Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Advanced frameworks for data privacy and ethical considerations in AI-powered library management

Ahmed Sayed M. Metwally [1,*], Yazeed Alhumaidan [2], Saad Alzahrani [2], Mohamed H. Abdelati [3]

[1]*Department of Mathematics, College of Sciences, King Saud University, Riyadh 11451, Saudi Arabia*
[2]*Department of Information Science, College of Humanities and Social Sciences, King Saud University, Riyadh 11451, Saudi Arabia*
[3]*Automotive and Tractor Engineering Department, Minia University, Minia, Egypt*

ARTICLE INFO

Article history:
Received 21 September 2024
Received in revised form
23 March 2025
Accepted 30 April 2025

Keywords:
Library management
Data privacy
Ethical challenges
AI implementation
Blockchain technology

ABSTRACT

Implementing artificial intelligence (AI) and blockchain technology in management systems transforms traditional libraries into advanced information centers that are data-driven and effectively managed. While these technologies enhance efficiency and operational capabilities, they also present two critical challenges: data privacy and ethical concerns. This study examines the role of AI and blockchain in library management, focusing on issues related to data privacy and ethical challenges that arise from their use. It also offers best practices to ensure safe implementation. The research adopts a comprehensive mixed-methods approach, involving qualitative interviews and quantitative surveys to identify these challenges within the system architecture, assess the effectiveness of current designs, and propose a complete framework using privacy-preserving technologies. This framework incorporates innovative cryptographic techniques, including homomorphic encryption, differential privacy, and zero-knowledge proofs, providing a novel model for the ethical use of AI in libraries. The findings indicate that robust data protection, transparency, and accountability are essential to building trust in AI-powered library services.

1. Introduction

The incorporation of sophisticated and innovative technologies like Artificial Intelligence (AI) and Blockchain has changed the library administration scenario fundamentally (Singh, 2024). Until recently, the word “library” suggested a place where books were stored and distributed rather than as a hub for knowledge exchange (MacGregor, 2020). But in the digital age, libraries are transforming into state-of-the-art information centers that use new tech to improve service and streamline operations as well as connect with users. Two technologies in particular, AI and blockchain (among many others that stack both out differently), have found new applications as well through this pivot that offer capabilities far beyond what a library is designed to do. Potential aside, the application of these technologies raises serious issues about privacy and ethical questions that can easily erode trust in users while complying with legal and moral standards (Schöpfel, 2018; Adams, 2024).

AI technology, such as machine learning and natural language processing, and computer vision, etc. have advanced so much over the years that libraries started using this to automate repetitive tasks like cataloging, classification of information retrieval (Jayavadivel et al., 2024; Abdelati et al., 2024). These improvements in efficiency and accuracy help libraries to better serve the needs of their users. For example, AI can process large datasets to deploy personalized recommendations that would support users' better experience and for resource management purposes which streamline workflows. In addition, there are more and more uses of AI-driven chatbots or virtual assistants to answer user questions, providing 24/7 coverage for library services (Meurisch and Mühlhäuser, 2021).

The broad-fledged data collection and processing necessitated by AI systems flirt with heavy issues of our time, namely those relating to your privacy and security when it comes to data. Libraries often store high-value private user data in the form of personal information, borrowing history, and search

* Corresponding Author.
Email Address: dalsayed@ksu.edu.sa (A. S. M. Metwally)
https://doi.org/10.21833/ijaas.2025.05.010
Corresponding author's ORCID profile:
https://orcid.org/0000-0001-8234-9545

preferences which need to be secured from misuse or unauthorized access. This dependence on AI also poses ethical challenges, most significantly the threat of algorithmic bias that can potentially result in unfair or discriminatory outcomes. For example, AI models that are developed based on biased datasets may inadvertently privilege certain groups of users over others and consequently contravene the bedrock principle of equitable access to information upon which library services rest (Shal et al., 2024; Manoharan et al., 2024).

Blockchains provide an adjunctive answer because they supply you with a way to achieve peer-to-peer, secure data management (de Haro-Olmo et al., 2020). Naturally, some of the features that blockchain delivers such as immutability; transparency and traceability among others have made library administration also look at using this technology to enhance data security. Blockchains have the potential to secure data integrity and rebuild user confidence (by offering tamper-proof transactional records, all while ensuring controlled access to digital archives that are not subject to manipulation) (Hrovatin et al., 2022). However, like all blockchain implementations, these are also challenges to overcome in the form of technical complexity and scalability issues as well as ethical guidelines for its use (Seddon, 1990; Schmidt, 2002).

The motivation behind this study is to overcome these challenges by developing an AI and blockchain technology integrated framework, which exploits the strengths of both countermeasures while dealing with their associated limitations. This research addresses a gap in the literature by understanding best practices and ethical implications involving AI, blockchain, data privacy for libraries to deploy these emerging technologies safely without violating one's trust or ethics; and by deriving actionable insights and practical solutions that can guide how academic libraries adopt such technology responsibly with minimal impact on decision-making.

In this paper, we examine the interrelated impact of AI and blockchain technologies on data privacy under ethical constraints in library management to explore how these can improve library services while preserving user privacy and fair dealing norms. The research project examines how securing against data risks like misuse, unauthorized access, and breaches is a complex task in AI-powered systems that use sensitive user-aware information.

One of the main research challenges addresses how to evaluate current data protection approaches in AI applications and highlight areas for improvement that may harm user privacy. The study contributes to a better understanding of privacy-preserving methods like differential privacy, federated learning & homomorphic encryption that can be integrated within AI frameworks towards improved data security. The research also explores AI's ethical challenges to librarians: these are transparency, accountability, and algorithmic bias; which can impact user confidence in the impartial operation of library services (Safdar et al., 2023; Abdelati, 2024).

The research in this regard is also the potential of blockchain technology to overcome these limitations, especially its ability to create secure and transparent data management systems. In this paper, the research combines blockchain and AI to explore how libraries can build complete system architectures that prevent unauthorized access to user data, with concrete mechanisms for enforcing accountability and ethics. This work proposes an innovative model for the ethical and safe integration of AI and blockchain into library administration in a manner that is scalable, extensible, and customizable for deployment to various library environments.

