识，更好的减少网络侵权现象的发生，我们一定要简化对侵权人责任追究的方式，在严格的责任认定标准下，再确认侵权人应当承担相应责任的基础上，对其实施处罚。只有这样我们才能够更好规范网络行为，更好的保护公民的生活安宁权。

4　结语

现如今，公民越来越注重权利的维护，而生活安宁权作为与我们的生活息息相关的一项重要权利，也逐渐引起人们的广泛关注。面对网络行为侵犯生活安宁权的现象，我们要做的不仅仅是责任的追究与处罚，我们更应该关注的是发生这种现象的根本原因，注重网络教育，加强道德法制宣传，从根本上减少此类现象的发生。只有这样，公民的生活安宁权才能得到更好的保护，我们也能享受到更加和谐美好的网络空间。

参考文献：

[1]王利明.生活安宁权：一种特殊的隐私权[J].中州学刊，2019（07）：46-55.

[2]方乐坤.论精神安宁权的界限及其构成[J].河南社会科学，2007（04）：99-101.

[3]饶冠俊.创新社会管理视角下的生活安宁权界定及法律保护[J].学术交流，2012（S1）：52-54.

区块链技术下的个人信息保护路径

◆刘敏

（中国人民公安大学　北京　100038）

摘要：当前，个人信息多被各大网络运营商收集并存储于中央数据库中，不仅使个人逐渐丧失了对个人信息的控制权，也增加了个人信息泄露的风险。区块链的去中心化、不可篡改性以及其所构建的新型信任机制，与个人信息保护存在一定的契合性，可以解决中心化信息存储机构下个人信息安全问题。但区块链技术本身与个人信息保护存在着内生冲突，如哈希化信息是否属于法律规范中的个人信息，区块链的不可篡改性与个人信息更正、删除需求之间的矛盾，区块链分布式架构与个人信息义务主体特定之间的矛盾等。因此，本文对哈希化信息进行了明确，从立法目的层面提出了更正与删除的替代措施，并对义务主体的明确提供了思路。

关键词：区块链；个人信息保护；去中心化；不可篡改

基金项目：北京市社会科学基金规划项目（20FXC028）

随着大数据时代的到来，个人信息数量呈指数型增长趋势，各大网络运营商广泛收集、处理个人信息，使得个人对信息的控制权逐渐虚化，个人信息自主权以及个人信息安全面临着前所未有的挑战。传统的个人信息保护模式以制度信任为主，通过不断加强个人信息保护立法，以实现对个人信息的规范性保护。然而，个人信息安全问题并未因此得到缓解，中心化机构下的个人信息泄露、个人控制虚化、伪造和篡改个人信息等现象仍屡见不鲜，传统的制度信任已难以满足大数据时代下个人信息保护的复杂性。因此，以去中心化为主要特点的区块链技术所构建的技术信任逐渐在个人信息保护中发挥作用。区块链这一概念由中本聪于 2008 年在比特币白皮书中提出，而后被许多国家和地区纳入国家发展战略。自 2016 年至今，我国出台了一系列政策和规定，将区块链正式列为国家战略的优先突破方向。区块链以其所具有的去中心化、不可篡改性、可追溯性、分布式节点共识机制以及智能合约等特点，广泛应用于征信、保险、医疗、知识产权、物联网、公益、智慧城市、政务服务等领域，一些学者也关注到区块链与个人信息保护的契合性，提出了将区块链应用到个人信息保护中的规范路径。然而，在肯定区块链作用的同时，也不能忽略区块链技术本身与个人信息保护的内在冲突，如区块链的不可篡改性与个人信息更正、删除之间的冲突，区块链的去中心化与个人信息保护中义务主体特定之间的冲突等。因此，在将区块链应用到个人信息保护的过程中，不可忽略区块链技术的局限性，应当通过技术与法律的双重保障，更好地实现个人信息保护。

