基于区块链的电子档案及其流转

**档案管理及其流转的一些问题**

1. 当事人对档案的重视性不足，不到用到是不会去接触。更对档案内的文件影响不深。

假设缺少文件，就会变成一件麻烦事。又如果知道档案缺少什么文件，则可以提前做准备。

1. 档案管理复杂。不同的人来自不同的地方，又去向不同的地方。往往出现丢失，改等问题。基于区块链的电子档案及其流转可以防篡改，防丢失。
2. 根据相关文件规定，转递档案须通过机要交通或派专人送取，严禁个人自带档案转递。因此，毕业生档案应由学校通过机要交通（包括EMS标准快递）或派专人转递，严禁毕业生个人自带档案转递。电子传递则省时省力。
3. 档案查询较麻烦，需本人携带证件到机构查询。电子查询方便快捷。
4. 特定行业档案管理费用居高不下。

档案的重要性与价值（作用）

档案已经成为现代社会发展史最为重要的文献参考资料之一，是国家机构社会团体组织及个人在社会活动中直接形成的有价值的各种历史文献资料。中华五千年的文化史，世代相传，档案发挥着独特的价值作用，它是将人类记忆延续成为联系过去和未来的信息传送纽带，通过历史记载，可以将人类的发展历史完整保存下来，成为后来人探究和探索历史发展的重要信息库。引经据典，古为今用，更好的为我国经济社会服务。可以说档案有力的推动了我们中华民族文明前进步伐的同时，在人类发展史中也发挥了极其重要的作用。  
    **1.档案的历史渊源**  
    档案是人类生存过程中直接形成的历史记录，在现了历史真实面貌的原始文献，具有历史的再现性、知识性、政治性、文化性、社会性、教育性和价值性等特点。  
   **2.档案工作的重要性**  
    档案具有历史再现性，形式多样的档案才具有查考价值。档案是人类记忆和把握事物发展规律的关键所在，档案的存在是人类发展史上的一项无形的宝贵财富，因此档案管理工作是维持历史面貌的重要事业，使瞬间变为永恒，为我们研究历史现象，准确掌握历史发展规律，服务服务社会发展提供了坚实的基础。做好档案工作是一个社会的、国家健康发展的需求，档案管理是每一个单位管理工作重要的一部分是提高单位工作质量和效率的重要条件，是对历史的真实记录，为促进科学发展提供了第一手资料，是进行科学管理，制定发展的好教材，为科学发展奠定了坚实基础。  
    **3.档案的价值**  
    从发展的角度出发，档案的社会价值就是对社会发展和人类生活的利用价值，是档案能过满足社会需求的重要表现所在，档案是历史的记录，是最原始、最真实的资料，档案能够发挥其作用，就充分体现档案的自身价值，也就是说档案的作用就是档案的价值。档案的作用是多方面的，但最主要的是可以概括为两个基本方面，即档案的凭证作用和档案的参考作用。  
档案工作既是一项基础性工作又是一项服务性工作，我们要充分认识档案的重要性和价值，在工作中要不断创新和完善档案管理工作制度，加强档案管理工作，使档案工作更好的服务于社会经济发展。

**用户视角下高校档案利用需求分析**

对于高校档案管理部门来说， 档案利用是档案工作最终的落脚点， 是体现工作价值的重要证明， 也是塑造良好形象， 提高师生归属感有效途径。当前， 高校内部管理的便利化、师生社会生活的增多以及教学活动的多元化等因素给档案利用与服务的开发提出了更高的要求。长期以来， 高校档案管理部门都采取着自上而下的档案利用开发对策， 存在着档案利用流程不科学、与师生需求之后、档案信息资源开发不彻底等诸多多问题。当下， 只有精准的识别用户的档案利用需求并开发与之相符的档案利用形式， 才能更好的服务师生， 提高档案利用与服务水平， 推动高校档案工作高质量发展。对此高校档案管理部门需要采取主动化的大服务， 主动把握用户对档案馆利用的需求。

企业档案是指企业在各项生产、 经营活动中形成的对国家、 社会和本企业具有保存价值的各种文字、 图表、 声像等不同形式的历史记录。 做好档案管理工作一个企业健康发展的需要， 档案管理工作是企业管理工作的一部分， 是提高企业工作质量和工作效率的必要条件，是维护历史真实面貌的一项重要工作。 科学规范的管理档案， 是衡量一个企业业绩与管理水平的重要尺度。 企业档案记载着这个企业发展史上的优秀成果， 对研究本企业的经营业绩和科学发展提供了第一手资料， 是进行科学分析， 扬长避短， 制定发展方向的好教材。 档案管理工作做好了， 一方面为企业高层管理人员及时了解企业整体经营状况， 适时调整经营策略提供准确依据， 为经营决策提供支持性证据；另一方面有利于有关各方准确认定企业经营成果， 为企业与各有关方面进行有益合作奠定坚实的基础。

做好档案管理工作， 不断地更新档案管理观念， 勇敢探索和尝试新的档案管理手段， 以全面、 真实地反映企业整体发展状况和经营成果。 档案管理成果同企业经营管理的有机结合决定了该企业资源配置的取向和模式， 对于实现该企业经营战略， 不断提高管理效率具有深远的影响。 因此， 做好档案管理工作对于不断提升企业在市场经济中竞争力具有重要意义。根据世界标准物业管理企业的管理模式和实际情况， 档案管理的归档内容划分为 11 个一级类目包含党群管理工作、 行政管理工作、 经营管理工作、 物业管理工等工作形成的文件资料。 物业管理企业档案管理工作应当坚持“及时归档、 合理分类、 规范整理、 安全保管、 方便利用” 的原则。 物业管理企业退出项目时要按照国务院《物业管理条例》、《天津市物业管理条例》 和《天津市物业管理企业退出项目管理暂行办法》 的规定要求， 将档案资料整理完毕后制作移交目录， 在规定时间内认真做好交接工作。

一、 科学规范的管理档案， 是衡量一个企业业绩与管理水平的重要尺度

一是规范化。 档案实行集中管理后， 统一印制档案装具， 统一进行人员培训， 统一整理方法， 统一验收标准， 有力地保证了案卷质量。 对文件借阅、 复印、 转出等环节都分别进行了登记造册进行控制， 切实做到了管理规范化， 为以后工作的顺利开展奠定了坚实的基础。

二是信息化。 为了提高档案管理效果和工作效率， 档案室利用津科档

案信息化管理软件， 为推进档案管理信息化建设创造了先决条件。 我们应用软件对文书档案实行文件集录入， 对业主档案实行案卷级录入， 对建筑类实行文件级和案卷级两级录入， 形成了纸质档案和电子档案并存共用的管理机制。 同时， 建立科学的检索方式， 实现了档案工作信息化管理， 使“死” 档案变成了“活” 信息， 切实强化了管理效果。