The primary objective of this research is to create an educating framework for the integration between AI and Blockchain technologies in Library Administration, which considers data privacy/ethical challenges. We also aim to give libraries a practical sense of some measures that can enhance data security, ensure user trust, and maintain high ethical standards with AI-driven services. For example, it measures the risk that AI poses to data privacy by determining if libraries face a higher likelihood of suffering from saved breaches or uncollateralized access and abuse of private information. It also examines the ethical considerations of AI and blockchain as they relate to libraries, including algorithmic bias, transparency, and accountability (Tariq et al., 2019; Moreno et al., 2016). Finally, the study assesses advanced privacy-preserving technologies such as homomorphic encryption, differential privacy, and zero-knowledge proofs to be possibly integrated into AI and blockchain frameworks to enhance data security while maintaining user anonymity. Finally, we put forward an original concept of the Ethical AI Deployment Framework providing a seamless and ethical way to administer libraries (colossal or individual) and ensure the incorporation of these technologies with privacy-preserving ways for providing robust stability in library management. The framework is designed to be scalable and malleable, providing relevance across a range of library contexts. The functions and relevance of these digital marketing tools to help public libraries in enhancing their services have been highlighted in Table 1.

2. Literature review

AI and blockchain technologies are gaining traction in library administration, much of which has appeared to be extensive literature reviewing the transformative power as well as challenges such as privacy issues and ethical concerns (Bubinger et al., 2021). This section reviews research done to date, the advantages and disadvantages of using AI or blockchain in libraries. This review is structured to examine AI for library management based on current trends, data protection issues, and ethical aspects of

biographies in using artificial intelligence implementation.

2.1. Current trends in AI for library administration

In this past decade AI technologies have increasingly penetrated library administration either for automating different functions from cataloging and classification to information retrieval or even assisting users in terms of user interaction (MacGregor, 2020). Machine learning, natural language processing, and predictive analytics are the most frequently used AI methods in libraries which can be provided for various purposes to improve the efficiency of services through customization. An example is the analysis of user behavior using machine learning to make recommendations for individual and natural language processing for a more accurate search. Libraries can employ predictive analytics to anticipate what users need and how resources are best allocated, leading to better (and more) service. However, the use of AI in a library has its own challenges as well. One of the most important concerns is that AI systems rely on huge datasets to be trained and optimized. At the same time, this dependence on data raises major concerns about privacy and how people's information is handled in an ethical way (Abdelati et al., 2023). Research indicates that while AI could substantially improve library services, it may also bring threats such as data protection liability and potential risks of privacy infringement. What's more, the complicatedness of AI algorithms has a corollary issue: They're so opaque that they not only hide from users how their data is used but also conceal the outcomes generated by an AI-driven process.

Considering recent research, building ethical AI frameworks has become crucial to ensure transparency, accountability, and user consent. To help improve model interpretability, concepts like explainable AI (XAI) have been recommended to offer users a better understanding of how decisions are being made by their models. Additionally, privacy-preserving methods like federated learning and differential privacy have been proposed to minimize the disclosure of sensitive data by AI models while maintaining their effectiveness.

2.2. Data privacy concerns in ai-powered libraries

The kind of information libraries collect and handle as part of their business means that data privacy is a big deal when it comes to AI-driven library administration. Libraries process a wide array of sensitive personal information — borrowing histories, search preferences, and other idiosyncrasies about who you are as an individual that is crucial to delivering personalized services but also represents significant privacy risks. AI systems need a huge amount of data which poses risks for libraries as they can lead to data breaches, unauthorized access, and personal information may well be used in an inappropriate way.

Table 1: Overview of digital marketing tools in public libraries

Tool/technology	Description	Relevance to libraries
Social media platforms	Channels like Facebook, Twitter, and Instagram used for engagement	Enhance community outreach and engagement
Email marketing	Targeted email campaigns for announcements	Personalizes communication with patrons
AI-based recommendations	Systems that suggest resources to users	Improves user experience and service efficiency
Blockchain technology	Ensure data integrity and secure transactions	Enhances trust and data security

The literature has emphasized that strong data protection mechanisms are necessary to protect user privacy in AI-driven settings. Data security improvement recommendations usually include encryption, access controls, and anonymization techniques. Yet these responses are not sufficient to meet the complex challenges that AI systems, many of which require fine-grained and detailed data on a scale to operate effectively.

More recent work advances privacy-preserving technologies (e.g., fully homomorphic encryption, differential privacy, and federated learning), which show potential for striking the balance between the benefits of gaining utility from user data and ensuring that inferences about individuals must be minimal. This allows encrypted data to be used in computations so that no sensitivity is leaked during any time of the processing pipeline. Differential privacy renders a strong mathematical assurance that the individual data point will never be re-identified, even when analyzing aggregated data thus protecting user particularity but not on Expense of AI quality. Federated learning allows AI models to be trained on a myriad of localized devices or servers, thus mitigating the gentrification factors.

For example, suppose a library employs differential privacy to aggregate borrowing patterns across individuals to reveal high-level trends. The library wants to know which materials are most borrowed. However, it does not want to expose the borrowing histories of patrons, and applying differential privacy lets the library know which materials are most prevalent while preserving patrons' borrowing histories. Data trends can be leveraged in a privacy-preserving manner – e.g., we can recommend trendy subjects or genres to new users based on aggregated trends observed in other users.

While such tactics are promising, they have been relatively slow to be operationalized in library environments due to a lack of both technical know-how and resources. Consequently, there is a huge demand for some sort of structured guidance that can be used by libraries to adapt these privacy-

enabling technologies into their AI systems and being able to exploit the advantages without compromising user data.

2.3. Ethical considerations in the implementation of AI

Outside of user data privacy issues, the deployment of AI in libraries has broader ethical considerations associated with it: transparency, fairness, and accountability just to name a few (e.g. algorithmic bias). Without proper oversight, AI systems can simply replicate the biases built into training data and produce discriminatory results that violate equal access to information. For instance, AI algorithms employed by search and recommendation engines can inadvertently prioritize a particular type of content or user group while excluding others entirely – this results in what is known as an information bubble or echo.

When AI drives decisions, transparency is an important ethical consideration because we need to understand how our data is used and the basis of those AI-driven choices. Most AI algorithms, specifically deep learning models are highly "opaque" making it impossible for users and even developers to understand (even if they wanted) how decisions were made by the algorithm. This lack of transparency undermines trust in users and poses a barrier to using AI technology within libraries.

