·社会治理与舆情·

区块链舆情存证方案设计及应用挑战

刘 峰[1,2] 杨 杰[2] 李志斌[3] 齐佳音[2,4*]

1. 华东师范大学 计算机科学与技术学院,上海 200062
2. 上海对外经贸大学 人工智能与变革管理研究院,上海 200336
3. 华东师范大学 数据科学与工程学院,上海 200062
4. 可信分布式计算与服务教育部重点实验室,北京 100866

[摘 要] 席卷全球的新冠肺炎(COVID-19)疫情,不仅带来了损害身体健康的病毒,也滋生了舆情空间的信息"病毒"。如何通过技术方案来应对极端重大突发事件下的信息"病毒"是当下备受关注的热点和难点。本研究面向舆情存证的三个难点:技术层面的信息与隐私安全、法理层面的合法性、运行层面的合理性,提出基于区块链技术的设计思路:融入零知识证明技术来解决公众数据隐私性问题、构建匹配舆情存证逻辑的智能合约来解决技术落地的法理性问题以及设计差分授权模式来解决决策业务的合理性问题。鉴于舆情存证是一个复杂的社会问题,本研究也对舆情存证系统实践中面临的巨大挑战和问题进行论述。新冠肺炎疫情必将过去,但是由此引发的极端重大突发事件下的信息"病毒"治理才刚刚开始,本研究只是抛砖引玉,以启发更多的学者来思考。

[关键词] 新冠肺炎疫情;区块链;隐私计算;舆情存证系统;零知识证明

回望 2020 年的上半年,新冠肺炎疫情肆虐全球。前所未有的疫情考验着各国政府的重大公共危机事件的治理能力。与疫情战场上复杂多变的情况相对应,另外一场由疫情引起并席卷了互联网的舆情"应对战"也同步打响!

在本次疫情引起的舆情事件中,谣言层出不穷,污名化网络暴力对疫情阻击战带来极大影响。围绕新冠肺炎的治疗,产生了许多谣言,如喝酒能抵抗新型冠状病毒、苯酚注射可以有效治疗新冠肺炎等。围绕新冠肺炎疫情的传播途径,也产生了诸多谣言,如眼神对视可以传播病毒、病毒是人为制造并携带进入武汉等。由于听信网络谣言,导致部分患者不去医院接受正规治疗,贻误了治疗时机;不实的网络谣言,也加剧了社会的恐慌情绪,增加了社会的不稳定因素。

除了谣言,本次疫情的舆情中还存在令人不安的污名化信息。如网络上出现了对疫情地区民众的

齐佳音 教授,博士生导师,上海对外经贸大学人工智能与变革管理研究院院长。2019 年入选国家级百千万人才工程,并被授予"有突出贡献中青年专家"荣誉称号;荣获 2019 年度全国高校人工智能与大数据教育教学人物创新奖;荣获 2019 年度中国产学研合作个人创新奖;2017 年入选上海市领军人才;2009 年入选教育部新世纪优秀人才。从事大数据、人工智能与管理创新领域的研究工作。

刘峰 华东师范大学博士生,上海对外经贸大学人工智能与变革管理研究院区块链技术与应用研究中心主任,中国计算机学会高级会员,中国自动化学会区块链专业委员会委员,清华 x-lab 区块链创新教育计划合作委员会专家委员。主要研究兴趣在区块链、深度学习、数据科学等学科交叉领域。担任多个国内核心学术期刊、国际会议、SCI/EI 等国际特约编辑及审稿人。

收稿日期:2019-07-26;修回日期:2020-10-30

* 通信作者,Email: qijiayin@139.com

本文受到国家自然科学基金项目(72042004)和国家重点研发计划项目(2017YFB0803304)的资助。

口诛笔伐,对不幸感染病毒民众的恐慌与歧视。另外,在本次疫情事件中,科学家遭到网络围攻也令人痛心。从中国科学院武汉病毒研究所石正丽研究员“制造病毒”,到中国疾病预防控制中心主任、中国科学院院士高福“接受调查”,再到中国科学院武汉病毒研究所陈全姣研究员“举报同事”,这些污名化信息荒唐低级,直接抹黑了科研人员的形象,影响了当前的疫情防控大局。

除此之外,有关瑞德西韦治疗新冠肺炎、零号感染者、病毒来源、病毒发源地等相关舆情都还在网络中漂浮,产生了各种版本的“阴谋论”,对民众心态、情绪、认知甚至倾向性选择产生了较大影响。甚至是“丁香园·丁香医生”平台发布的信息,与新冠肺炎疫情相关的谣言就高达 134 起。网络舆论可信度的缺失无疑增加了舆情治理的难度[1]。