三是安全化。 档案实行集中管理后， 硬件条件要比原来基层管理要好得多， “十防” 工作也落实到了实处， 档案管理的安全系数很高。 更重要的是通过建立档案查阅监督机制， 严把了档案查阅关。 在档案查阅这个环节上， 不允许任何个人和本局与档案业务无关的人员查阅档案内容， 是在档案员的监督下进行。 由于管理机制的进一步科学化和规范化， 档案的安全性、 完整性和保密性得到了有效保证。

**用户视角下高校档案利用需求分析**

* 一、高校档案用户的需求
* 1、全面性
* 全面性主要指档案资源的全面性。随着我国基础通信设施的不断完善和各领域信息化建设的快速推进， 人们对于信息资源的使用习惯和使用需求也发生了较大的改变。在传统档案利用模式下， 用户的查询和检索所获取的档案信息十分精准但信息量也较少， 当如今， 人们的信息接受能力已经大幅度提升， 对于高校教师和学生这一高素质群体来说更是如此。用户往往希望通过较为简捷的操作就获取更加全面的档案信息。用户通过档案了解一个事件， 往往希望了解事件的整个过程及其影响，直接相关的档案信息能构建一个较为完整的事件框架， 但在细节方面的记录可能有所欠缺， 这对用户全面了解这一信息造成了阻碍。如教师在查询教学档案时， 希望通过可视化的界面更为直观的了解到相关信息。学生希望查询自己的活动参与情况、在校获奖证明等等。这些都要求高档案管理部门改变信息资源开发、组织和分布的状况， 从而更好地满足用户获取信息的需求。
* 2、多样性
* 用户群体的广泛性对档案信具有多样性的特征。对于一般的档案管理部门来说， 用户年龄、职业、认知背景、学历、目 的的不同都会对档案信息的内容提出不同的要求。对于高校师生这一特定的用户群体来说， 用户特征趋于相似， 用户需求也在一定时期内较为单一， 多以教学档案、财会档案和行政当纳的利用为主。但随着师生以及社会档案利用意识的不断提高以及高校人性化服务的发展， 高校档案利用需求也呈现出多样性的特征。如残疾学生对档案形式的特殊需求； 教师对档案学术价值的要求； 普通用户无目 的性或对档案信息的休闲功能的要求。可以预见到的是， 随着高校档案信息化程度的不断加深， 用户获取档案信息会更为便捷， 在利用效率提高的推动下， 用户的档案利用需求也会区域多样化。息提出了不同的要求， 需求也会随之不一样

3、时效性

* 在互联网时代， 信息的时效性是衡量信息价值的重要依据之一， 随着用户信息获取和使用习惯的改变， 其对用户信息的实践也提出了更高的要求， 希望准确、及时、高校的获取信息。档案作为宝贵的信息资源， 其对时效性的要求就更为突出。与一般档案的使用不同， 高校档案利用本身就具有十分明显的周期性。一般来说， 受到学生就业、考研和学校的人事招聘等事项的影响， 6、 9、 12这三个月 份的档案利用量较多。如在6月 份，学生在签订就业协议和申请出国时， 需要提供本人的学籍卡、成绩单等档案， 对时效性有着较高的要求。另一方面， 高校档案的利用还与高校政策及建设紧密相关， 如高校校园建设、学位评估等， 会使高校基建档案、教学档案、行政档案等需求量陡然增加。在这种背景下， 档案的时效性以及查询效率就更为重要，直接关系着高校自身的发展。
* 二、高校档案利用工作中存在的不足
* 1、档案收集与归档工作有待完善档案信息资源是档案利用的基础和价值所在， 上文的分析中可以看到， 当前档案利用需求呈现出全面性和多样性的特征， 这样给档案管理部门的档案收集工作提出了更高的要求。但从当前高校档案的收集与归档工作来看， 还存在着内容单一， 种类偏少的问题。笔者通过对多所高校的档案门户网站进行调查发现， 大多高校档案关咯部门缺乏专门档案的分类办法， 一般根据《教学档案实体分类办法》开展档案收集和归档工作， 难免存在局限性。而随着档案资源与种类的不断增多， 滞后的分类办法会限制档案内容的丰富性， 仅能较为客观的展示档案信息， 这与档案利用需求的多样性和全面性是矛盾的。另一方面， 部分高校的档案收集工作效率较低， 仅以档案管理部门为主体进行开展， 没有让用户参与进来， 导致档案信息资源与用户需求产生落差。
* 2、档案利用与服务的知晓度低
* 上文的分析中可以看到， 高校档案利用呈现出较强的波动性， 通常集中在6、 9、 12月 ， 同时受到高校政策及建设影响， 但在其他月 份， 档案利用率就呈现出明显的下滑。出教学、考研、出国、就业外， 其他类型的档案利用还较少， 这一定程度上表明了高校面向的用户档案利用意识还较为薄弱， 这一方面是用户缺乏主动性， 另一方面也是由档案管理部门宣传工作不到位导致的。在用户需求多样性和全面性的背景下， 多数用户表现出有利用档案的意愿以及获取档案信息的渴望。但当前， 大多数的高校档案利用宣传基本以门户网站或者线下的宣传栏为主要方式， 面向的是本身已经使用过档案服务的人， 缺乏主动性和针对性， 没有开发潜在用户。
* 3、档案人才队伍建设有待加强
* 相对于专门的档案管理机构， 高校档案馆的正式人员编制通常较少， 多数高校仅有4-6名在编专职人员。而随着档案利用需求全面性、多样性和时效性的逐渐凸显， 档案处理量和复杂程度都会成倍增长， 对于服务效率的要求也会不断提高。另外，信息化建设加快， 为满足广大用户对数字化学生档案的利用。
* 4、用户反馈机制不健全
* 一般来说， 为提高档案服务质量， 高校档案馆会对利用者的信息以及利用内容进行登记， 但缺乏后续的跟踪和回访工作， 对于用户的利用结果也并不关心。从用户需求的角度来说，完善的用户反馈机制是推动档案利用服务创新与优化的重中之重。大部分高校对用户使用情况的记录主要是从档案馆的角度对档案利用结果的登记， 而非从用户角度对利用效果或者满意度的登记。用户反馈有助于档案馆了解工作不足， 因此， 反馈环节应被视为档案利用的最后一个流程加以规范。

**区块链的五个基本特征**

区块链是分布式数据存储，点对点传输，共识机制，加密算法等计算机技术在互联网时代的创新应用模式。虽然不同报告中对区块链的介绍措辞不尽相同，但“去中心化、开放性、自治性、信息不可篡改和匿名性”这五个基本特征得到了共识性。