1　个人信息保护现状

个人信息安全问题是当今社会治理的一大难题，我国出台了近百部有关个人信息保护的法律、行政法规、国家标准等规范性文件[1]，以期解决个人信息安全问题。但法律的事前规制效果较差，事后补救又具有滞后性和损失的不可弥补性，且法律的外在规制使得个人信息保护的内在问题无法得到妥善解决。因此，个人信息保护仍面临着诸多困境。

1.1 信任危机

信任是社会良好运行的基础。随着经济社会的发展，人与人之间的交往基础实现了由人际信任向制度信任的转化。制度信任是依托于契约、法规、制度等建立起来的信任，作为一种中介形式的存在，其终极目的仍是达到人际信任。互联网时代仍延续这种制度信任，以第三方机构为代表的中心化网络运营商通过制定一系列条款和政策，以减少交易双方重新建立信任的成本，通过对中心化机构的信任高效完成交易。然而，对中心化机构信任的过度依赖，反而会造成信任的弱化。一方面，中心化机构掌握着海量的个人信息及交易信息，信息不对称现象严重，与传统的线下交易相比极易造成垄断现象[2]，部分互联网平台存在售卖个人信息、非法利用个人信息以及滥用权力引导舆论等情况。另一方面，中心化存储导致数据过度集中，风险暴露程度高，极易遭受黑客攻击，系统一旦瘫痪就会出现海量的个人信息泄露以及被篡改等风险。因此，以中心化机构为代表的制度信任在互联网时代具有一定的局限性，也会导致用户逐渐丧失对中心化机构的信任。

1.2 个人信息泄露

个人信息的收集和使用是网络运营商提供产品和服务的重要基础，也是大数据时代信息技术发展的必备要素，个人信息的聚集有利于最大程度实现信息价值，促进经济发展和社会治理。然而，中心化机构为了谋取私利，可能非法利用其掌握的大量个人信息，导致个人信息的泄露。且中央数据库又极易遭受外在攻击，而数据一旦被泄露，则会影响到庞大的社会群体。根据《2021 年黑灰产行业研究及趋势洞察报告》显示，2021 年共监测到有效数据泄露事件共 1700 余起，涉及近 500 家企业、30 多个行业，其中，数据类型主要集中在平台用户信息，占比高达 98%，其次是公民个人信息、数据库账号等[3]。这些泄露的数据通常会被用于诈骗、营销推广等，这也是近年来我国电信诈骗剧增的主要原因之一，严重危及用户的信息安全、财产安全以及社会秩序。

1.3 个人控制虚化

个人信息自决权理论在德国 1983 年“人口普查案”中首次被提出[4]，现已成为各国在个人信息保护立法中所普遍遵循的理论基础。20 世纪 70 年代，美国提出“公平信息实践准则”，将其作为个人数据隐私保护的一项基本原则，其亦是建立在个人信息自决权的基础之上[5]。纵观我国有关个人信息保护的立法，我国在个人信息保护的立法理念上总体采取个人信息控制论，2021 年出台的《个人信息保护法》更是将告知同意作为收集和处理个人信息的一项基本规则。令人遗憾的是，依托于个人信息自决权的告知同意规则并未达到预期效果，实践中信息处理者抽象且模糊的告知、因信息不对称引起的同意基础匮乏以及因信息处理者的绝对地位而导致用户意思表示不自由等情形屡见不鲜，严重削弱了告知同意规则的适用效果。个人对信息的控制权逐渐被架空，即使在收集阶段合法获取了个人信息，之后的处理以及大数据对信息的二次挖掘和利用也大多处在用户不知情的情况下，个人实质上丧失了对个人信息的控制权。

2　区块链在个人信息保护中的作用

区块链是一种分布式账本数据库，分布式账本是相较于中心化存

储而言的，其以去中心化为主要特征，通过链式结构将一个个单独的区块按照时间顺序链接起来。传统的数据库中也有类似的拉链表模式，但区块链在此基础上增加了哈希、时间戳等新技术，以此保证整个区块链的准确性和完整性[6]。区块链通过分布式账本、共识机制、智能合约以及密码学等相关技术[7]，保证了链上数据的不可篡改、公开透明、可信任度以及隐私保护等，并通过点对点分布式网络架构，实现了去中心化。

