是需要大量的计算能力才能使区块链网络达成共识。如果我们减少战俘的难度，那么共识的速度就会快得多，但安全性也会降低。区块链中存在许多类似的情况，例如，加密和签名算法更安全；这将不可避免地导致操作时间的增加。在这个阶段，已经出现了一些可能的解决方案，如用PoS等共识算法取代战俘，但它们的安全性尚未得到证明。对于加密和签名算法，我们试图在确保安全的条件下减少密钥的长度，以提高效率。为了进一步提高效率，我们只能期望设计出更轻量级的密码签名算法。在效率和安全之间似乎存在着矛盾。如何使效率与安全共存将是未来的研究重点。

8.2 透明度和隐私性的共存

在公共区块链中，数据透明度已经最大化，但缺乏隐私。相比之下，在私有区块链中，权限以牺牲数据透明度为代价而被严格控制。在区块链投票系统中，区块链的数据透明度是该系统的一个重要特征。选民希望尽可能多的数据保持透明，所以他们知道投票系统能公平、公平地表达了所有选民的意愿。然而，在区块链系统中，更透明的数据意味着用户的隐私。区块链中的隐私一直是研究的热点话题，考虑到数据透明度的隐私保护将使这个问题更加具挑战性。目前的解决方案是使用联盟区块链。联盟区块链结合了公共区块链和私有区块链的优势，以及透明度和隐私性，这使得联盟区块链应用于多种情况。然而，在许多需要使用公共区块链的场景下，透明度和隐私仍然难以平衡。

8.3 高并发性和高吞吐量的共存

在大型投票系统中，通常有大量用户同时参与投票，系统需要同时处理许多投票请求，这要求投票系统具有高并发能力。然而，现有的区块链解决方案通常无法实现高事务吞吐量，特别是在一些公共区块链平台上。例如，比特币系统的吞吐量为7TPS，以太坊的吞吐量为8TPS，这远远不能满足大型投票系统的要求。低吞吐量可以说是链结构化区块链的一个常见问题。这是因为链结构区块链采用同步一致，事务需要经过验证才能附加到区块链上，从而使网络中所有节点的状态能够同步。为了实现高并发性和高吞吐量共存，有一些异步共识解决方案，如Tangle、IOTA和带有有向无环图-(DAG)结构化区块链[19,47]的XDAG，首先将事务附加到区块链上，然后进行验证。理论上，具有DAG结构的区块链的并发性越高，其吞吐量就越高。

9 试验结论

近年来，人们一直有兴趣设计基于区块链的投票系统，以规避现有的基于纸质的投票系统和电子投票系统的限制。因此，我们研究了这些方案，并根据它们的特征，如区块链的类型、一致的方法和参与者的规模，对其进行分类。我们还提出了一个系统的，

深入分析了不同的基于区块链的投票系统，并确定了一些潜在的研究机会。

参考文献

[1] 乌穆特·卡布克，埃鲁尔·阿迪格泽尔和埃尼斯·卡拉尔斯兰。2018.关于区块链技术对电子投票系统的可行性和适用性的调查。*内部。J.广告。平均分辨率。投入。请提交电子邮件。工程师。* 7，03（2018），124－134.DOI：https://doi.org/10.17148/ijarcce.2018.7324

[2] 穆罕默德萨莱克阿里，马西莫维奇奥，米格尔平切拉，杜卢伊，法比奥安东尼利，和侯赛因雷赫马尼。2018.区块链在物联网中的应用：综合调查。*IEEE通讯。冲浪。导师。*21，2（2018），1676－1717.

[3] A.Ã B.Ã已保持警惕。 2017.一种概念性的基于区块链的安全电子投票系统。*内部。J.网络信息。安全。应用程序。*9，3（2017）.

[4] 巴塞罗那州。2014.公共比特币区块链中的用户隐私。2019年8月2日检索自https://pdfs。semanticscholar.org/549e/7f042fe0aa979d95348f0e04939b2b451f18.pdf.