In response to these ethical dilemmas, experts in the field have urged for more transparent or interpretable AI models that can explain how decisions are made. In other words, AI techniques are supposed to lift the veil of secrecy on AI systems and allow users to better understand what factors contribute to decisions that an AI system makes. On the other hand, fairness-aware algorithms have been discussed for neutralizing biases on AI systems to treat all user groups equally.

Accountability is another important ethical benchmark that libraries must meet by ensuring the AI works ethically and legally. Those activities will also include things like mechanisms for auditing AI algorithms, monitoring their output, and managing unintended consequences that do result. To successfully navigate the complex ethical landscape of AI deployment in libraries, it is crucial that we adopt guidelines and best practices for ensuring responsible use in a manner consistent with user trust and established standards.

2.4. Blockchain applications in enhancing data security

In terms of automatic library service based on massive data and AI, the application of blockchain technology may be an ideal solution to supervise large-scale information security implementation in libraries. The fact that it is decentralized and immutable makes blockchain a perfect solution for keeping the integrity of data because traditional methods as you know depend on centralized systems which are prone to attacks. Blockchain can dramatically lower the risk of data breaches and unauthorized access by creating tamper-proof records of transactions that will be detected if altered (Chengxi, 2022).

One tangible application for the library management aspect of blockchain could be safeguarding interlibrary loan records. Blockchain can be used to record these transactions safely and immutably to provide data transparency but prevent any undesired intervention in the transactions of the libraries within a consortium. It gives access to libraries and the users in the form of a non-tampered record, which increases data security and the system's credibility among the users.

Blockchain in libraries is not just about data security; it carries numerous enticing features like the possibility of enhanced transparency, better user trust, and more efficient administrative processes. The blockchain can, for instance, serve as a secure digital archive or be used to catalog the provenance of digital artifacts and manage rights around these materials that allow libraries improved autonomy with their content and assets. Furthermore, the ability to automate processes that are mundane in nature such as inter-library loans, and access permissions through smart contracts—self-executing contracts with the contract terms directly written into code will allow increased operational efficiency within libraries.

But of course, the introduction of blockchain in libraries has its own hurdles to overcome. Adoption barriers, including technical complexity, problems with scalability, and the need for specialized expertise Furthermore, although blockchain technology ensures the quality of data stored on it very strictly — there is little to no doubt that if some information entered a block in one state, then left this block at another time for any participant. It does not give us impersonality, naivety, and access immediately. All parties have an unedited history script available leading them from the genesis transaction through all participating actions each second. To overcome these restrictions, researchers are moving forward with the idea of privacy-preserving blockchains which undoubtedly maintain blockchain's proven security facet and include higher-level encryption methods like zero-knowledge proofs through which transaction validation is probable without sharing anything private (Quasim et al., 2020).

Insights from the literature lead to considering a potential way for which blockchain and AI can be integrated, providing us with an effective means of resolving data privacy problems as well as ethical issues (Zhang, 2019). With the secure data management features of blockchain and AI's computing power, libraries have generated a complete framework for delivering robust data security principles alongside transparency including ethics. This article describes how we put these insights together to come up with a new framework combining AI and blockchain technology while

preserving privacy, creating such an architecture that will assist in the fair adoption of those technologies within libraries (Ma and Xia, 2022).

Table 2 presents the main themes resulting from AI and blockchain literature in libraries- dimensions used for identifying problems targeted by our study.

Table 2: Key themes and gaps in the literature on AI and blockchain in libraries

Theme	Key findings	Identified gaps
Ethical AI implementation	Emphasis on transparency and accountability	Limited practical guidelines for libraries
Data privacy challenges	Risks associated with data collection and management	Need for robust frameworks tailored to libraries
Blockchain applications	Potential for enhancing data security and transparency	Lack of empirical studies in library settings
Digital transformation	Positive impacts on user engagement	Underexplored in small or underfunded libraries

The latest strategies associated with privacy-preserving AI have tested federated learning and homomorphic encryption, which can run the potential representation to get the outcome without making it centralized (Chen et al., 2020; Jones et al., 2020). MedTech technologies can use concepts like federated learning, where models train on local devices instead of needing local data, allowing more privacy-safe approaches for AI model development. While these frameworks deal with data security, they do not provide data integrity and transparency which is essential in a public service environment such as the library (Negru et al., 2021; Barsha and Munshi, 2023).

There have also been frameworks for making ethical AI like Explainable AI (XAI) to transparent the AI decision-making process by making operations more interpretable to the user. Explainable AI (XAI) frameworks offer insights into how AI works that can help engender user trust; however, they typically do not address the privacy concerns surrounding the data input into the model. We provide a framework that bridges this gap by a composition between privacy-preserving technologies, such as differential privacy and zero-knowledge proofs, and ethical safeguards.

The use of blockchain, when integrated with our framework, is also a distinguishing feature from existing models, as it provides a secure, immutable ledger that allows data integrity and transparency in library transactions. An example of this is recording interlibrary loan transactions through blockchain as it allows a tamper-proof, shared record accessible to users and library staff. This two-pronged privacy-preserving AI and blockchain approach provides an aptly customized fit for library requirements, having nuances around both data privacy and ethical considerations.

Overall, our proposal both draws from the existing literature and adds to it by implementing a unique integrated approach focusing on the realization of all relevant aspects of the problem (especially privacy, ethics, and data integrity) toward AI-enabled library management, which renders the solution wide-ranging as well as practical.

3. Research methodology

Through a thorough mixed-methods research design incorporating both quantitative and qualitative, the study provides a comprehensive analysis to investigate how AI & blockchain technologies affect data privacy and ethical considerations in library management. A mixed-methods methodology was chosen because it provides a comprehensive perspective on the research problem — thus allowing for triangulation and integration of different data types to enhance generalizability and reduce bias.

The study employs a mixed-methods approach intended to offer a fuller picture surrounding the complicated matters of AI and blockchain for libraries. Using a quantitative design, survey data documenting key trends, including user trust and privacy concerns, gave researchers an overview of trends across participants. Interviews yielding qualitative data provided additional richness, highlighting nuanced perspectives on topics such as the transparency of algorithms and their ethical implications. Including both allowed us to find the middle ground and fulfilled the standards of new expectations in ethics and privacy in data research.

3.1. Research design

The study is designed as a sequential explanatory mixed-methods approach; whereby it includes collecting and analyzing quantitative data first, followed by qualitative data to extend the understanding of the results obtained from its initial phase. This design was chosen to allow the broad range of quantitative data to be balanced against deep qualitative insights, assisting in building a more nuanced understanding of some complex topics surrounding privacy and ethics related more broadly as well to AI library administration.