1．去中心化

所谓去中心化，是指由于区块链使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。

2．开放性

所谓开放性，是指区块链系统是开放的，除了对交易各方的私有信息进行加密，区块链数据对所有人公开，任何人都能通过公开的接口，对区块链数据进行查询，并能开发相关应用，整个系统的信息高度透明。

3．自治性

区块链的自治性特征建立在规范和协议的基础上。区块链采用基于协商一致的规范和协议（如公开透明的算法），使系统中的所有节点都能在去信任的环境中自由安全地交换数据，让对“人”的信任改成对机器的信任，任何人为的干预都无法发挥作用。

4．信息不可篡改

所谓信息不可篡改，即一旦信息经过验证并添加到区块链，就会被永久地存储起来，除非同时控制系统中超过51%的节点，否则单个节点上对数据库的修改是无效的。正因为此，区块链数据的稳定性和可靠性都非常高，区块链技术从根本上改变了中心化的信用创建方式，通过数学原理而非中心化信用机构来低成本地建立信用，出生证、房产证、婚姻证等都可以在区块链上进行公证，拥有全球性的中心节点，变成全球都信任的东西。

5．匿名性

所谓匿名性，是指节点之间的交换遵循固定算法，其数据交互是无须信任的，交易对手不用通过公开身份的方式让对方对自己产生信任，有利于信用的累计。

**区块链技术对电子档案归档的应用探究**

随着移动网络的发展和Web2.0技术的广泛运用，社交媒体在全球范围内得到了空前发展，也带来了社交媒体信息量的指数级增长，这些类型多样、数量庞大的信息中蕴含着巨大的情报价值和凭证价值，有必要对其进行归档保存以提供长久利用。目前，受制于政策、理念以及技术等因素，社交媒体信息归档的可行性方案仍然处于探索阶段，相应的理论仍有待形成，仅美国、英国、澳大利亚等西方发达国家制定了相关政策且付诸实践。2009年，比特币诞生并获得成功，经过近几年的发展，其底层技术——区块链技术已经被广泛应用于金融、法律、保险、房地产等领域。2016 年，我国国务院印发了《“十三五”国家信息化规划》，正式将“区块链技术”纳入国家规划。2017年，国家档案局将“区块链技术在电子档案管理中的应用”列入科技立项选题，区块链技术正式进入档案界视野。本文以区块链作为技术突破口，为社交媒体信息归档中的实际困难提供一种可行性解决思路。

**相关概念界定**

**1.区块链技术**

区块链技术，简称BT(Blockchain technology)，也被称为分布式账本技术，是一种互联网数据库技术，其特点是去中心化、公开透明，让每个人均可参与数据库记录。2015年，区块链脱离了对比特币的依附，被公认为是全新的独立技术，可以被广泛应用于社会经济和生活等不同场景。经过近年来的快速发展与演变，区块链技术已经形成了5大技术特征，包括分布式(Decentralized)、免信任(Trustless)、时间戳(Time Stamp)、非对称加密 (Asymmetric Cryptography)和智能合约(Smart Contract)。

**2.社交媒体信息**

社交媒体(Social Media)指互联网上基于用户关系的内容生产与交换平台。社交媒体是人们彼此之间用来分享意见、见解、经验和观点的工具和平台，现阶段主要包括社交网站、微博、微信、博客、论坛、播客等。顾名思义，社交媒体信息是国家机构、社会组织或个人在社交媒体平台上形成的各种形式的记录。社交媒体信息具有类型复杂、质量参差不齐、信息发布随意、个性化、碎片式、互动性、社会性等特点，因此对社交媒体信息进行归档保存存在诸多困难。

**社交媒体信息归档难点**

当前，部分西方国家的政府机构或档案馆已经开始社交媒体信息归档工作，而且已经形成了完整的管理制度与操作流程，比较有代表性是的美国、英国和澳大利亚，归档信息类型主要是政务社交媒体信息。相较之下，我国在社交媒体信息归档方面的意识、政策、技术与实践等方面都处于起步阶段，尚未建立完整的模型，与西方国家还存在很大差距。纵观国内外社交媒体信息归档现状，虽已具备一定的理论研究与实践积累，但在社交媒体信息的采集、鉴定、组织、保存等环节仍然存在一些难点。

1. **档案化鉴定问题**

社交媒体信息档案化鉴定是指对社交媒体信息的价值和真伪进行判定，其目的是挑选并保存有价值的社交媒体信息，构建留存社会记忆。鉴定分为价值鉴定和真伪鉴定，目前后者是社交媒体信息档案化的主要难点。真伪鉴定是对社交媒体信息的真实性进行鉴别，难点在于鉴定的对象是社交媒体平台上海量性、碎片化的网络信息。社交媒体的低门槛特征使网民由被动的信息受众转变为信息制作和传播主体，可以随时随地发表所观所想。《2017微信数据报告》显示，微信日登录用户9.02 亿人，日发送消息380亿次，朋友圈日发表视频6800万次。社交媒体信息指数型增长的同时，信息带有鲜明的个人色彩，具有较强的随意性。部分用户为了提高自身关注度，肆意制造和转发虚假信息，使得社交媒体平台上充斥了大量的不实信息。另一方面，由于现有的法律及社交媒体平台对信息发布管控的缺失，无法从源头上解决社交媒体信息的真实性问题。有学者认为，在社交媒体信息归档过程中，应该弱化信息的真实性问题，但“弱化”并不意味着“取消”，真实可信的信息作为档案保存构成了有效的社会记忆，对社会发展起到支持作用。

**2.采集的完整性问题**

社交媒体信息采集应遵循全面性和整体性原则。全面性原则是指有价值的信息都应该妥善保存，社交媒体信息是碎片化的，单个的信息记录往往无法体现自身价值，只有尽可能多地将碎片信息汇集起来才能发挥效用；整体性原则是指将同一主题的信息尽可能保存，只要是同一主题或事件的信息，包括发布、转发、评论或其他格式信息都应尽可能地收集。此外，元数据是社交媒体档案的重要组成部分，有助于社交媒体档案的长期管理，缺少元数据的社交媒体档案是不完整的，应对元数据进行采集归档。目前，英国的社交媒体信息归档政策规定，归档内容仅限于机构自身在第三方社交媒体平台上发布的原创信息。而美国、澳大利亚等国家则指出，要关注用户的评论互动信息，例如澳大利亚政府机构规定，保存转发的内容，需要经过原创发布者的同意，归档转发内容的元数据也需要遵守相关书面协定。可见，即使在实践先行的西方发达国家，由于版权保护和技术的限制，采集的社交媒体信息也具有很大的局限性。