[5] 亚历克斯·比鲁科夫、德米特里·霍夫拉托维奇和伊凡·普斯托加洛夫。 2014.比特币P2P网络中客户端的匿名化。在2014年ACM SIGSAC计算机和通信安全会议的论文集上。acm，15-29岁。

[6] 比斯塔雷利，曼蒂拉奇，圣塔西尼，和桑蒂尼。2017.一个基于比特币的端到端投票系统。*在应用计算研讨会论文集上（SAC‘17）中。*ACM，纽约，纽约，1836-1841年。DOI：https://doi.org/10.1145/3019612.3019841

[7] 区块链铅笔。 2018.祖格加密镇进行瑞士第一次基于区块链的市政调查。检索于2020年3月6日，从http://www.bite5.com/index.php/article-872.

[8] 区块链技术公司，2016年。投票观察者----------世界上最透明的投票机。2019年7月28日从https://pdfs.semanticscholar.org/5b6a/0b0ff2c574d9bb8bad9e191b22f44c92add7.pdf.检索

[9] 博德基、巴塔查里亚、坦瓦尔、提吉、库马尔和奥拜达先生。2019.区块链实现了智能的旅游和酒店管理。《2019年计算机、信息和电信系统国际会议会议记录》（CITS’19）。ieee指数，1-5岁。

[10] 大卫。查姆。 1983.无法追踪的付款的盲签名。在《密码学的进展》中，大卫·查姆，罗纳德·L.里维斯特和艾伦·T。谢尔曼股份有限公司（电子版）。美国施普林格，波士顿，马萨诸塞州，199-203年。

[11] 大卫。查姆。 2003.*无法追踪的电子邮件、返回地址和数字笔名。*美国施普林格，波士顿，马州，211-219。DOI：https://doi.org/10.1007/978-1-4615-0239-5_14

[12] *大卫乔姆和尤金范海斯特。1991.组签名。在第十届密码技术理论与应用国际年度会议论文集上（EUROCRYPT‘91）。*施普林格-弗拉格，柏林，257-265年。http://dl.acm.org/citation.cfm?id=1754868.1754897

[13] 金光赵蒙德，A。米格拉尼，尼拉吉·库马尔，M。S.奥拜达和德彪。 2020.物联网环境中基于机器学习的区块链管理：趋势、挑战和机遇。（未发表）。

[14] M.R.克拉克森说。冲，和A。 C.Ã迈尔斯。 2008.走向一个安全的投票系统。*IEEE安全与隐私研讨会论文集（SP‘2008）。*354－368.DOI：https://doi.org/10.1109/SP.2008.32

[15] 以太坊的贡献者。2019.以太坊区块链资源管理器。2019年8月2日从https://etherscan.io/检索。

[16] 维基百科的贡献者。 2019.比特币的可伸缩性问题。2019年8月2日从https://en.wikipedia.org/w/index.php?title=Bitcoin_scalability_problem&oldid=908933182.检索

[17] 罗纳德克莱默，伊万达姆加德，和贝瑞舍恩制造商。1994.部分知识的证明和简化的证人隐藏协议的设计。*在密码学进展会议（94），YvoG。*下降（版）。施普林格，柏林，174-187年。

[18] 克里斯卡尔纳内，亚历山大埃塞克斯，萨拉杰米刘易斯，奥利维尔佩雷拉，和凡妮莎蒂格。 2019.骑士们和恶棍们进行选举：网络投票和无法察觉到的选举舞弊。*IEEE安全。优先。* 17，4（2019），62－70.

[19] M.Divya和长长天B.Biradar。2018.IOTA-下一代区块链。*内部。J.工程师。投入。科学研究。*7，04（2018），23823－23826.

[20] 菲利普·尤因。 2019.你需要知道的关于美国的情况。选举安全和投票机器。检索自https://w二战期间。npr.org/2019/08/31/754412132/what-you-need-to-know-about-u-s-election-security-and-voting-machines.