This was followed by an extensive literature review that helped to identify the voids and shaped the theory of change for study. A review was carried out and this also directed the development of research questions as well as shaped how data would be collected. The sequential method was advantageous, as quantitative findings were employed to identify the main themes and areas of crucial interest that were followed by qualitative investigation.

3.2. Qualitative component

The study's qualitative part was based on interviewing the key players such as library directors, IT people, and end-users who need or produce linked data. The qualitative methodology was used to capture the personal experiences and perceptions of the participants which contributed

more rigor in understanding some ethical considerations with difficulties, on privacy issues about AI and blockchain integration into libraries. The interview protocol, which was specifically designed to focus on the themes identified in our quantitative analysis and areas where more detail could cast new light is here. A series of open-ended questions were developed to elicit participant experiences and perspectives in their own words. During the interviews, major thematic areas were: How AI/blockchain technologies are perceived; Concerns around data privacy and ethical implications Perceived challenges in the implementation phase.

A purposive sample of 20 participants with different roles in the library was selected to capture a broad range of perspectives. Interviews were conducted either in person or via video call, depending on participants' preferences and availability. Each session lasted approximately 45 to 60 minutes and was audio recorded with informed consent, then transcribed verbatim into a digital document. The qualitative data were analyzed using thematic analysis, a flexible method suited for identifying and interpreting patterns within data. This approach was chosen for its ability to provide detailed insights into participants' experiences and reasoning. The analysis followed six key steps: familiarization with the data, coding, generating initial themes, reviewing themes, defining and naming themes, and writing up the findings. This method enabled a thorough exploration of the complex ethical, privacy, and technological challenges—particularly those related to AI and blockchain—faced by libraries.

For systematic analysis of qualitative data, thematic analysis was carried out. We initially thoroughly reviewed participants' responses to extract common themes around privacy, security, and ethics. Next, data coding was applied to classify it meaningfully into key concepts and words. However, we aggregated these codes into wider overarching themes (e.g., "Trust and Privacy Concerns"), indicating problems that participants saw as particularly serious. This iterative process helped guarantee the legitimacy and robustness of the themes that reflected participants' concerns. Last, topics such as "Algorithmic Transparency" and "Ethical Safeguards" were included in the results, providing a systematic overview of the ethical and privacy properties of these sensitive information technologies in library systems.

3.3. Quantitative component

The quantitative end of the work entailed administering a structured survey to thousands of library users and staff. The survey sought to find vast data on how the participants were experiencing/receiving it, and what they considered with respect to implementing AI/blockchain technologies in library settings. The survey development was guided by the findings from a literature review whose aim was related to key research focus areas (i.e. data privacy concerns, ethical challenges, perceived level of trust in AI and blockchain technologies) pertinent to questions being addressed here collectively as well. The survey consisted of several parts, such as general information, AI and blockchain awareness perceptions of data privacy concerns (specifically for AI), ethics related to it also how much they could trust in the services using this technology.

A stratified random sampling method was used to distribute the survey among 200 library users and staff from a variety of library settings, including academic, public, and special interest group (SIG) libraries. This approach ensured a sample that reflected diversity in both demographic characteristics and library roles. To maximize participation, the survey was distributed both online and in person, resulting in a high response rate of 75%. The quantitative data collected through the survey were analyzed using descriptive statistics to summarize key features such as means, medians, modes, and frequency distributions. To explore relationships between variables and identify factors influencing user trust and satisfaction with AI and blockchain technologies, inferential statistical methods were applied, including correlation and regression analyses. Correlation analysis was used to determine the strength and direction of relationships among key components such as perceived data security, AI system transparency, and average trust scores. Regression analysis was then employed to examine how these variables influenced overall satisfaction and trust, helping to identify user perceptions that either support or hinder the acceptance of AI and blockchain technologies in library environments.

3.4. Ethical considerations

Ethical considerations in making design decisions on such a delicate subject were heavily emphasized throughout the study. All participants gave written informed consent before participation after being presented with the purpose of the study, all methods utilized in it, and possible risks. Participants provided written consent for us to keep their data confidential and not report on any individual details of the survey or follow-up interviews. All data were de-identified by removing any identifying information, and digital research materials will be stored securely with encryption methods as well as password protection to safeguard this information.

Methods for analgesic study followed ethics guidelines from the institutional review board regarding respect for people, beneficence, and justice. Throughout the research, debriefing sessions were regularly conducted with the researchers to discuss ethical matters related to it and monitor that ethics was compiled at the highest level. Moreover, the study design included steps to protect participants: sensitive topics were handled gently, and all respondents could freely withdraw from the

research without a penalty. Table 3 presents information on the data collection methods used for this study as well as participant demographics.

4. Results

The findings of this work help us to give an overall glance over the issues related to AI and blockchain applications for library administration. In this section the results of both qualitative and quantitative components are discussed together under suitable headings, to give a clearer picture of those key themes or patterns that were found in our data. The mixing of these findings results in fine-grained knowledge of how user trust, data security, and ethical standards are affected by those Techs implemented in library settings.

4.1. Presentation of qualitative data

The qualitative portion of the study consisted of 20 semi-structured interviews with key stakeholders, specifically library administrators, IT staff, and users. The thematic analysis of the interview data suggested several important themes that shed light on what participants think and experience in relation to AI & blockchain technologies used for library administration.

Table 3: Research design and methodology

Component	Description	Details
Research design	Mixed-methods approach combining qualitative and quantitative data	Justification for combining approaches
Data collection methods	Interviews, surveys, and digital Analytics	Specific tools and platforms used for data gathering
Participant demographics	Library staff, administrators, and users	Number of participants, roles, and library types

Themes: Four main themes emerged from the analysis, namely, data privacy fears are greatest when it comes to sharing personal or sensitive information; ethical issues have significant weight in decision making but practical obstacles persist and should not be ignored; perceptions of AI & blockchain capabilities may magnetize incorrect expectations. Many participants expressed strong concerns about the privacy of their personal data, particularly around borrowing histories and search preferences. Transparency in decision-making was a recurring theme, with several participants warning that the invisibility of algorithms could undermine user trust. The ethical implications category focused on algorithmic bias and the risk of discriminatory results. AI models are easily prone to become biased because of the bias already present in training data, which could result in unfair treatment towards certain groups as observed by participants. There was a great deal of talk about accountability and how to intervene when such biases occur, along with proposals for greater regulation or at least code-of-ethical standards in the deployment of AI in libraries.