**3.归档中的个人隐私问题**

公民个人在社交媒体平台上发布的信息内容偏向生活，个性化和私密性特征明显。社交媒体平台的开放性和即时性决定了用户既是信息制作的主体，也是信息发布的主体。目前，个人用户的隐私保护意识普遍薄弱，大多数用户在通过社交媒体平台表达心情的同时，也泄露了真实姓名、手机号码、家庭成员、家庭住址等个人信息，人们无从知道这些数据未来会流向哪里、被如何利用。美国国会图书馆（LC）认为，除了公共信息、热点事件以外，人们忽视了日常生活信息的重要性，这类信息自带社会记忆属性，具有很高的研究价值，因此作为日常生活信息的集中反应，个人社交媒体信息需要得到妥善保存。目前，我国档案部门尚未制定统一的标准来对社交媒体平台上形成的日常生活信息进行管理，如何鉴定哪些个人发布的信息属于档案、在利用过程中如何避免侵犯个人隐私等问题都未得到解决。因此，在对社交媒体信息进行归档保存的过程中，需要从法律、技术的角度，权衡好维护社会整体记忆与保护用户个人隐私之间的关系。

**4.保存的安全性问题**

社交媒体档案保存的安全隐患存在于档案形成前和形成后两个阶段，形成前的状态是社交媒体信息，存储在运营商的服务器中；档案形成后通常保存在归档机构的数据库中，目前国外主流的归档主体有政府机构、国家图书馆、国家档案馆、第三方记忆机构等。档案形成前的安全性问题体现在我国网络信息安全保管规范的缺失，没有建立信息失存与失范的管理机制，在网络运营方出于一定目的对服务器中的信息进行修改、删除等操作后，信息资产面临失真甚至流失的风险。国外社交媒体信息的档案保存机构各不相同，比较有代表性的是，英国档案馆负责社交媒体档案的收集、组织、归档、维护与长久保管并提供利用，建立了社交媒体档案库；澳大利亚由各个政府机构形成者负责社交媒体文件的捕获与管理，属于政府整体框架下的分布式管理模式；美国是在各联邦政府机构归档后再移交给美国档案与文件署（NARA）。可见，除了澳大利亚，其他大部分西方发达国家都采取集中保存的模式。这种中心化的数据库存在巨大的风险，无论是数据库本身遭到破坏，还是中心数据库和外部中断的通信出现问题，都会导致数据库不能发挥作用。同时，火灾、地震等不确定因素也会对中心化数据库造成潜在威胁。

**基于区块链技术的社交媒体信息归档**

一项新技术最终能否实施并得到普及，由诸多因素决定，最关键的一点就是该技术是否具有适宜的应用环境。区块链技术自发展以来已被应用于诸多领域，通过分析其在社交媒体信息归档方面的适用性，以期解决社交媒体信息归档的几大困境。

**1.对社交媒体信息归档的适用性**

“去中心化”是区块链技术和社交媒体信息的共同特性。作为新兴的信息技术，区块链使用时间戳和数字密码技术，把交易记录记载在数据块中，这些数据块是按时间序列组成的，并使用共识机制把数据存储到分布式数据库内，生成的数据记录是唯一的、永久保存的、不可逆向篡改的，因此在不依靠任何中心机构的情况下就可实现可信的交易。这种分布式数据存储结构决定了区块链技术是去中心化的。同时，社交媒体在技术底层就是按照去中心化的模式进行设计和运作的，每个个体都是一个节点，每个节点都能建立连接，每个节点都可以参与表达，输出影响力。传统的社会大众媒体，包括报纸、广播、电视等，内容由专业媒体机构全权负责，话语权掌握在少数人手中，这些专业媒体机构成为一个个信息中心。社交媒体是由普通大众主导的信息传播活动，一种由传统的“点到面”转化为“点到点”的对等传播，普通用户能够借助平台自由发声，打破了少数机构垄断信息的格局。由于区块链技术与社交媒体信息都有“去中心化”的特征，为区块链技术在社交媒体信息归档方面提供了天然的应用优势，在此基础上，将区块链技术运用于社交媒体信息归档，有助于推动档案管理模式的变革。

**2.解决社交媒体信息归档难题**

区块链技术不是一个单项技术，而是一个集成了多方面研究成果的综合性技术系统。区块链技术的基础架构由数据层、网络层、共识层、激励层、合约层和应用层组成。其中，数据层封装数据区块、链式结构、时间戳、非对称加密等技术；网络层封装数据传播机制、P2P网络、数据验证机制等；共识层主要包括网络节点的各类共识算法；激励层封装了经济激励的分配机制和发行机制，从而将经济因素集成到区块链技术体系中来；合约层是区块链可编程的基础层，包括各类脚本代码、算法机制和智能合约；应用层则封装区块链技术的各种应用场景，包括政府部门、金融机构、科技企业和资本市场等。区块链技术具有普适性的底层技术框架，其时间戳、动态的整体数据链、非对称加密算法、分布式数据库等特性都能够为众多领域带来深刻变革。

**(1)时间戳解决档案真实性问题**

区块链是由无数个区块首尾相接组成的数据链，每个区块在生成时都会自动加盖一个时间戳，时间戳可以作为存在性证明(Proof of existence)的关键参数，能够证实特定数据必然在某特定时刻是的确存在的。利用区块链的时间戳特性，能够解决社交媒体信息归档在信息溯源和信息防伪方面的难题。

第一，时间戳特性有助于鉴别社交媒体信息的真实性和所有权归属。社交媒体平台的交互性使得用户可以任意捏造、修改和转发信息，一条信息经过多次删改和转发后，往往难以判别信息归谁所有、是否真实。区块链上的每个用户在发布一条原创信息时都会自动加盖时间戳，并且其他用户的每一次转发、修改等操作也都被记录在数据链中，形成了以时间为序列的信息数据链，鉴定工作者可在数据链中抽丝剥茧、追本溯源，找到最初发布的原创内容及其所有者，形成真实、完整的社交媒体档案。

第二，时间戳特性能够保证社交媒体档案在保存后不可篡改和伪造，提高档案信息数据的稳定性。社交媒体档案属于电子档案的范畴，不同于纸质档案，电子档案可被轻易篡改。而时间戳特性决定了区块链的开放性、透明性，就好像多联复写的发票或收据，修改或者销毁单张数据都无法改变其他单据的数据记录。也就是说，每一个社交媒体信息区块都处于全网的监控与审查之中，篡改区块链上的数据及操作记录将耗费难以想象的成本。

**(2)动态的整体数据链解决采集完整性问题**

区块链是一种把区块以链的方式组合在一起的数据结构，每一个区块的前端都包含了前一个区块的交易信息压缩值，形成了区块与区块前后相接的一条长链。这种所有区块包含前一个区块的引用结构，让现存的区块集合形成了一个动态的整体数据链（如图1所示）。