[21] 齐峰、德彪、刘哲、丁王、金光崔。 2020.IEEEP1363标准中基于身份的签名方案的多方签名协议。*IET信息。安全。* 1，99（2020），1－10.DOI：10.1049/iet-ifs.2019.0559

[22] 齐峰、德彪、谢拉利、穆罕默德汗拉姆和库马尔。2019.区块链系统隐私保护的调查。*J.网络信息。投入。应用程序。* 126（2019），45－58.DOI：https://doi.org/10.1016/j.jnca.2018.10.020

[23] 阿莫斯菲亚特和阿迪沙米尔。 1987.如何证明你自己：识别和签名问题的实际解决方案。在密码学进展会议论文集（86），安德鲁M。（英文版。）。施普林格，柏林，186-194年。

[24] S.金匠，S。米卡利，和C。机架上的人。 1989.交互式证明系统的知识的复杂性。*暹罗，j。投入。* 18, 1 (1989), 186－208. DOI：https://doi.org/10.1137/0218012arXiv：https://doi.org/10.1137/0218012
[25] Dimitris A.灰的.2002.对一个安全的电子投票系统的原则和要求.*投入。安全。*21, 6 (2002), 539－556.
[26] 拉杰什，古普塔，坦瓦、苏丹汉舒、库吉、穆罕默德、奥巴达和萨达恩。2019.习惯：基于区块链的医疗保健4.0的远程办公框架。*《2019年计算机、信息和电信系统国际会议会议记录》（CITS'19）*。ieee指数，1-5岁。
[27] 大师网络。 2018.莫斯科的积极公民项目引入了区块链技术，以提高投票的可信度。检索于2020年3月6日，从http://mini.eastday.com/mobile/180315175458878.html.
[28] *R.哈尼塔和B.拉哈德。2017.基于区块链的电子投票记录系统设计。在2017年第11届电信系统服务和应用国际会议的会议记录中(TSSA'17)。1－6.*信息信息：//doi.org/10.1109/TSSA.2017.8272896
[29] P.哈尔马森，G.K.哈里阿尔森，M.哈姆达卡和哈贾尔姆蒂森。F. 2018.基于区块链的电子投票系统。2018年IEEE第11届云计算国际会议记录（云'18）。 983－986.信息信息：//doi.org/10.1109/CLOUD.2018.00151
[30] 日本时报》。2018.筑波在日本第一个部署在线投票系统。检索于2020年3月5日，从 htpw 二战期间。japantimes.co。jp/单位单位ws/2018/09/02/national/politics-diplomacy/new-online-voting-system-介绍了城市子谷。
[31] 斯尼哈尔卡达姆，查万，库尔卡尔尼，和帕蒂尔。2019.利用区块链技术进行数字电子投票系统的调查。*内部。J.广告。科学研究。平均分辨率。工程师。*趋势：4.2（2019）。
[32] 金日仁、敏庆和洪成菲。 2017.基于区块链的在线投票系统的应用方法研究。*内部。J.联系人。自动运行。*10, 12 (2017), 121－130.
[33] 阳光明媚的金和斯科特·纳达尔。 2012.PPCoin：具有获取证明的点对点加密货币。检索自https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf.
[34] 马科维奇。2017.区块链：区块链技术作为安全可靠的电子投票系统的基础。DOI：https://doi.org/10.31235/osf.io/9qdz3
[35] 丹尼尔·拉里默。2014.委托接收证明(DPoS)。已从https://en.bitcoinwiki.org/wiki/DPoS中检索到。
[36] K.李安，J。詹姆斯先生。Ejeta，和H。金正日。 2016.使用区块链的电子投票服务。*J.请进行"挖掘"。论坛。安全。*第11条第（2016）条。DOI：https://doi.org/10.15394/jdfsl.2016.1383
[37] 尹张林和慈春廖。2017.对区块链安全问题和挑战的调查。这是从https://pdfs.semanticscholar.org/f61e/db500c023c4c4ef665bd7ed2423170773340.pdf.中检索到的
[38] Y.刘和Q。王王。 2017.一种基于区块链的电子投票协议。检索于2019年7月28日，从视频观察器。目录。
[39] 嘉卓柳、姜、宣王、振浩农、何浩、斌方。2019.一种基于智能契约的安全分散式无信任电子投票系统。*参见2019年第18届IEEE计算与通信中的信任、安全与隐私国际会议/第13届IEEE大数据科学与工程国际会议（TrustCom/BigDataSE'19）。我，570-577。*
[40] 帕特里克·麦科里，暹罗人F。沙汉达什提和冯浩。 2017.拥有投票人最大隐私的会议室投票的明智合同。*在金融密码学和数据安全方面，阿格洛斯·基亚利亚斯。*)。施普林格国际出版公司，查姆，357-375。
[41] 基督教度表。2017.分布式投票系统的设计。阿克西夫：1702.02566。检索自http://arxiv.org/abs/1702.02566.
[42] 隐私保护报告。 2017.对克贝罗斯的匿名支持。2019年7月28日从https://tools.ietf.org/html/rfc8062检索。
[43] 中本聪。2008.比特币：一个对等的电子现金系统。检索自http://www.academia.edu/download/54517945/Bitcoin_paper_Original_2.pdf.
[44] 卡西姆·纳西尔，伊尔汉姆A。卡斯，马纳尔阿布塔利布和阿里布纳西夫。 2018.超分类帐结构平台的性能分析。*安全。请提交电子邮件。网络信息。*2018 (2018).DOI：https://doi.org/10.1155/2018/3976093
[45] 穆罕默德·奥拜达特和新雷丁·布德里加。 2007.*电子系统和计算机网络的安全。*剑桥大学出版社。
[46] 潘尼亚，三木袋，冯浩，和比玛尔罗伊。 2020.一个针对分散的博尔达计数投票的智能合同系统。*IEEE横向。工程师。请进行管理。* 67, 4 (2020), 1323－1339.DOI：https://doi.org/10.1109/TEM.2020.2986371
[47] 塞圭波波夫。 2016.缠结的东西。 1 (2016), 3.检索于2019年3月从http://arxiv.org/abs/1705.04480.
[48] 罗伯特黎曼和斯蒂芬格鲁巴赫。2017.分发协议在拯救值得信任的在线投票。阿克西夫：1705.04480。检索自http://arxiv.org/abs/1705.04480.
[49] Ronald L.里维斯特,阿迪·沙米尔和耶尔·陶曼.2001.如何泄露一个秘密.在《关于密码学进展的会议论文