Participants identified practical implementation challenges as a central theme, noting the need for specialized technical expertise, limited resource availability, and repetitive administrative tasks as key barriers. Despite these difficulties, many still expressed positive views regarding the potential benefits of AI and blockchain technologies. For instance, Automation Intelligence—primarily interpreted as artificial intelligence, though it may also include machine learning—was seen as valuable, even in contrast to concerns in public discourse about job displacement due to automation. Similarly, participants viewed blockchain as a promising tool, particularly in areas related to data integrity and security. Exemplifying quotes from participants are provided to illustrate and support these emerging themes.

- I am curious how these AI systems are using my borrowing history. We don't have visibility into who has this data and why. (Library User)
- AI can vastly help but without transparency in this process, it is difficult for us to trust the results. We must figure out how you make decisions. (Library Administrator)
- Keeping IT on the rails and making sure that things run correctly is executives' main stressful point. One of the biggest challenges there, over all these decades, has been finding technical skills to manage your systems for you too! Ultimately, it is not just about technology but also having the people skilled to use that fantasticness. (IT Staff)

Fig. 1 shows the frequency of themes identified from qualitative data, with data privacy concerns as the most frequent theme, followed by ethical issues and practical challenges.

4.2. Presentation of quantitative data

The quantitative part of the study involved a structured survey administered to 200 randomly selected library users and staff, with 150 valid responses collected after accounting for the response rate. The survey explored participants' experiences, perceptions, and concerns regarding the use of AI and blockchain technologies in libraries. It specifically examined issues related to data privacy, trust, and satisfaction with the implementation of these technologies.

Descriptive statistical analysis revealed that 68% of respondents were concerned about data privacy and how their personal information was handled by AI systems. Additionally, 55% expressed concern over the lack of transparency in AI processes, and 48% highlighted ethical issues—such as bias—as key factors affecting their trust. Overall satisfaction

with AI and blockchain usage in libraries was moderate, with only 40% reporting high satisfaction.

Correlation analysis showed a strong positive relationship between perceived data security and user trust ($r = 0.72$, $p < .01$), suggesting that increased confidence in these systems is closely linked to users' sense of data protection. A significant positive correlation was also found between transparency in AI processes and trust ($r = 0.65$), indicating that greater transparency may enhance user confidence.

Regression analysis was conducted to identify key predictors of user trust and satisfaction with AI and blockchain technologies. The findings indicated that perceived data security, transparency of AI processes, and efforts to reduce algorithmic bias were significant predictors, collectively explaining 58% of the variance in trust scores ($R^2 = .58$). Addressing these factors is essential for building and maintaining user trust in the adoption of AI and blockchain systems in library environments.

Fig. 2 illustrates the proportion of respondents with concerns about data privacy, where 75% expressed concerns, and 25% did not. Fig. 3 shows the satisfaction levels with AI and blockchain implementations, with most respondents reporting satisfaction, while fewer expressed dissatisfaction.

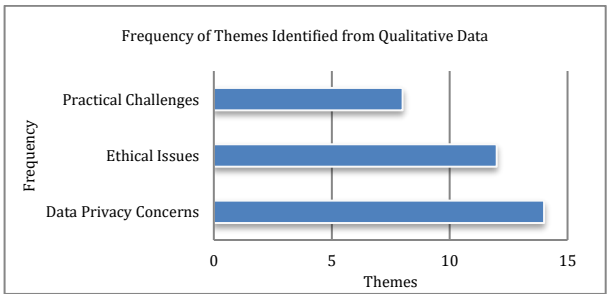

Fig. 1: Frequency of themes identified from qualitative data

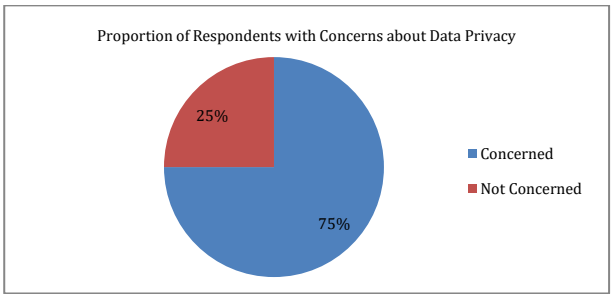

Fig. 2: Proportion of respondents with concerns about data privacy

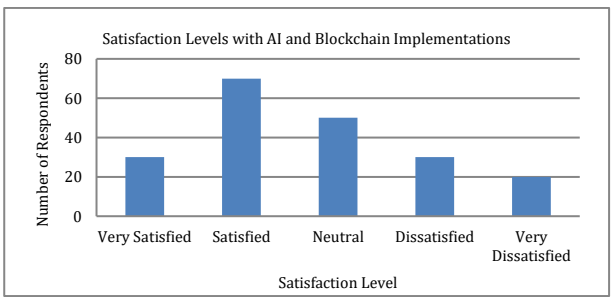

Fig. 3: Satisfaction levels with AI and blockchain implementations

4.3. Analysis of the findings

This study is among the first attempts to present a synthesis of qualitative and quantitative data privacy and ethical challenges in library administration associated with AI and blockchain technologies, which offers insight into the broad perspective. The quantitative figures substantiate the qualitative themes by reflecting both in terms of primary areas for improvement highlighted amongst stakeholders.

Integrating Findings: Data Privacy Emerges as Top Concern in Both Qualitative and Quasi-Quantitative Research The high association between perceived data security and user trust reemphasizes the importance of solid protection mechanisms. Again, the focus on transparency in two sets of data implies that making AI more transparent and accountable to its users is key for trustworthiness.

The qualitative look at ethics in algorithmic management questions provides a nice side piece to the quantitative results of how these influences play out with respect to building trust among users. This is substantiated by regression analysis which shows that an important predictive factor of trust in AI is attempts to manage ethical aspects (bias mitigation, transparency), leading one to believe that there should be specific rules and guidelines on ethics involved around the implementation of AIs.

Proposed Advanced Framework: Drawing from the integration of our findings, an advanced framework for responsible and secure use of AI-enabled blockchain in library administration. The framework builds upon the world-class techniques in privacy-preserving computation such as homomorphic encryption, differential privacy, and zero-knowledge proofs to ensure data are safe from misuse. These methods implement a set of creative remedies to the challenges revealed in their research and thus identify potential means for maintaining private user information whilst capitalizing on AI/Blockchain advantages.