可见,在突发重大公共卫生事件的特殊时期,舆情“病毒”与疫情“病毒”一样,都需要用特殊手段来治理。区块链作为一种解决信任问题的技术,在此背景下受到关注,如有学者认为区块链技术在重塑新闻商业模式、新闻版权保护、信源追溯与打假、流量交换与变现、维护新闻客观性方面可以发挥一定的价值[2~4],区块链作为一种分布式账本技术,具有不可篡改、去中心化等特点,可以应用于突发事件的应急管理[1]。

然而,对于区块链技术是否适合应用到舆情治理中,同时也存在反对的声音。Andries 认为区块链技术的部署有些会和先行欧洲的通用数据保护法规(GDPR)不相兼容[5]。Qi 等人在一项基于区块链和数据隐私的调研中也给出了一些关于隐私保护挑战反而会阻碍区块链应用发展研究的结论[6]。另外,Hannah 等人则认为在加拿大关于涉及数据隐私类的应用程序设计中不仅需要“被动地”尊重人权(human rights)[7],而且还需要主动地采取一定的措施来确保加拿大公民的权利和自由得到尊重和保护。总的来说,对于区块链等技术应用于舆情存证的关键点也是民众的担忧点,尤其是民众对隐私保护的需求、对人权不被侵犯的考虑和数据信息安全的担忧是重中之重。

考虑到传统的电子数据存储服务中存储的数据本身有着易修改、可删除、可拷贝等特性,由此导致了电子证据的使用在存证、取证、示证等方面还存在一些问题。如在存证环节,存证数据容易被丢失和篡改、发生问题后追溯困难等;在取证环节,存在取证不经济、难以用合法的纸质方式展示等。因此相比于传统的电子存证的方法,利用区块链进行存证则有着很多的优势。首先,因为是去中心化的链式结构,政府职能部门上传舆情存证信息到区块链平台时会相对便捷;其次,由于技术上公开透明、可溯源、难篡改的特性,也使得区块链绑定电子舆情存证信息的可信度较高。为了让有关职能部门在应对舆情信息时能够更为高效的处理,将舆情存证信息的数据信息和系统业务拆分,进而以服务化方式输出给决策者,确保其在可接受服务体验标准下能做好舆情处置的决策;同时通过合并重组相似的业务组织,也能够在舆情监管过程中降低处理业务的成本,使得职能划分明确。

基于以上考虑,在重点聚焦公众数据的隐私性、技术落地的法理性和决策业务的合理性的同时,还需要考虑到让有关职能部门对舆情信息能够有更好的掌控,加强舆情信息治理,提高公信力,完善舆情产业链条,最终促进舆情生态健康有序发展。因此本研究尝试提出一种基于区块链技术的舆情存证技术方案,尽最大程度在保护公众数据隐私、维护公民权益的同时,帮助职能部门有效治理网络舆情信息。

1　基于特定舆情治理的协议簇研究与设计

1.1　极端突发重大事件中舆情治理的关键问题

如何在重大突发的舆情风暴中借助区块链技术实现高效的网络舆情治理,同时保护信息主体,即保护递交舆情信息进行存证的人或自治群体的隐私,关键的问题就在于能否充分运用密码学理论使得舆情存证信息系统内外数据在信息论上实现保密性和隐匿性,能否编写相应功能的智能合约实现舆情存证信息业务的自动化维护,以及能否用密码学技术改进业务,提高决策效率。

针对这些问题,本文将会从内生性数据隐私的安全性、外生性舆情信息的法理性以及舆情信息系统业务的完备性上进行分析讨论。

1.2　内生性数据隐私的安全性研究

内生性数据是指在舆情存证信息系统中进行公示后在系统内部流动的数据。这些数据往往直接关联上链进行存证的信息主体的身份信息。如果不对这些内部流动的数据加以安全防护,那么敌手攻击系统后,便很容易窃取信息主体的隐私信息,对他们造成安全威胁。

为了保护内生性数据的隐私,给出如下的安全方案,如图 1 所示。

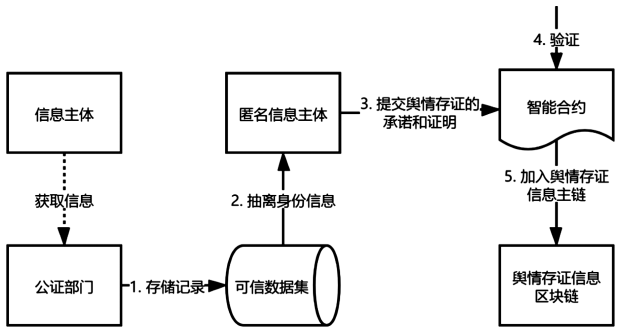

图 1 内生性数据隐私保护流程

从图 1 中可以看出，在进行内生性数据操作前，隶属于政府的公证部门需要获取信息主体的相关信息。然后公证部门在内部进行受理，将该部分信息存储在一个不对外公开的可信数据集中。从这个可信数据集中抽离出有关该信息主体的身份信息，使用这个身份信息生成相应的匿名信息主体。公证部门代理信息主体使用匿名信息主体的身份将需要上传的舆情存证信息的承诺和证明等提交到智能合约中验证，验证合法通过之后，就将该舆情存证信息加入到舆情存证信息主链中去保管。