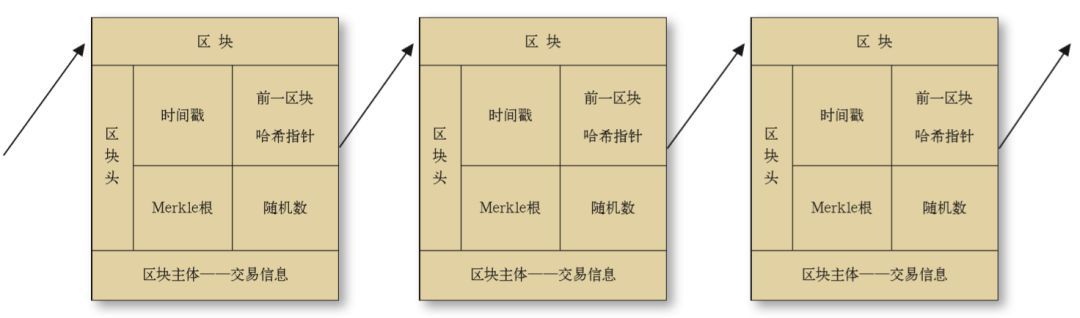


图1 区块链结构示意图

毫无疑问，社交媒体平台上的发布内容本身就是数据价值最高的部分，而转发、评论、点赞、收藏等信息也从不同侧面反映了原内容的某种属性，具备一定的凭证价值。区块链技术将发布的内容连同元数据动态地融合成一个完整的数据实体，每一个数据实体都可以被看成是区块链中的一个创始区块，包括创建者、发布日期、地理数据等字段都被存储在该区块中，而围绕这条信息产生的互动性操作就产生了其他区块，按照时间序列排列在创始块之后，形成一条单向的、不可逆的完整数据链。因此，在采集过程中，以区块为信息采集的基本单位，能够解决社交媒体信息采集过程中的元数据、操作数据与发布信息数据分离的问题，从技术上解决了社交媒体信息采集的完整性问题。

**(3)非对称加密算法解决用户个人隐私问题**

非对称加密是一种新的密钥交换协议，允许在不安全网络上的通信双方交换信息，解决了信息公开传送和密钥管理问题。非对称加密通过公钥和私钥两个不同的密钥来进行加密和解密，如果用公钥对数据进行加密，只有对应的私钥才能解密；如果用私钥进行数据签名，只有公钥可以来验签。

社交媒体平台上蕴含着大量的个人日常生活信息，构成了社会记忆的重要组成部分，有必要对其进行归档保存。然而，用户发布的一条信息记录中可能包含多个不同的主题，在归档过程中难免会将涉及个人隐私的信息纳入归档范围，为日后的档案利用埋下了侵犯个人隐私的隐患。非对称加密算法能够有效解决这一问题，使用公钥和私钥对区块链中档案数据进行加密和解密，归档主体如档案馆、图书馆等掌握档案库的公钥，信息所有者即社交媒体用户掌握私钥。归档主体使用公钥对区块链上的每条档案数据进行加密，只有掌握私钥的信息所有者才可以进行解密。同样，信息所有者也可用私钥对自己的信息进行加密，只有掌握公钥的归档主体才能验签查看。通过区块链的非对称加密，允许用户在自己的设备上运行节点接入网络，节点与节点之间实时互连，用户信息以加密的形式存储在网络节点上，形成一个分布云，只有掌握了秘钥的人才能查看数据。因此，在机构或个人发送查档需求时，可以使用私钥来验证身份，如果查档主体所持私钥不能解密档案数据，说明其对该数据不具备查档权限（如图2所示）。

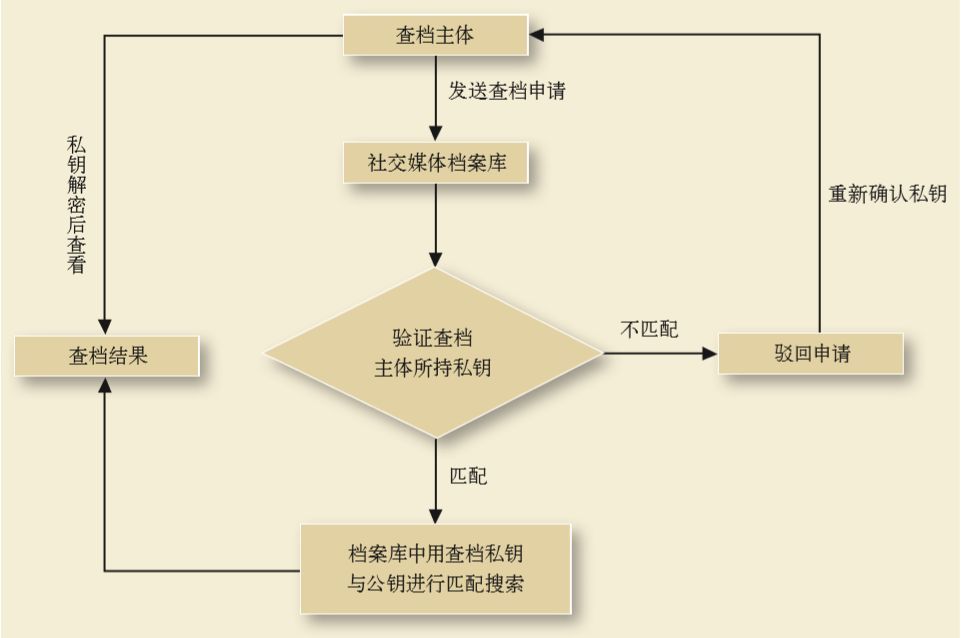


图2 基于区块链技术的社交媒体档案查询流程图

**(4)分布式数据库解决档案保存安全性问题**

从本质上来说，区块链技术是一种链式存取数据技术，通过网络中多个参与计算的节点来共同参与数据的计算和记录，并且互相验证其信息的有效性。去中心化数据库安全且便捷，所以区块链技术被认为是对现有互联网技术的升级与补充。