This work is a perfect fit for homomorphic encryption, which means you can compute over encrypted data without ever decrypting it — allowing private information to remain secure count both sides of the processing pipe. Differential privacy protects the anonymity of individual data points, even when conducting in-depth analysis of aggregate datasets. Zero-knowledge proofs allow one party to prove that they know a secret without revealing any additional details, thus these can be used as an efficient mechanism for data integrity and privacy in blockchain implementations. This same framework, this comprehensive understanding surrounding just how ethics plays into AI in a library setting might revolutionize the field and become an impressive innovation in its own right.

Table 4 presents a summary of the key quantitative and qualitative findings related to user engagement rates, satisfaction levels, and the challenges faced by libraries in implementing AI and blockchain technologies. The data highlight patterns

in user responses and provide insights into the broader impact of these technologies on library services and user experiences. Fig. 4 illustrates the correlation between perceived data security and user trust, showing a positive relationship where higher perceived data security tends to correlate with higher user trust. Fig. 5 shows the impact of factors such as transparency and algorithmic bias mitigation on user trust, with transparency demonstrating a greater impact.

Table 4: Summary of quantitative and qualitative findings

Finding	Quantitative data	Qualitative insights
Engagement rates	Average engagement rates on social media platforms	Staff emphasize the need for consistent content
User satisfaction	75% of users report satisfaction with digital services	Users appreciate personalized recommendations
Challenges identified	60% of libraries face budget constraints	Staff highlight the need for digital skills training

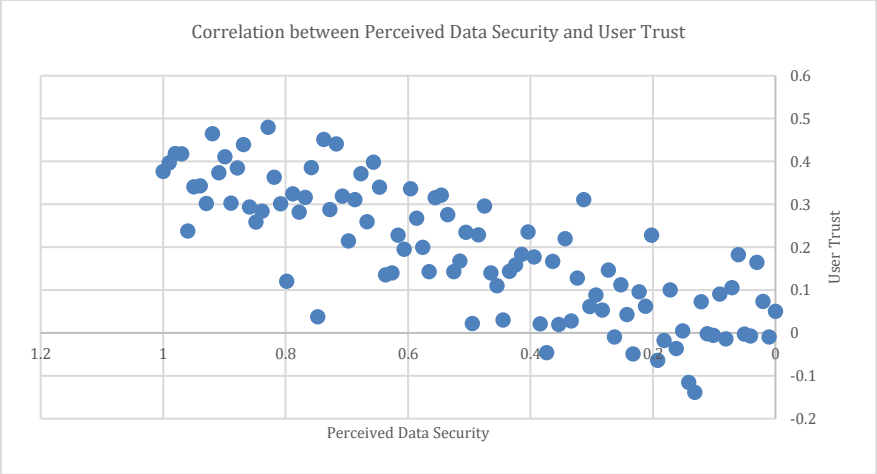

Fig. 4: Correlation between perceived data security and user trust

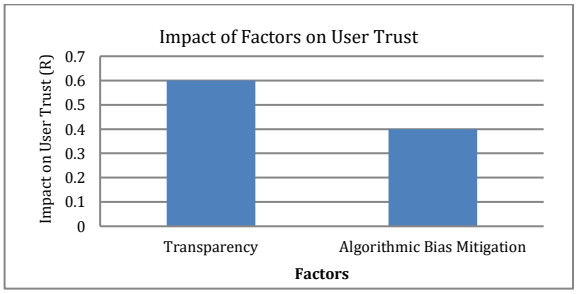

Fig. 5: Impact of factors on user trust

5. Discussion

This section synthesizes the findings of both components of our work — qualitative and quantitative studies, presenting an overarching discussion on what this means for library administration vis-a-vis AI and blockchain technologies in general. Our discussion is based on the central themes that emerged from our results, emphasizing issues around data privacy and ethical considerations as well as approaches to utilizing more developed frameworks to tackle these challenges.

5.1. Addressing research focus

Relevance/Importance of the Topic: This study aims to serve all focus areas with a detailed analysis of how AI and blockchain technologies in library administration influence data privacy and ethical standards. AI as a part of the platform will also significantly enhance user engagement and operational efficiency by providing personalized services to users through automation of different routine activities. Nevertheless, the results highlight significant issues about data privacy and ethical AI practices that still present major impediments to the wider implementation of these applications by libraries. Concerns about data privacy, raised consistently across both the qualitative and quantitative findings, are particularly important as they highlight the risks associated with excessive AI-based passive monitoring. A strong correlation was observed between users' perception of data security and their trust in AI systems, indicating that libraries must adopt effective safeguards to protect users from potential misuse or fraud. These protective measures are essential not only for legal compliance but also for maintaining user trust in AI-powered services. Participants also expressed ethical concerns about algorithmic bias and the limitations of applying one-size-fits-all AI solutions in diverse library settings. They emphasized the need for clearer regulations and specific guidelines to support responsible AI use by library professionals. These concerns echo wider debates in the existing literature, which call for AI systems to be more transparent, accountable, and fair. This reflects a broader need to develop and refine ethical frameworks that can guide the implementation of AI in libraries in a responsible and equitable manner.

While the decentralized and immutable nature of blockchain technology offers promising opportunities for enhancing data security, its technical complexity presents notable challenges, particularly in terms of scalability. The study highlights that although blockchain can improve data integrity and trustworthiness, its implementation must be carefully managed to avoid introducing new

ethical and technical issues. To address these concerns, the proposed framework incorporates privacy-preserving techniques designed to strengthen data protection and safeguard user privacy. This approach aims to ensure that the benefits of blockchain are realized without compromising ethical standards or creating additional risks.