以上阐述的是关于内生性数据的业务流程，而技术方面并没有过多的描述。因此下文将会把图 1 展现的技术流程进行公式符号化，进一步说明设计方案在隐私安全上的严密性。

定义一个信息主体 CIS，拥有需要上传的信息集合 $S=\{CIS_C, CIS_{\neg C}\}$，其中 CIS_C 属于该信息主体的核心信息（身份证号、手机号等），$CIS_{\neg C}$ 属于该信息主体的非核心信息（性别、年龄等）。有公证部门 ND，负责接收 CIS 的信息集合 S。接收到集合 S 之后，公证部门会通过内部签名将其存放到由政府部门保管的可信数据集 T 中。这个过程可以表现为以下的公式：

$$S \rightarrow ND: Sig(S, ND_{id}) \rightarrow T \tag{1}$$

其中 ND_{id} 是公证部门用来签名的部门标识，然后交由可信数据集验证，验证通过之后保存该部分签名信息。存储信息完成之后，必要时需要将存储的 N 个信息主体的信息集合 S_i 中的不同的核心信息 CIS_{Ci} 提取出来构建匿名信息主体身份 AIS_i，使用该匿名身份进行舆情存证信息的上链操作，其中 $i \in \{1, 2, \cdots, N\}$。由此，就在一定程度上保证了信息主体的身份安全。

有了信息主体的匿名，接下来就可以对上链的舆情存证信息进行安全保护。因为隐匿身份并不能完全保证上传信息的隐私安全，所以上链同时还使用了零知识证明技术来保护舆情存证信息。所谓零知识证明，是 20 世纪 80 年代由 Goldwasser 等提出的一种可以在示证者不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的密码学技术手段[8]。本文使用零知识证明来保护匿名信息主体与链上合约之间的数据交互的过程。即视匿名信息主体为示证者，链上合约为验证者。如图 2 所示。

从图 2 中可以看出，对于某个匿名信息主体 AIS，拥有需要上链进行存储的加密舆情存证信息 m。为了不让 m 泄露出去，AIS 需要对 m 进行隐私封装，即在与链上合约进行交互的时候只提交舆情存证的承诺 $Mcom$、证明 $Mproof$ 和相关的加密输入信息。图 2 中产生承诺的计算公式中的 pb 为匿名信息主体 AIS 提交承诺时使用的公钥，r 为随机数。舆情存证信息的承诺类似于匿名信息主体对外的宣告，表示自己上传了一份舆情信息。同时，为证实承诺的真实性，AIS 还需要利用一组私密钥对（pr，r）

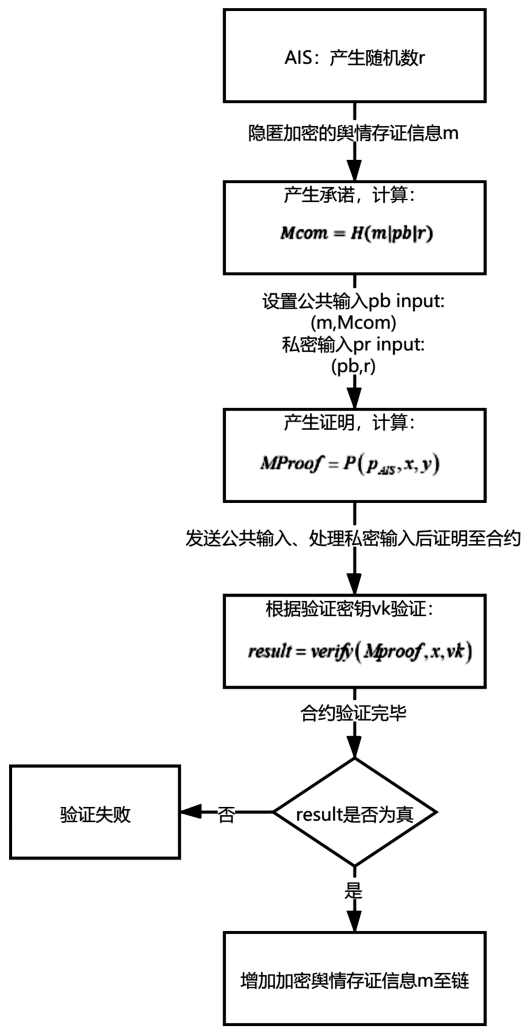

图 2 内生性舆情存证信息上链流程

和证明密钥 p_{AIS} 来向合约提供一份证明去验证,即 $Mproof$。p_{AIS} 会存储在链下匿名信息主体的设备中。

而链上特定的智能合约将会从传输信道中拿取承诺、证明以及相关输入参数进行验证,如果验证合法通过,那么就会将加密的舆情存证信息提交到舆情存证信息区块链中进行存储,保证信息不被篡改,也方便日后进行正确的舆情决策。