集》(ASIACRYPT ‘01)中,科林·博伊德(Ed.).施普林格，柏林，552-565年。

[50] S.F.Sayyad，曼格什帕瓦尔，阿舒德什帕蒂尔，范达纳帕塔尔，S.F.Sayyad，曼格德什帕瓦尔，阿舒托什帕蒂尔，汪达纳帕塔雷，和普拉亚格波杜瓦尔。2019.区块链投票的特点：一个调查。*内部。J.创新型产品。平均分辨率。科学研究。技术技术。* 5 (2019)，12－14.检索自htpw二战期间。academia.e都道wnload/58599085/IJIRSTV5I9012.pdf.

[51] R.学术者。2001.点对点体系结构和应用程序分类的点对点网络的定义。*在第一届点对点计算国际会议的论文集上。* 101－102.DOI：https://doi。org/10.1109/P2P.2001.990434

[52] 杰尼尔沃拉，阿南德纳亚尔，苏迪普坦瓦尔，提吉，库马尔，穆罕默德S。奥拜达特和乔尔J。P.罗德里格斯。C. 2018.呵呵：一个基于区块链的框架来保护电子健康记录。在2018年IEEEGlobecom研讨会的会议记录中(GCWkshps‘18)中。ieee指数，1-6岁。

[53] 王宝成、孙佳伟、何云华、丹东庞、宁晓路。2018.基于区块链的大规模选举。*项目。投入。科学研究。*129 (2018)，234－237.DOI：https://doi.org/10.1016/j.procs.2018.03.063

[54] 博士。加文的木材。 2014.以太坊：一个安全的分散的广义交易分类账。检索自https://ljk.imag.fr/membres/Jean-Guillaume.Dumas/Enseignements/ProjetsCrypto/Ethereum/ethereum-yellowpaper.pdf.

[55] 张林强、洪李、孙利民、石志强、何云华。2017.海报：面向使用区块链的完全分布式用户身份验证。. 在2017年IEEE隐私意识计算研讨会论文集（PAC‘17）中，IEEE，202-203。

[56] 盖伊·齐斯金德，奥兹·内森，等人。 2015.分散隐私权：使用区块链来保护个人数据。*在2015年IEEE安全与隐私研讨会的论文集中。*我，180-184。

2020年3月收到；2020年8月修订；2020年11月接受