2.1 分布式节点共识机制

去中心化是区块链最核心的特征，其主要依托于分布式系统架构，以此实现点对点的数据共享，其运作原理仍是基于共识算法机制。在传统的中央数据库存储模式下，黑客攻击和信息处理者售卖是导致个人信息大规模泄露的主要方式[8]。而区块链是基于分布式账本的去中心化数据库，各节点之间地位平等，任何节点对数据的操作都会被其他节点所察觉，因此强化了各节点之间对数据泄露的监控。外部对区块链的攻击和篡改，也需经过共识机制的认可，各节点都具备验证功能，黑客必须达到 51%以上的算力才能攻破区块链，而随着区块数量的不断增加，达到这种算力是十分困难的。即使一个节点被攻破或信息有所损失，但因分布式账本的存储机制，其他节点也有完整的数据备份，不会影响整个网络体系的正常运行。同时，去中心化的分布式系统不存在中心化机构，单个节点无法控制整个区块链的信息处理方式，不会出现因谋取私利而售卖个人信息的情况[9]。因此，区块链是防止个人信息泄露的有效途径。

区块链分为公有链、私有链和联盟链。在公有链网络中，任何主体都可以自由加入或退出，其上的所有节点都可以验证区块信息，除了个人的私密信息被加密外，其他节点的所有数据信息均对外公开，且进行分布式记账，个人可以通过节点掌握对个人信息的使用。区块链的透明性增强了用户对个人信息的控制，保障了个人对信息利用的知情权，在出现侵犯个人信息的情形时可以即时查询并追溯调查，避免了中心化机构系统下对信息利用的不知情甚至对侵犯个人信息的不知情等情形。且这种去中心化的分布式存储结构，使得区块链上每一节点的数据完全相同，可以消除中心化存储模式下的信息不对称问题，避免信息控制者利用信息不对称实施侵犯用户合法权益的行为。

2.2 智能合约

智能合约是一种区别于传统合约的计算机交易协议，通过事先协商拟定合同条款，而后将合同内容转换为代码形式以便于电子化交易，是区块链的核心技术之一。在符合预定条件的情况下，智能合约便会自动执行，不以当事人的意志为转移[10]，且一旦执行即具有不可篡改性，保证了合同的稳定性，有利于在合同双方之间建立互信。

智能合约摆脱了第三方机构的束缚，创建了一种基于智能合约本身的信任机制[11]。智能合约建立在去中心化的模式之上，实现了点对点网络结构的交易模式，双方通过私人密钥形式进行交易，免除了对第三方信赖的构建。同时，智能合约具备自我执行机制，只要符合预先设定的条件，合同便会自动履行，无需考虑当事人的意思自治。因此，这种基于算法的机器式运作，更有利于在没有信任基础的交易双方之间迅速有效地建立信任关系。技术信任赋予了信任关系新的生命力，使信任不再局限于带有感情色彩的人际信任以及带有时代色彩的制度信任，创建了大数据时代特有的信任机制。但技术信任不是最终目的，任何方式的使用最终都是为了达到人与人之间的信任，构建技术信任并不意味着彻底抛弃人际信任与制度信任，而应根据各自特点适用到不同领域。在个人信息保护方面，现行的制度信任已难以为继，通过智能合约等去中心化形式构建的技术信任更有利于大数据时代下个人信息保护中信任问题的解决。

2.3 哈希函数

哈希函数是密码学中的一个重要分支，它可以将任意大小的数据转化为固定大小的二进制串，由此得出的固定长度的字符串即为哈希值。区块链由“区块”和“链”两部分构成，“区块”又可分为“区块头”和“区块体”（如图 1 所示）。个人信息经哈希化后输出固定的哈希值，该哈希值会被记录在下一个新的交易区块的区块头中，新的交易区块将按照时间顺序链接到原来的区块上，这样，各交易区块按照顺序链接起来，保证了数据的完整性。个人信息收集、使用等流转的全过程均会被记录并加盖时间戳，实现了数据的可追溯性，用户可有效控制个人信息，避免因不知情、信息不对称等原因无法实质控制个人信息被使用等问题。