此外,在递交舆情信息过程中,外部表征是一个匿名的信息主体 AIS 上传了一份加密的舆情信息到舆情存证信息主链上,但是外部无关人员并不会知晓上传的舆情存证信息的具体内容,也不会知道是谁上传的,因为在上传之前已经隐匿了信息主体的真实身份。所以,综合看来,该基于内生性数据的隐私方案是较为安全的。

1.3　外生性舆情信息的法理性研究

与内生性数据相对,外生性数据是指和系统内部的模块、业务不会产生直接影响的数据流。这里只讨论与系统研究高度相关的外生性舆情存证信息的处理方式。对上链前未经特别筛选的舆情信息、链上下载后的舆情信息进行分析,使得舆情存证信息在政策法规上能够做到合情合理。如以参考数据保护体系相对成熟的欧洲相关法律为例,依照《一般数据保护条例》(General Data Protection Regulation)中首次明确的第 17 条的删除权(被遗忘权)条款,即 Right to Erase (Right to be Forgotten)[9]。为此对于舆情存证系统而言,其存证的舆情信息还应考虑删除功能。本研究通过使用区块链的智能合约技术来实现去中介干预的舆情信息删除功能。

图 3 所示是一个标准的外生性舆情存证信息的流转过程。将根据图 3 对舆情信息存证、取证与自动删除的过程进行具体的描述。

从图 3 可以看出,舆情存证信息 x 经过加密后上传到区块链进行保存,一旦上链即会转换为内生性数据。与此同时,位于链上的舆情存证信息平台会将对应舆情信息存储节点的位置信息放到外部数据库存储。取证时,需要通过外部的数据库查询对应内生性的舆情存证信息节点的位置,然后从链上调用相应的内生性舆情存证信息,对该加密的舆情存证信息进行反向解码后,获取到可读的舆情存证明文信息。最后,取证结束,需要将取证信息摘要上链,同时取证信息存储节点的位置也需要加密存储到外部数据库。

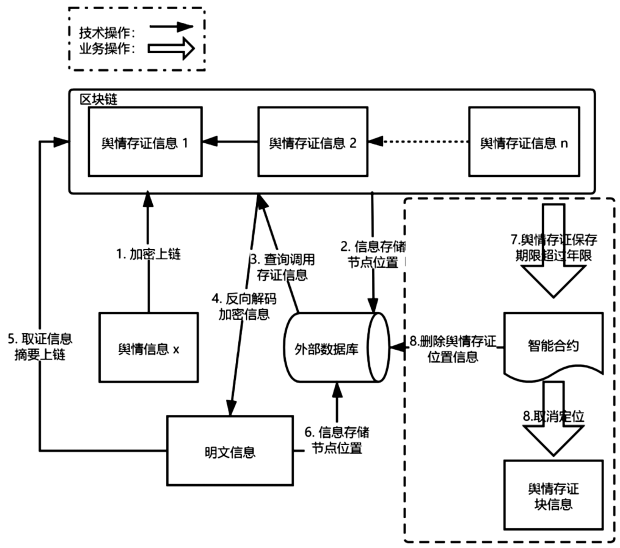

图 3　外生性舆情存证信息流转过程

上述是法理范围内的舆情存证信息的存证、取证方式。但如果链上的舆情存证信息超过法理规定的保存期限如五年之期已过[10, 11],则系统会利用智能合约操作外部的分布式存储数据库对相关内生性舆情存证信息的存储位置信息进行自动化删除。图 4 所示给出了智能合约处理过期舆情存证信息的过程,以便对法理性研究进行详细解释说明。

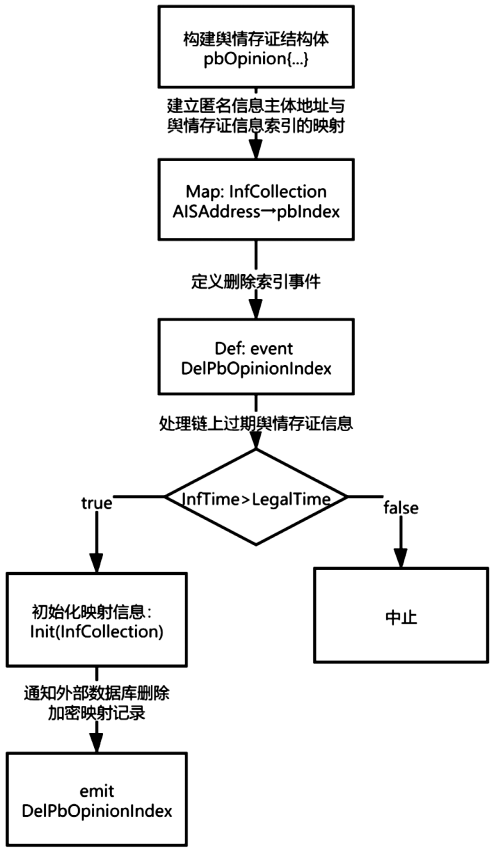

图 4　过期舆情存证信息的处理方式

因为对于单个区块的块信息是很难篡改的，所以要想合理处理链上失效的舆情信息，可以通过删除其相关的映射信息，即取消外部数据库中记录的索引信息。这样就会在大量舆情信息存储的区块中无法准确查找到对应的舆情存证块信息。并且链上失效的舆情存证信息也是经过加密处理的，在没有获取特定解密方式的前提下，也是无法查阅的。正如图 4 中所示，先将原来合约中对应索引下的舆情信息初始化，然后触发删除外部数据库中对应索引的事件。