区块链的分布式特性能够解决档案保存的安全性问题，主要体现在两个方面：第一，分布式账本能够降低信息资产流失的风险。区块链的分布式账本是把全部记录分布式地保存在整个网络的多个记账节点上，每个节点的账本数据都是一模一样的，也就意味着单个节点的数据篡改是没有任何意义的。如果系统发现两个账本对不上，它就认为拥有相同账本数量较多节点的版本才是真实的账本数据，那些少部分不一致的节点账本不是真实的，而是被篡改过的数据账本。简单来说，单个节点的数据错误或篡改不会对整体数据产生破坏性影响。因此，社交媒体运营商即使删改了服务器中的数据，区块链中的其他节点依然能够保存完整的信息记录。第二，分布式数据库能够大力提升档案基础设施防护水平。目前，档案管理机构的信息管理系统和数据库都是基于中心化网络建立的，一旦中心服务器受到攻击，就可能会导致整个系统的瘫痪。运用分布式数据库技术，建立一个社交媒体档案信息智能交互系统，将档案信息数据分布式地存储在系统的各个节点上，由所有节点共同维护。这样，即使某一个节点上的数据受损，也不会导致全部档案信息数据的丢失。

《全国档案事业发展“十三五”规划》将制定社交媒体文件的归档管理办法列为核心工作之一。目前，国内外都在积极致力于推进社交媒体信息归档的理论与实践研究。区块链这一新兴技术已经被广泛运用于多个领域，然而，社交媒体信息归档是一项工作量巨大、流程复杂、技术要求高的系统性工程，还需要档案部门、运营商和第三方的共同合作，从制度、资金、技术等方面来保障这项创新性工作的稳步推进。

**基于区块链的电子档案及其流转的展望**

* 当事人对档案的重视性不足，不到用到是不会去接触。更对档案内的文件影响不深。
* 假设缺少文件，就会变成一件麻烦事。又如果知道档案缺少什么文件，则可以提前做准备。
* 2.档案管理复杂。不同的人来自不同的地方，又去向不同的地方。往往出现丢失，改等问题。基于区块链的电子档案及其流转可以防篡改，防丢失。
* 3.根据相关文件规定，转递档案须通过机要交通或派专人送取，严禁个人自带档案转递。因此，毕业生档案应由学校通过机要交通（包括EMS标准快递）或派专人转递，严禁毕业生个人自带档案转递。电子传递则省时省力。
* 4.档案查询较麻烦，需本人携带证件到机构查询。电子查询方便快捷。
* 5.特定行业档案管理费用居高不下。其市场较高。

基于区块链的不可篡改性档案一旦输入则永远为真，记录在世，则便于流转，降低的流转成本与丢失风险；

* 基于区块链的信息化档案成为数据流，便于随时随地查看，验证，同时便于档案拥有者反应情况，实现互通，降低了储存成本与维护成本

# blockDocumentManagement

### 需求设计

##### 传统模式

某组织对档案进行管理，此时所有权在个人，使用权在管理人员。管理员可以在个人不知情的情况下对文档进行修改，或在个人授意下进行修改。由于档案的在一般情况下具有唯一性，所以管理员的操作对个人档案的影响具有非常大作用。

个人对文档进行转移是不允许的，是由组织进行统一转移的，但发生文档丢失或损毁的情况，后果又是十分严重的。

##### 区块链模式下

当文档需要进行操作时，必须由个人同意，在个人账户上操作生成独一无二的erc721的代币，无论是修改还是增加，都必须在个人账户上操作生成，并且生成的erc721地址必须公布，或上报与上级。之后在进行其他操作

### 合约核心代码

$("#Btn\_CreatItem").click(function () {

console.log("Btn\_CreatItem");

$("#load\_ci\_img").show();

let \_txt = $("#prodid").val()

// console.log($("#arraytxt").val().length)

if (\_txt.length < 3) {

alert("长度不能小于3")

} else {

contract.methods.CreatItem(\_txt).send({ from: accounts[0], value: 0.02 \* Math.pow(10, 18) }).then(

function (result) {

console.log("result", result);

if (result.status) {

$(".txt\_CreatItem").html("添加成功")

getBalance();

} else {

hide

$(".txt\_CreatItem").html("添加失败")

}

$("#load\_ci\_img").hide();

}

)

}

}

)

### 术语与缩写解释

Blockchain 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。是一个共享的分布式账本，其中交易通过附加块永久记录。

Block 在比特币网络中，数据会以文件的形式被永久记录，我们称这些文件为区块。一个区块是一些或所有最新比特币交易的记录集，且未被其他先前的区块记录。

区块头 区块头里面存储着区块的头信息，包含上一个区块的哈希值（PreHash），本区块体的哈希值（Hash），以及时间戳（TimeStamp）等等。

中本聪 自称日裔美国人，日本媒体常译为中本哲史，此人是比特币协议及其相关软件Bitcoin-Qt的创造者，但真实身份未知。

加密货币 加密货币是数字货币（或称虚拟货币）的一种。是一种使用密码学原理来确保交易安全及控制交易单位创造的交易媒介。

Node 由区块链网络的参与者操作的分类帐的副本。

Oracles Oracle通过向智能合约提供数据，它现实世界和区块链之间的桥梁

去中心化 去中心化是一种现象或结构，必须在拥有众多节点的系统中或在拥有众多个体的群中才能出现或存在。节点与节点之间的影响，会通过网络而形成非线性因果关系。

共识机制 共识机制是通过特殊节点的投票，在很短的时间内完成对交易的验证和确认；对一笔交易，如果利益不相干的若干个节点能够达成共识，我们就可以认为全网对此也能够达成共识。

POW Proofof Work，是指获得多少货币，取决于你挖矿贡献的工作量，电脑性能越好，分给你的矿就会越多。

POS Proofof Stake，根据你持有货币的量和时间进行利息分配的制度，在POS模式下，你的“挖矿”收益正比于你的币龄，而与电脑的计算性能无关。

智能合约 智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

时间戳 时间戳是指字符串或编码信息用于辨识记录下来的时间日期。国际标准为ISO 8601。

图灵完备 图灵完成是指机器执行任何其他可编程计算机能够执行计算的能力。一个例子是Ethereum虚拟机(EVM)。

51%攻击 当一个单一个体或者一个组超过一半的计算能力时，这个个体或组就可以控制整个加密货币网络，如果他们有一些恶意的想法，他们就有可能发出一些冲突的交易来损坏整个网络。

Dapp 是一种开源的应用程序，自动运行，将其数据存储在区块链上，以密码令牌的形式激励，并以显示有价值证明的协议进行操作。

DAO 可以认为是在没有任何人为干预的情况下运行的公司，并将一切形式的控制交给一套不可破坏的业务规则。

DistributedLedger 数据通过分布式节点网络进行存储。分布式账本不是必须具有自己的货币，它可能会被许可和私有。

DistributedNetwork 处理能力和数据分布在节点上而不是拥有集中式数据中心的一种网络。

预言机 预言机是一种可信任的实体，它通过签名引入关于外部世界状态的信息，从而允许确定的智能合约对不确定的外部世界作出反应。预言机具有不可篡改、服务稳定、可审计等特点，并具有经济激励机制以保证运行的动力。