哈希值具有抗碰撞性，每个区块产生的哈希值都是唯一的，如果改变数据中的任何一部分，都会产生完全不同的哈希值。若任何一个区块发生变动，如被删除或交易数据被篡改，则链上所有的区块均会检测到，因为被篡改后的区块生成的哈希值与原来的哈希值完全不同，原来的哈希值找不到对应的区块数据[12]。同时，哈希值的不可逆性也可有效保证信息安全，经过哈希化后的个人信息都是固定长度的字符串，无法识别出具体内容，也无法从已知的哈希值中推导出原始数据，因此可在一定程度上认为其不具有特定识别性。且区块链中节点的关键身份信息在传输时往往通过私钥进行加密，即使链上的信息发生泄露，只要私钥没有泄露，这些信息就无法破解，从而失去利用价值[13]。因此，哈希函数是证明数据没有被篡改的重要方式。

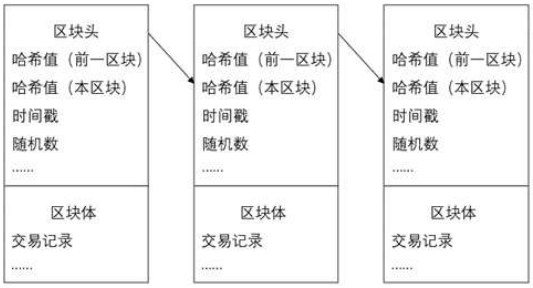

图 1 区块链结构图

3 区块链与个人信息保护的冲突

诚然，区块链的去中心化、不可篡改性、可追溯性以及其所构建的新型信任机制等在个人信息保护方面发挥了重要作用，但区块链技术本身与个人信息保护仍存在着内在冲突。

3.1 哈希化的个人信息与法律规范中的个人信息

世界各国在有关个人信息保护的法律规范中，普遍将“可识别性”作为界定个人信息的核心要素。我国《个人信息保护法》第 4 条第 1 款规定，“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。”由此可见，我国亦是将具有“识别可能性”的信息纳入《个人信息保护法》的规制当中。区块链在存储个人信息时，通过哈希函数将信息进行哈希化处理，最终得到固定长度的哈希值，由于哈希值具有不可逆性，不能反向推导出原始数据，因此，有学者认为，经哈希化后的个人信息可追溯性极低，实现了个人信息的匿名化[14]。但也有学者认为，尽管哈希化后的信息很难破解，但并非不能实现，且我国个人信息保护的立法理念是以保护为主，因此在具备识别可能性的情况下，应当将这种相对匿名状态的哈希化信息纳入个人信息保护的客体[15]。由此可见，哈希化后的个人信息是否达到了《个人信息保护法》中的匿名化状态仍存在巨大争议。

3.2 区块链不可篡改性与个人信息更正、删除的冲突

个人信息的更正和删除是实现个人信息控制的重要方式。我国《民法典》第 1037 条规定了自然人可以对个人信息进行更正和删除，在此基础上，《个人信息保护法》第 46 条、47 条分别对更正权和删除权的适用情形与义务主体进行了细化。欧盟《通用数据保护条例》第 16 条、17 条也分别规定了数据主体的更正权和被遗忘权，美国最严厉的个人隐私保护法案《加州消费者隐私法案》也赋予消费者以删除权。由此可见，无论是域内还是域外，都将个人信息的更正和删除作为实现个人信息自决权的重要方式。然而，不可篡改性是区块链最核心的特征之一，区块链上的数据按时间顺序形成了链式存储结构，只允许追加而难以删除，这也是保证信息真实性和完整性的重要方式。区块链的去中心化特征意味着无论是区块信息的增加还是修改与删除，都必须凭借共识机制完成。但是，由于各节点地位平等且都不具有直接控制区块链上信息的能力，因此要达到 51%以上的节点共识十分困难，随着节点数量的不断增多，这种结果几乎不可能实现。