此外，考虑到存在敌手攻入外部分布式数据库窃取信息的情况，即可能存在窃取所有舆情存证的节点位置信息从而破坏外生性数据隐私的问题，还需要将外部数据库中的链上舆情存证的映射信息进行加密，即非明文存储。方式如图 5 所示。

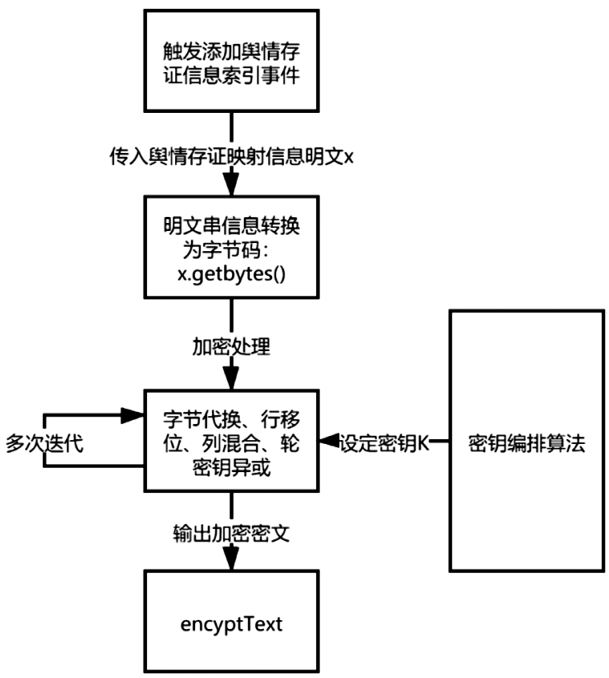

图 5　外部数据库中舆情存证映射信息的二次加密

从图 5 的加密流程可以看出，是用密码学算法 AES 对称加密技术进行二次加密的，因为对称加密方式计算量小，解密是加密的逆过程，加密和解密映射信息的时候也就相对高效。此外，为了避免相同明文产生相同加密的结果，使用 AES 的 CBC 模式，即将密码进行分组链接，引入随机的初始变量加强安全性。这样就可以有效防范敌手在多项式时间内使用暴力破解的方式对舆情存证信息进行攻击。

1.4　舆情信息系统业务完备性研究

1.4.1　基于舆情存证信息决策的业务体系

为了相关职能部门能对突发的负向舆情风暴进行有效处理，设计了图 6 的架构方案。

从图 6 中可以看出，信息主体存证时，需要将舆情信息公示到电子公示板上，然后由群众、媒体在公示期间查询监督舆情信息，并把舆情信息反馈到下级政府部门，由下级政府部门根据具体情况进行处理。公示期结束之后，需要将电子公示板上的舆情信息上报给下级政府部门。待下级政府部门受理之后，将送审材料公示到电子公示板上，此时群众、媒体同样可以在公示期间查询监督送审材料，并将送审材料的反馈信息交由上级政府部门处理。在送审材料公示期结束后，上级政府部门会从电子公示板上拿到送审材料，然后送审到纪检部门。最后由纪检部门批阅转交到国有存证机构（公证部门），由该机构上传存储舆情信息到舆情存证信息平台。

为了实现舆情存证获取的高效决策，需要由上级政府部门讨论筛选出一批人员充当授权主体，对公检法三大部门调取舆情存证信息的请求进行差分授权。本研究给出一种“群—主”签名的方式来实现这种授权机制。具体方式如图 7 所示：

从图 7 中可以看出，以指定三个授权人员为例，由上级政府部门对指定的授权人员分发私钥分片 $gsk[i]$，$i\in\{1,2,3\}$，然后不同的授权人员会利用各