零知识证明 零知识证明由S.Goldwasser、S.Micali及C.Rackoff在20世纪80年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

PrivateKey 私钥是一串数据，它是允许您访问特定钱包中的令牌。它们作为密码，除了地址的所有者之外，都被隐藏。

PublicKey 是和私钥成对出现的，公钥可以算出币的地址，因此可以作为拥有这个币地址的凭证。

AES 密码学中的高级加密标准(Advanced Encryption Standard，AES)，又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。

Wallet 一个包含私钥的文件。 它通常包含一个软件客户端，允许访问查看和创建钱包所设计的特定块链的交易。

冷钱包 通俗来说冷钱包就是将数字货币进行离线下储存的钱包，玩家在一台离线的钱包上面生成数字货币地址和私钥，再将其保存起来。而冷钱包是在不需要任何网络的情况下进行数字货币的储存，因此黑客是无法进入钱包获得私钥的。

SPV 轻钱包依赖比特币网络上其他全节点，仅同步与自己相关的数据，基本可以实现去中心化。

全节点 全节点是拥有完整区块链账本的节点，全节点需要占用内存同步所有的区块链数据，能够独立校验区块链上的所有交易并实时更新数据，主要负责区块链的交易的广播和验证。

Byzantinefailures 拜占庭将军问题是由莱斯利·兰伯特提出的点对点通信中的基本问题。含义是在存在消息丢失的不可靠信道上试图通过消息传递的方式达到一致性是不可能的。因此对一致性的研究一般假设信道是可靠的，或不存在本问题。

超级账本 超级账本（hyperledger）是Linux基金会于2015年发起的推进区块链数字技术和交易验证的开源项目。通过创建通用的分布式账本技术，协助组织扩展、建立行业专属应用程序、平台和硬件系统来支持成员各自的交易业务。

闪电网络 闪电网络的目的是实现安全地进行链下交易，其本质上是使用了哈希时间锁定智能合约来安全地进行0确认交易的一种机制，通过设置巧妙的“智能合约”，使得用户在闪电网络上进行未确认的交易和黄金一样安全。

P2P 即对等计算机网络，是一种在对等者（Peer）之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。

Mining 挖矿是获取比特币的勘探方式的昵称。利用电脑硬件计算出币的位置并获取的过程称之为挖矿。

矿工 尝试创建区块并将其添加到区块链上的计算设备或者软件。在一个区块链网络中，当一个新的有效区块被创建时，系统一般会自动给予区块创建者（矿工）一定数量的代币，作为奖励。

矿地 是一个全自动的挖矿平台，使得矿工们能够贡献各自的算力一起挖矿以创建区块，获得区块奖励，并根据算力贡献比例分配利润（即矿机接入矿池—提供算力—获得收益）。

公有链 完全开放的区块链，是指任何人都可读取的、任何人都能发送交易且交易能获得有效确认的、全世界的人都可以参与系统维护工作，任何人都可以通过交易或挖矿读取和写入数据。

私有链 写入权限仅面向某个组织或者特定少数对象的区块链。读取权限可以对外开放，或者进行任意程度地限制。

联盟链 共识机制由指定若干机构共同控制的区块链。

主链 主链一词源于主网（mainnet，相对于测试网testnet），即正式上线的、独立的区块链网络。

侧链 楔入式侧链技术（pegged sidechains），它将实现比特币和其他数字资产在多个区块链间的转移，这就意味着用户们在使用他们已有资产的情况下，就可以访问新的加密货币系统。

跨链技术 跨链技术可以理解为连接各区块链的桥梁，其主要应用是实现各区块链之间的原子交易、资产转换、区块链内部信息互通，或解决Oracle的问题等。

硬分叉 区块链发生永久性分歧，在新共识规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会发生。

软分叉 当新共识规则发布后，没有升级的节点会因为不知道新共识规则下，而生产不合法的区块，就会产生临时性分叉。

Hash 一般翻译做"散列"，也有直接音译为"哈希"的。简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。

哈希率 假设挖矿是解一道方程题，而且只有把每个整数代入才能算出来，那么哈希率就是每秒处理数据的速度。

Hashtree 哈希树是一种树形数据结构，每个叶节点均以数据块的哈希作为标签，而非叶节点则以其子节点标签的加密哈希作为标签。

SHA256 SHA-256是比特币一些列数字货币使用的加密算法。然而，它使用了大量的计算能力和处理时间，迫使矿工组建采矿池以获取收益。

Kyc KYC是Know Your Customer的缩写，意思是了解你的客户，在国际《反洗钱法》条例中，要求各组织要对自己的客户作出全面的了解，以预测和发现商业行为中的不合理之处和潜在违法行为