3.3 区块链分布式架构与个人信息义务主体特定的冲突

我国《个人信息保护法》对个人信息处理者的概念作出了界定，并对其应尽的义务做了详细规定，欧盟《通用数据保护条例》也对数据控制者进行了定义。两者都是基于数据信息的中心化管理，将对信息处理的目的与方式具有决定性作用作为实质判断标准，对权利主体与义务主体作了明确区分。然而，区块链是以去中心化为主要特征，每个节点在享受区块链服务的同时，又与其他区块存在着验证关系，因此，个人节点实质上兼具着双重身份。私有链具有部分去中心化特征，因此仍有可能存在一个类似中心化机构的信息控制者。但公有链是点对点的分布式网络架构，每个节点可以决定加入或退出，是自己信息的控制者，但单个节点无法决定整个区块链上信息的处理，也无法实质履行法律规定的相应义务，根据实质判断标准，个人节点无法成为个人信息保护的义务主体，这就导致区块链中信息处理者不明，《个人信息保护法》中义务的执行面临巨大困难。

4 区块链与个人信息保护之间冲突的协调

4.1 明确哈希化信息的性质

我国《个人信息保护法》第 73 条规定，“匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。”匿名化信息由于无法识别到特定个人，不会侵犯到个人合法权益，因此许多国家都未将其列入法律保护的范围之内。但是，匿名化数据有着非常严格的要求，欧盟委员会重要咨询机构的第 29 条工作组认为，只有在符合识别性、链接性和推定性[16]时，才能将数据视为完全匿名化，否则仍要受到法律规制。就是否符合“特定识别性”，学界出现了两种观点，一是绝对主义，其以最终是否能被破解为出发点去认定数据的匿名化；二是相对主义，其在综合考虑所投入的金钱、时间等成本的基础上，判断数据是否符合匿名化标准。虽然区块链去中心化的特征使得链上的节点分布于世界各地，但网络中的活动信息与公钥相结合，仍存在可能被识别的风险，且匿名是相对的，随着计算机科学的不断发展，原来被认定为不可识别的信息仍有可能关联到个人。因此，哈希化信息仍具备可识别性，应纳入法律的规制范围之内。

4.2 赋予更正、删除以新的内涵

法律赋予个人以更正、删除权，旨在保障个人信息的准确性，避免因信息错误而妨碍信息主体正当行使权利，因此，更正和删除只是达到此种效果的一种方式，并非唯一路径。《通用数据保护条例》第 16 条对更正权规定了替代措施，可以通过“提供额外声明”的方式对数据进行完善。在区块链中，可以通过添加新区块的方式，对之前信息存在错误的区块进行更正和补充说明，达到覆盖原有区块的目的。新区块上链同样也需经过所有节点的一致认可，防止信息主体随意更改信息，保证区块链信息的稳定性和准确性。对于删除而言，我国法律目前尚未对其作出明确定义，但通说认为，只要达到数据的“不可使用”即可[17]。“删除”分为绝对删除和相对删除，绝对意义上的物理删除难以实现，因此可采取达到“不可使用”标准的相对删除措施。我国《个人信息保护法》第 47 条规定，“法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。”第 51 条对安全技术措施作出了具体规定，如加密、去标识化等。此外，匿名化抑或是删除链接都是有效的相对删除方式。因此，对区块链上的数据信息进行加密后删除密钥或对信息采取去标识化或匿名化等，都不失为一种有效的信息处理规则。

4.3 对节点进行区分以明确义务主体

在明确区块链中义务主体时，应当对参与共识机制的节点与仅选择区块链服务的节点进行区分。按照实质判断标准的要求，信息主体需要对信息处理的目的和方式产生实质影响，才能成为法律规定的义务主体。若信息主体选择区块链服务仅是为了单纯使用某项服务，如信息备份等，而并未作为节点参与到共识机制对其他信息处理产生实质影响，则不能苛责其承担安全保障、应急处理等义务[18]。以金融机构为例，若其只用区块链存储用户的交易信息，而并未实质影响数据的处理目的与方式，则其不能作为承担责任与义务的主体。对不同节点之间的区分，可以将不具有实质控制能力节点排除在义务主体之外，同时为义务主体的明确提供了一定的参考。