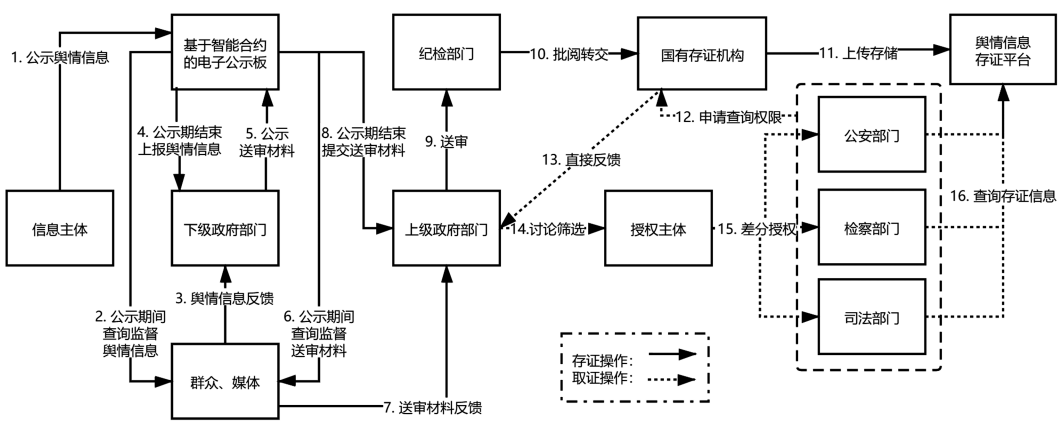

图 6　舆情存证信息决策架构图

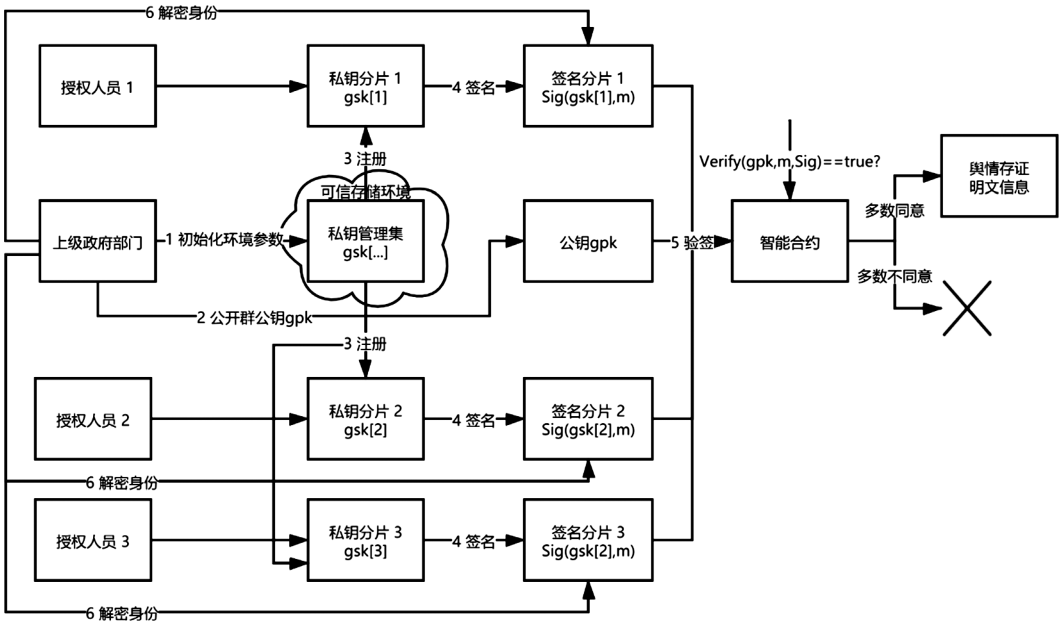

图 7　差分授权设计方案

自的私钥分片进行签名 $Sig(gsk[i],m)$,然后交由智能合约利用公开的公钥 gpk 进行签名验证,如果多数人员同意授权,那么相关部门就可以获取到经过外生性数据取证处理的舆情存证明文信息;如果多数人员不同意,则无法获取相应信息。最后,上级政府部门利用私钥管理集中的 $gsk[\cdots]$公示授权人员信息,以便于决策的公开透明。此外,因为该过程中仅上级政府部门可以通过自己的管理私钥,识别授权成员的个体身份,而且任一成员不能冒充其他成员进行签名,从而也使得上级政府部门的监管决策成为可能。

1.4.2　基于智能合约的公示路径多样性研究

上面主要阐述了正常情况下舆情存证系统的完备性。本小节将针对舆情信息上链决策前的公示方式做额外的补充,即需要考虑舆情信息公示期结束后的反馈路径。图 8 为公示期结束的信息反馈处理方式:

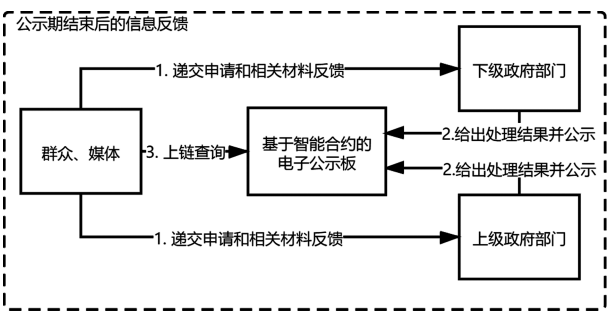

图 8　公示期结束的信息反馈处理方式

如图 8 所示,对于公示期结束的信息反馈,此时群众、媒体在反馈信息的同时还需要递交申请和相关的证据材料给下级政府部门或者上级政府部门。由政府部门给出处理结果并公示到电子公示板上,然后群众、媒体查询电子公示板,获悉处理结果。图 9 是基于智能合约的电子公示板的设计流程图。