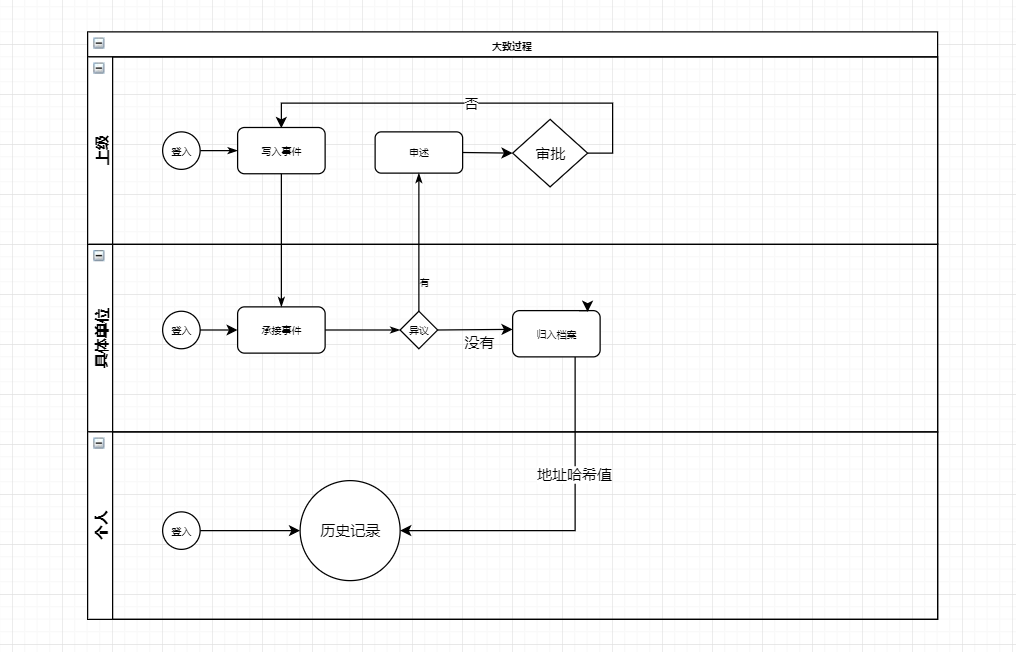
### 总结体会

1 代码书写规范

2 注释书写规范

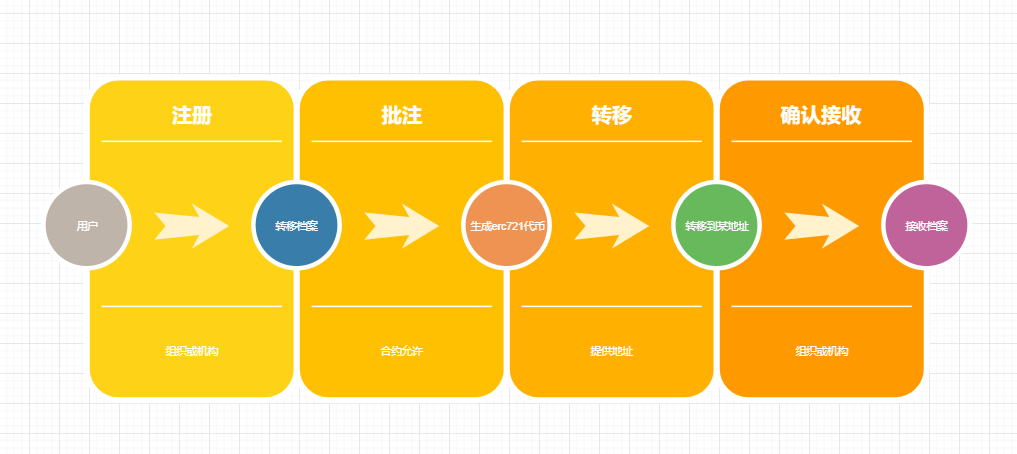
3 命名规范

4逻辑结构要清晰



# 系统分析与设计

## 系统总结结构



## 开发环境的配置

|  |  |  |
| --- | --- | --- |
| 类别 | 标准配置 | 最低配置 |
| 计算机硬件 | 32G内存运行，1T磁盘储存 | 16G内存运行，512G磁盘储存 |
| 软件 | Remix，vcode | Remix，vcode |
| 其它 |  |  |

## 运行环境的配置

|  |  |  |
| --- | --- | --- |
| 类别 | 标准配置 | 最低配置 |
| 计算机硬件 | 16G内存运行，512G磁盘储存 | 4G内存运行，216G磁盘储存 |
| 软件 | Windows，mas，linux | Windows |
| 其它 |  |  |

## 系统功能描述

### 功能汇总

|  |  |
| --- | --- |
| **子系统A** | |
| 模块名称 | 功能简述 |
| *approve* | *批准某个账户转移* |
| *safeTransferFrom* | *转移* |
| *…transferFrom* | *转移* |
| **子系统B** | |
| 模块名称 | 功能简述 |
| *balanceOf* | *查询余额* |
| *ownerOf* | *查询拥有者* |
| *…getApproved* | *查询批准者* |

|  |  |
| --- | --- |
| 模块名称 | **子系统A** |
| 功能描述 | *主要的设置功能* |
| 接口与属性 | **function approve(address to, uint256 tokenId) public {**  **address owner = ownerOf(tokenId);**  **require(to != owner);**  **require(msg.sender == owner || isApprovedForAll(owner, msg.sender));**  **\_tokenApprovals[tokenId] = to;**  **emit Approval(owner, to, tokenId);**  **}**  **function setApprovalForAll(address to, bool approved) public {**  **require(to != msg.sender);**  **\_operatorApprovals[msg.sender][to] = approved;**  **emit ApprovalForAll(msg.sender, to, approved);**  **}**  **function safeTransferFrom(address from, address to, uint256 tokenId) public {**  **safeTransferFrom(from, to, tokenId, "");**  **}**  **function safeTransferFrom(address from, address to, uint256 tokenId, bytes memory \_data) public {**  **transferFrom(from, to, tokenId);**  **require(\_checkOnERC721Received(from, to, tokenId, \_data));**  **}** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 模块名称 | **子系统B** |
| 功能描述 | *服务于个人（组织）查询功能* |
| 接口与属性 | **function balanceOf(address owner) public view returns (uint256) {**  **require(owner != address(0));**  **return \_ownedTokensCount[owner].current();**  **}**  **function ownerOf(uint256 tokenId) public view returns (address) {**  **address owner = \_tokenOwner[tokenId];**  **require(owner != address(0));**  **return owner;**  **}** |
| 补充说明 |  |

|  |  |
| --- | --- |
| 检查项 | 测试人员的类别及其评价 |
| 窗口切换、移动、改变大小时正常吗？ | Y |
| 各种界面元素的文字正确吗？（如标题、提示等） | Y |
| 各种界面元素的状态正确吗？（如有效、无效、选中等状态） | Y |
| 各种界面元素支持键盘操作吗？ | Y |
| 各种界面元素支持鼠标操作吗？ | Y |
| 对话框中的缺省焦点正确吗？ | Y |
| 数据项能正确回显吗？ | Y |
| 对于常用的功能，用户能否不必阅读手册就能使用？ | Y |
| 执行有风险的操作时，有“确认”、“放弃”等提示吗？ | Y |
| 操作顺序合理吗？ | Y |
| 有联机帮助吗？ | Y |
| 各种界面元素的布局合理吗？美观吗？ | Y |
| 各种界面元素的颜色协调吗？ | Y |
| 各种界面元素的形状美观吗？ | Y |
| 字体美观吗？ | Y |
| 图标直观吗？ | Y |
|  |  |
| … |  |
|  |  |
|  |  |
|  |  |

# 系统界面及操作

## 系统访问与登录

* **访问方式一：通过网址直接访问**

在地址栏键入<http://127.0.0.1:8080/> 访问地址http://127.0.0.1:8080/app.html并回车，浏览器中会出现系统登录页面。



## 用户注册

系统用户登录前，首先根据自己所在科室（处室）的职务向经理或副经理（正处或副处）注册申请相应工作管理的岗位职责权限。

用户注册步骤如下：

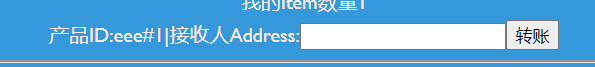
* 打开用户注册对话框

打开系统登录页面，点击“注册”按钮，弹出“用户注册”对话框。

* 提交注册流程

输入用户信息，并选择相应职权后，选择注册审核人，（如果是科员或科长注册，注册审核人为本部门的副处长或处长，如果是处长及以上级别用户注册，注册审核人为系统管理员）点击“提交”后，提示用户注册流程启动。

## 转账查询



## 记录查询