5　结语

我国《民法典》将个人信息保护纳入了人格权编的规范体系之下，对个人信息保护进行了原则性规定，《个人信息保护法》的出台为个人信息保护提供了可操作规范。然而，个人信息安全问题仍存在诸多问题，借助区块链进行个人信息保护成为一种趋势。区块链构建的新型信任机制解决了原有制度信任下的信息不对称问题，实现了个人对信息的自主控制权，在防止信息泄露与篡改方面发挥着重要作用。

区块链技术与个人信息保护之间的内在冲突，根本是源于区块链的去中心化与个人信息保护法律规范的中心化体系之间的矛盾。在处理两者之间的冲突时，不能以牺牲区块链的原有特性为代价去迎合个人信息保护的需要，区块链之所以应用广泛并被列入国家发展战略，正是因为其所具有的去中心化、不可篡改等核心特征，这些特征也契合了个人信息保护的多方面需求。因此，除了从技术层面解决两者的冲突之外，可以加强对现有法律规范的目的解释，使其适应大数据时代下不断发展变化的新形势。通过区块链对个人信息进行保护的同时，区块链的公开透明也能更好地实现信息共享，实现个人信息的社会价值。当然，区块链技术本身仍有待进一步完善，个人信息保护也是一个复杂且长期的系统工程，许多理论问题以及技术规范问题仍有待进一步研究与探讨，以更好实现区块链与个人信息保护的结合。

参考文献：

[1]齐爱民，张哲.识别与再识别：个人信息的概念界定与立法选择[J].重庆大学学报（社会科学版），2018，24（2）：119-131.

[2]杨继. 区块链、互联网信任与制度设计[J]. 上海经济研究，2021（6）：27-38.

[3]鬼谷实验室，永安在线情报平台. 2021 年黑灰产行业研究及趋势洞察报告[EB/OL]. https://mp. weixin.qq.com/s/xGY1PxoH9Tlio2mWH7QLjw?.

[4]Volkszählungsurteil，BVerf G 65，1.

[5]王苑.数据权力视野下个人信息保护的趋向——以个人信息保护与隐私权的分立为中心[J].北京航空航天大学学报（社会科学版），2022，35（01）：45-57.

[6]黄芸芸，蒲军.零基础学区块链[M]. 北京：清华大学出版社，2020.

[7]王从光.区块链技术应用于个人信息保护的法理解读与治理[J].西北民族大学学报（哲学社会科学版），2021（6）：107-117.

[8]王禄生，王爽. 困境溯源与模式创新：基于区块链的个人信息合作治理研究[J]. 中国行政管理，2020（12）：56-61.

[9]陈奇伟，聂琳峰. 技术+法律：区块链时代个人信息权的法律保护[J]. 江西社会科学，2020，40（6）：166-175.

[10]王雨乔. 智能合约的机器信任构想：论信义义务之转向[Z]. 复旦大学法律评论，2020：219-230.

[11]许可.决策十字阵中的智能合约[J].东方法学，2019（03）：44-55.

[12]（美）提安娜·劳伦斯.区块链精要：全球数字化时代的区块链多重博弈[M]. 鄢倩等译. 北京：清华大学出版社，2021.

[13]李志杰，郭杰群，王阳雯.区块链+：重构与赋能[M]. 上海：格致出版社：上海人民出版社，2021.

[14]Ameer Rosic. What Is Hashing? [Step-by-Step Guide-Under Hood Of Blockchain] [EB/OL]. https://blockgeeks.com/guides/what-is-hashing/?amazonai-language=zh.

[15]罗勇. 特定识别与容易比照：区块链背景下的个人信息法律界定[J]. 学习与探索，2020（3）：59-65.

[16]El Emam K，Alvarez C. A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques[J]. International Data Privacy Law，2015，5（1）：73-87.

[17]Information Commissioner’s Office， Deleting personal data[EB/OL]. https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf.

[18]王禄生. 区块链与个人信息保护法律规范的内生冲突及其调和[J]. 法学论坛，2022，37（3）：81-95.