从图 9 中可以看出,下级政府部门或者上级政府部门对群众、媒体提交的相关信息和材料进行整

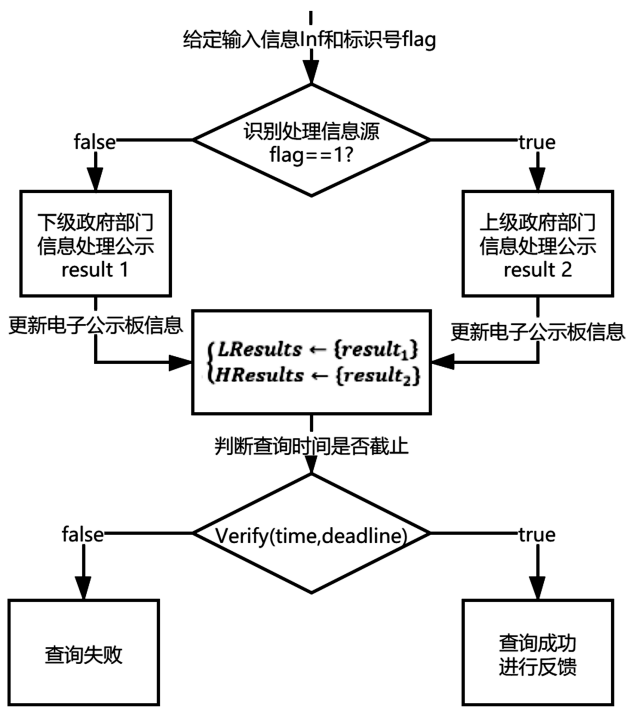

图 9　基于智能合约的电子公示板的设计流程图

合处理后，会利用信息结果处理的函数接口提交到电子公示板上，由电子公示板识别信息源后，分类别加入到不同的公示信息集合里，然后更新旧电子公示板上的信息。群众、媒体只要在查询处理结果的截止期限内查询反馈结果都是合法正常的。否则，超过时限，电子公示板将会自动剔除这些信息，使得查询无效。

综上，系统的业务设计上实现了存证时信息公开透明、多级部门层级监督，确保舆情存证信息的有效性、合法性；取证时上级政府部门进行差分授权，有助于基层快速获取舆情信息、及时处理决策。所以这种跨组织、跨部门授权基层组织、部门查询舆情存证信息，快速取证、固证的方式是相对合理的。

2 舆情存证平台面临的挑战与问题

舆情存证平台是在国家特定极端情况下的特殊舆情治理方案，并非常态化舆情治理方案。目前还只是在理念以及初步技术方案的探讨阶段，可能在实践中还面临诸如用户层面、管理层面、技术层面、法律层面等多重挑战，必将是一个磕磕绊绊的过程。

首先，社会抵制是用户层面的最大问题。舆情存证平台原本是希望促使社会公众理性在互联网上发布信息，但也有可能成为引爆舆情的火药点。网络空间作为一个相对宽松的意见场，社会公众已经习惯了匿名和自由，突然被带上“存证”言论的“紧箍咒”，绝大多数成员都会深感被冒犯，即使在极端的情况下，也不容易获得社会公众的谅解。

第二，管理层面也面临不少挑战。在系统的管理模式上，是采取强制性的还是自愿性的，这是个不得不面对的问题。对于舆情的采集，要根据最小化原则，只采集必要的数据，而严格禁止不必要的采集，但是如何界定哪些舆情信息是必要且符合最小化原则是值得考虑的。对于采集来的舆情信息，应严格规定使用的目的、场景、时限等，一旦核实不存在问题，就应立即销毁数据，并作公众告知，但这些都需要在国家层面做出严谨论证之后给出具体的严格规范。

第三，技术层面有待进一步改进。首先，在技术层面上看，必须要融合其他“互联网＋”技术，积极拥抱大数据、人工智能等技术优势，来更好更快地解决现有电子数据存证中存在的诸多痛点。但由于是在极端特定情况下来使用的，那么就需要足够的极端特定情况的数据来进行模型训练，因而很容易仅仅起到存证的单一作用。另外，存证数据的安全性问题也值得关注，一旦信息泄露，那么将可能对无辜的社会公众带来至深的负面影响，令他们有可能遭受网络人肉、网络欺凌，甚至社会偏见与社会污名。