5.2. Scientific contributions and novel framework

This study offers several scientific contributions that can support policymakers in better understanding the role of AI and blockchain technologies in library administration. Its primary contribution is the development of a novel framework that integrates advanced privacy-preserving techniques—such as homomorphic encryption, differential privacy, and zero-knowledge proofs—into traditional AI and blockchain systems. This marks a significant advancement over conventional approaches, as it directly addresses a wide range of data privacy and security concerns while also mitigating key ethical issues identified in the research. The framework introduced in this study is designed to enhance fairness and accountability in AI systems by utilizing verifiable computation. This ensures that AI-generated outcomes can be verified locally or exponentially without disclosing the global values used during computation. Homomorphic encryption enables data to remain encrypted throughout processing, allowing sensitive information—such as library users' borrowing histories or search patterns—to stay protected while still being analyzed. This provides strong mathematical assurances that individual identities cannot be traced from aggregated data, preserving user anonymity. Similarly, zero-knowledge proofs are used in blockchain applications to validate transactions and ensure data integrity without exposing any confidential information. By integrating these technologies, the proposed framework addresses both data privacy and ethical concerns such as algorithmic bias and lack of transparency. It demonstrates how libraries can implement AI and blockchain responsibly, offering a model that could inform ethical deployment across other institutions. The adaptability of the framework also allows it to be tailored to the specific needs of different library environments, making it a practical and scalable tool for promoting responsible innovation in the sector.

5.3. Implications for AI and blockchain-powered library administration

The findings of this study hold important implications for the future development and implementation of AI and blockchain technologies in library administration. While the results demonstrate the potential for these technologies to enhance operational efficiency and data management, they also underscore the critical need to address privacy and ethical concerns from the outset. Libraries must prioritize transparency and accountability, ensuring that users understand how their data is used and can trust decisions generated through AI systems.

The enhanced framework proposed in this study provides a practical guide for libraries to adopt emerging technologies in a responsible and ethical manner. By incorporating privacy-preserving mechanisms, libraries can protect user data, reduce concerns over surveillance or misuse, and foster trust in digital services. This is especially important in a climate where data breaches and concerns over personal information misuse are increasingly common.

The study also highlights the importance of continuous monitoring and evaluation during the deployment of AI and blockchain systems to ensure compliance with ethical standards and alignment with user expectations. Libraries should develop and enforce clear guidelines and protocols, including regular external audits of AI algorithms and fairness assessments, to ensure ethical practice. These measures should be developed collaboratively, involving input from users, policymakers, and technology providers.

Beyond libraries, the findings and framework presented in this study have broader relevance for other public service sectors—such as healthcare, education, and public administration—where data privacy and ethical AI use are similarly critical. Libraries can serve as role models for responsible innovation, demonstrating how institutions can integrate advanced technologies while maintaining ethical standards and prioritizing user trust in the digital age.

5.4. Future research and limitations

This study provides a comprehensive foundation for understanding the technical, ethical, and privacy-related challenges associated with the use of AI and blockchain in library administration. However, it also acknowledges certain limitations that should be addressed in future research. One limitation lies in the qualitative component, which included a relatively narrow range of stakeholder perspectives—though the insights gained were valuable. Future studies should aim to include a more diverse group of participants, particularly individuals with varying levels of familiarity and comfort with AI technologies, including those used by major providers such as Microsoft.

Additionally, the findings may have limited applicability beyond the library sector, as the study focuses specifically on library contexts. To broaden its relevance, future work could involve adapting and testing the proposed framework in other public service domains. Conducting formative and validation studies across different sectors would offer important insights into how the framework performs in various settings. Longitudinal studies

could also help assess the framework's effectiveness over time, particularly in maintaining data privacy, fostering user trust, and enhancing satisfaction with AI and blockchain applications.

The research further suggests that there is room for continued technological enhancement of the proposed framework. Innovations such as federated learning and other privacy-preserving machine learning approaches offer promising ways to improve data protection without diminishing AI system performance. As new technologies emerge, it will be important to integrate them into the framework to ensure their ongoing relevance and effectiveness in ethical AI deployment.

Finally, the study emphasizes the need for collaborative efforts among libraries, technology providers, and policymakers to establish standardized guidelines and best practices for AI and blockchain implementation. Such cooperation is essential to realizing the benefits of these technologies while upholding strong ethical standards and protecting user privacy.

Table 5 Comparison between current study findings and the extant literature illustrating commonalities as well differences that inform contributions for this investigation. Table 6 summarizes the main findings of this study with practical recommendations for libraries.

Table 5: Comparison of current study findings with existing literature

Focus area	Current study findings	Comparison with Literature
Ethical AI use	Framework proposed for ethical AI implementation	Similar calls for ethical standards in other studies
Blockchain benefits	Enhance data integrity and security in libraries	Confirmed by existing studies on blockchain in archives
User engagement	Digital tools improve engagement significantly	Consistent with findings from other digital transformation research

Table 6: Summary of contributions and recommendations

Contribution	Practical implication	Recommendation for libraries
Ethical AI framework	Provides a clear guideline for implementing AI responsibly	Adopt and adapt the framework to specific contexts
Enhanced user engagement	Validates the effectiveness of digital marketing tools	Invest in training and technology to maximize impact
Data security improvements	Highlights blockchain's role in securing library data	Explore blockchain applications tailored to library needs

6. Conclusion

This study comprehensively examines AI and blockchain technologies on data privacy and ethical concerns in library administration. While the envisioned applications of this integration are potential opportunities to expand library services, they come with an equally rich set of data risks associated with a liberal use, including privacy and security concerns either directly or through indirect activity such as algorithmic bias and ethical dilemmas. This means that libraries need to put into practice a strict data protection policy in place and transparency of AI methods, along with creating guidelines for the ethical use of blockchain technology. This could allow libraries to take advantage of AI and blockchain without compromising the privacy or ethical standards that are a hallmark feature.

The conclusion of the study is that AI integration severely suffers from threats to data privacy, which sounds an alarm for robust Data Protection measures. It also underscores the significance of transparency and accountability in AI systems, which undercuts user trust while hoping to dampen ethical concerns. Although blockchain technology can introduce new promising approaches to data security, its efficacy should be tempered by ethical and technical cautions. Further research should aim to validate the proposed frameworks methodologically and investigate how AI/Blockchain will reshape library administration for good or bad terms. When libraries responsibly embrace these technologies, they will be positioned to serve users better and remain the trusted stewards of data for which we can hold them accountable. This research establishes a systematic approach that can ensure the ethical and secure deployment of these technologies while protecting user privacy on the one hand and complying with ethics on the other.

Acknowledgment

The authors extend their appreciation to the Libraries Commission at the Ministry of Culture – Saudi Arabia for funding this work through the Library Research Support Program.

Compliance with ethical standards

Ethical considerations

This study was conducted in accordance with institutional review board guidelines. All participants provided written informed consent. Data were anonymized and stored securely in compliance with privacy standards.