第四，法律层面，这一领域还是空缺，需要论证研究。以新冠肺炎疫情数字化接触者跟踪 App 的应用为例，为了推出“健康码”，中国在 2020 年 3 月 6 日发布了新版《信息安全技术个人信息安全规范》，明确了“行踪轨迹”属于“个人敏感信息”，在收集此类信息时，需要满足“最小必要原则”和“合法性原则”，只有在“与公共安全、公共卫生、重大公共利益直接相关”等 11 种例外情形下才不必征得授权同意。2020 年 4 月 16 日，欧盟委员会发布了“支持抗击新冠疫情应用程序的数据保护指引”，提出对于新冠肺炎疫情数字化接触者追踪技术应用的 7 个数据保护必要条件。对于舆情存证系统也是一样，需要对极端特定情况的可能应用提前做出法律层面的周全考虑，才能为舆情信息存证的合法性提供根本的基础。

3 结论及展望

突如其来的新冠肺炎疫情不仅带来了新冠病毒，也带来了网络空间的信息“病毒”。在极端特定情况下，科学有效地消除网络空间中的信息“病毒”，就能对发布这些信息“病毒”的人形成足够的威慑。在此目标下，本研究给出了在充分考虑公众的信息隐私安全、舆情存证的法理性、业务运行合理条件下的一种基于区块链技术的舆情存证信息系统的设计方案。

但是，舆情存证信息系统不仅仅涉及技术问题，更重要的是涉及诸多社会问题，公众的言论自由权、人权、隐私保护、伦理道德等等一系列复杂因素。技术方案容易给出，但是与此配套的社会机制方案才更重要。如果没有令社会公众接受的配套社会机制方案，技术层面的研究还需要搁置以待合适的时机。

针对当前各界关注的舆情存证问题，本文的研究期望可以起到抛砖引玉的作用，这一领域还有很大的研究空间有待更多学者探索。

参 考 文 献

[1] 李健，宋昱光，张文. 区块链在突发事件应急管理中的应用研究. 经济与管理评论，2020，36(4)：5—16.

[2] 匡文波，杨梦圆，郭奕. 区块链技术如何为新闻业解困. 新闻论坛，2020(1)：18—20.

[3] 匡文波，黄琦翔，郭奕. 区块链与新闻业：应用与困境. 中国报业，2020(5)：16—19.
[4] 姜云婷. 可行性的展望：区块链技术在新闻行业中的运用. 传播力研究，2019，3(7)：46.
[5] Humbeeck AV. The blockchain-GDPR paradox. Journal of Data Protection & Privacy，2019.
[6] Feng Q，He DB，Zeadally S，et al. A survey on privacy protection in blockchain system. Journal of Network and Computer Applications，2019，126：45—58.
[7] Alsdurf H，Bengio Y，Deleu T，et al. COVI White Paper. arXiv，2020.
[8] Goldwasser S，Micali S，Rackoff C. The knowledge complexity of interactive proof systems. SIAM Journal on Computing，1989，18(1)：186—208.
[9] 薛丽. GDPR 生效背景下我国被遗忘权确立研究. 法学论坛，2019，34(2)：100—109.
[10] 赵锋.《征信业管理条例》述评. 征信，2013(4)：51—53.
[11] 佚名. 中华人民共和国网络安全法. 新疆农垦科技，2017(1)：80—82.

The Design of Public Opinion Evidence and Its Application Challenges Based on Blockchain

Liu Feng[1, 2]　Yang Jie[2]　Li Zhibin[3]　Qi Jiayin[2, 4*]

1. *School of Computer Science and Technology*, *East China Normal University*, *Shanghai* 200062
2. *Institute of Artificial Intelligence and Change Management*, *Shanghai University of International Business and Economics*, *Shanghai* 200336
3. *School of Data Science and Engineering*, *East China Normal University*, *Shanghai* 200062
4. *Key Laboratory of Trusted Distributed Computing and Services*, *Ministry of Education*, *Beijing* 100866

Abstract　The epidemic of the Coronavirus Disease 2019 (COVID-19) that is sweeping across the country has not only carried the virus harmful to health, but also spread the information "virus" in the public opinion space. How to deal with information "virus" in extreme major emergencies through technical solutions is a hot topic and a challenge of concern nowadays. This article proposes a blockchain technology-based design idea to address the three difficulties of public opinion evidence: information and privacy security at the technical level, legality at the legal level, and rationality at the operational level. The design incorporates zero-knowledge proof technology to solve the problem of public data privacy, builds smart contracts that match the logic of public opinion archiving to solve the problem of legality in technology landing, and designs a differential authorization model to solve the problem of rationality in decision making. As public opinion archiving is a complicated social issue, we also discussed the challenges and problems in the practice of public opinion archiving system. COVID-19 will eventually end, but the triggered governance of information "virus" in extreme major emergencies has just begun. This article is a preliminary introduction to inspire more scholars to be engaged in this issue.

Keywords　COVID-19; blockchain; privacy computing; public opinion archiving system; zero-knowledge proof

(责任编辑　刘　敏)

* Corresponding Author, Email: qijiayin@139.com