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Abdelati MH (2024). Smart traffic management for sustainable development in cities: Enhancing safety and efficiency. International Journal of Advanced Engineering and Business Sciences, 5(1): 49-62. https://doi.org/10.21608/ijaebs.2024.242361.1088

Abdelati MH, Abd-El-Tawwab AM, Ellimony EEM, and Rabie M (2023). Solving a multi-objective solid transportation problem: A comparative study of alternative methods for decision-making. Journal of Engineering and Applied Science, 70(1): 82. https://doi.org/10.1186/s44147-023-00247-z

Abdelati MH, Abd-El-Tawwab AM, Ellimony EEM, and Rabie M (2024). Efficient transportation planning: a case study of multi-dimensional solid transportation problem. Journal of Engineering Science and Technology Review, 17(5): 32-38. https://doi.org/10.25103/jestr.175.04

Adams RJ (2024). Information technology and libraries: A future for academic libraries. Taylor and Francis, London, UK. https://doi.org/10.4324/9781003505877

Barsha S and Munshi SA (2023). Implementing artificial intelligence in library services: A review of current prospects and challenges of developing countries. Library Hi Tech News, 41(1): 7-10. https://doi.org/10.1108/LHTN-07-2023-0126

Bubinger H and Dinneen JD (2021). Actionable approaches to promote ethical AI in libraries. Proceedings of the Association for Information Science and Technology, 58(1): 682-684. https://doi.org/10.1002/pra2.528

Chen H, Hussain SU, Boemer F, Stapf E, Sadeghi AR, Koushanfar F, and Cammarota R (2020). Developing privacy-preserving AI systems: The lessons learned. In the 57th ACM/IEEE Design Automation Conference, IEEE, San Francisco, USA: 1-4. https://doi.org/10.1109/DAC18072.2020.9218662

Chengxi S (2022). Application of block chain technology in Wisdom Library under public health emergencies. Academic Journal of Computing and Information Science, 5(5): 51-56. https://doi.org/10.25236/AJCIS.2022.050507

de Haro-Olmo FJ, Varela-Vaca ÁJ, and Álvarez-Bermejo JA (2020). Blockchain from the perspective of privacy and anonymisation: A systematic literature review. Sensors, 20(24): 7171. https://doi.org/10.3390/s20247171 **PMid:33327652 PMCid:PMC7765152**

Hrovatin N, Tošić A, Mrissa M, and Kavšek B (2022). Privacy-preserving data mining on blockchain-based WSNs. Applied Sciences, 12(11): 5646. https://doi.org/10.3390/app12115646

Jayavadivel R, Arunachalam M, Nagarajan G, Shankar BP, Viji C, Rajkumar N, and Senthilkumar KR (2024). Historical overview of AI adoption in libraries. In: Senthilkumar KR (Ed.), AI-assisted library reconstruction: 267-289. IGI Global, Hershey, USA. https://doi.org/10.4018/979-8-3693-2782-1.ch015

Jones KM, Briney KA, Goben A, Salo D, Asher A, and Perry MR (2020). A comprehensive primer to library learning analytics practices, initiatives, and privacy issues. College and Research Libraries, 81(3): 570-591. https://doi.org/10.5860/crl.81.3.570

Ma Z and Xia Z (2022). Exploration of university library management mode from the perspective of blockchain technology. Frontiers in Business, Economics and Management, 3(2): 47-49. https://doi.org/10.54097/fbem.v3i2.262

MacGregor R (2020). Responsible operations: data science, machine learning, and AI in libraries. The American Archivist, 83(2): 483-487. https://doi.org/10.17723/0360-9081-83.2.483

Manoharan G, Ashtikar SP, and Nivedha M (2024). Integrating artificial intelligence in library management: An emerging trend. In: Senthilkumar KR (Ed.), AI-assisted library reconstruction: 144-157. IGI Global, Hershey, USA. https://doi.org/10.4018/979-8-3693-2782-1.ch008

Meurisch C and Mühlhäuser M (2021). Data protection in AI services: A survey. ACM Computing Surveys (CSUR), 54(2): 1-38. https://doi.org/10.1145/3440754

Moreno J, Serrano MA, and Fernández-Medina E (2016). Main issues in big data security. Future Internet, 8(3): 44. https://doi.org/10.3390/fi8030044

Negru AE, Betev L, Carabaș M, Grigoraș C, Țăpuș N, and Weisz S (2021). Analysis of data integrity and storage quality of a distributed storage system. EPJ Web of Conferences, 251: 02035. https://doi.org/10.1051/epjconf/202125102035

Quasim MT, Algarni F, Radwan AAE, and Alshmrani GMM (2020). A blockchain based secured healthcare framework. In the International Conference on Computational Performance Evaluation, IEEE, Shillong, India: 386-391. https://doi.org/10.1109/ComPE49325.2020.9200024

Safdar M, Qutab S, Ullah FS, Siddique N, and Khan MA (2023). A mapping review of literature on blockchain usage by libraries: Challenges and opportunities. Journal of Librarianship and Information Science, 55(3): 848-858. https://doi.org/10.1177/09610006221090225

Schmidt J (2002). Unlocking the library: Marketing library services: A case study approach. IFLA Publications, 99: 87-97. https://doi.org/10.1515/9783110962215.87 **PMCid:PMC2014432**

Schöpfel J (2018). Smart libraries. Infrastructures, 3(4): 43. https://doi.org/10.3390/infrastructures3040043

Seddon S (1990). Marketing library and information services. Library Management, 11(6): 35-39. https://doi.org/10.1108/EUM0000000000832

Shal T, Ghamrawi N, and Naccache H (2024). Leadership styles and AI acceptance in academic libraries in higher education. The Journal of Academic Librarianship, 50(2): 102849. https://doi.org/10.1016/j.acalib.2024.102849

Singh Y (2024). Managing the heart of knowledge: Strategies for library administration and management. International Journal of Scientific Research and Engineering Development, 7(2): 337-343.

Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, Baker T, Hammoudeh M, and Ghafir I (2019). The security of big data in fog-enabled IoT applications including blockchain: A survey. Sensors, 19(8): 1788. https://doi.org/10.3390/s19081788 **PMid:31013993 PMCid:PMC6515199**

Zhang L (2019). Blockchain: The new technology and its applications for libraries. Journal of Electronic Resources Librarianship, 31(4): 278-280. https://doi.org/10.1080/1941126X.2019.1670488