2023

A Blockchain tool to detect and mitigate e-book piracy: a case study of Kenya.

Nzangi, Joy Mwende
School of Computing and Engineering Sciences
Strathmore University

A Blockchain Tool to Detect and Mitigate E-Book Piracy: A Case Study of Kenya

By

Joy Mwende Nzangi

124553

Master of Science in Computing and Information Systems

July, 2023

A Blockchain Tool to Detect and Mitigate E-Book Piracy: A Case Study of Kenya

By

Joy Mwende Nzangi

124553

Submitted in partial fulfillment of the requirements for the degree Master of Science in Computing and Information Systems at Strathmore University

School of Computing and Engineering Sciences Strathmore University

Nairobi, Kenya

July, 2023

Declaration and Approval

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Student Name: Joy Nzangi

Sign:  **Date**: Thursday 31st May 2023

Approval

The dissertation of Joy Nzangi was reviewed and approved for examination by the following:

Professor Ismail Ateya Lukandu

School of Computing and Engineering Sciences,

Strathmore University.

Dr. Julius Butime,

Dean, School of Computing & Engineering Sciences,

Strathmore University

Dr. Bernard Shibwabo,

Director of Graduate Studies,

Strathmore University

Abstract

Numerous online e-book markets have emerged along with the growth of e-book readers. This has also increased the speed and ease with which people share books. As a result, piracy has been skyrocketing since there is no security for books being shared, allowing only one person to have one copy of the purchased books. Globally, e-book piracy has been a significant setback for publishers, as the available solutions cannot offer the necessary content protection. A good example is the strict Digital Rights Management (DRM) that occasionally annoys real readers by preventing them from accessing their books or forcing them to forfeit ownership if the platform is shut down. Publishers, online platform providers, and writers currently comprise the e-book market. E-book piracy has real-world consequences that affect both publishers' and authors' bottom lines and their ability to produce more books. This work developed a non-fungible-token-based e- book platform that enables writers to self-publish e-books and sell them without the risk of piracy. NFTs, or non-fungible tokens, are digital assets that stand in for real-world things like artwork, collectibles, and game assets. New Financial Instruments (NFTs) use blockchain and smart contracts as their underlying digital infrastructure. When published, each book will have a separate non-fungible token (NFT) attached to it. The study used a trusted and secure e-book transaction system that meets the following security requirements: license verification for each e-book, content confidentiality, right to read authorization, authenticating a genuine buyer, confirming the validity and integrity of e-book contents, direct purchase safety, and preventing e-book piracy and illegal downloading. The developed solution will be a lifesaver for the e-book industry in Kenya and other regions worldwide since they offer an easy way for readers and authors to easily make secure e-book transactions with zero risk of piracy or denial of access for legitimate access users.

Keywords: Blockchain, E-book, Non-Fungible Tokens, Piracy, Smart Contracts.

Table of Contents

List of Figures

List of Tables

Abbreviations/ Acronyms

E-book - Electronic book

GDP - Gross Domestic Product

IPFS - Interplanetary File System

KECOBO - Kenya Copyright Board

NFT(s) - Non-Fungible Token(s)

Definition of Terms

Blockchain A blockchain, or distributed ledger, is a distributed database that records transactions in a chronological chain of blocks. As more and more building blocks are added to this chain, it lengthens (Zibin Zheng et al., 2017).

Ledger One or more blocks that have been verified and authenticated by the relevant members of the network and on which transactions have been recorded (Rasure, 2021).

Non-Fungible Tokens (NFTs) NFTs are unique digital tokens that prove possession of an item of content, such as a digital painting, a game item, or a collectible. NFTs are digital assets that are traded on online marketplaces for cryptocurrencies like Ethereum and that use cryptographic mechanisms to replicate the properties of physical items like scarcity, uniqueness, and proof of ownership (Regner et al., 2019).

Smart Contracts Smart contracts are decentralized, anchored scripts on blockchains or similar infrastructures that allow the transparent execution of predefined processes (Ante, 2020).

Acknowledgments

I am eternally grateful to Almighty God for all His love, kindness, guidance, knowledge, and wisdom. I am grateful to my supervisor, Professor Ismail Ateya, for his exceptional help with this project. Thank you for your excellent advice, guidance, and persistence during the duration of my proposal. My heartfelt thanks go out to my family and friends for their unwavering support.

Chapter 1: Introduction

1.1 Background

The World Wide Web connects the world by facilitating global opportunities. E-books can be sold to readers by authors and publishers. Despite the advantages, E-book piracy is a global problem (Karaganis, 2011). Malicious websites or individuals obtain a copy of a publication and distribute it for free or for a fee on the Internet. According to (Fisk, 2009), "piracy" is "the illegal copying and distribution of intellectual property without the owner's permission." A copyright is the exclusive, transferable legal right to print, publish, perform, film, or record a work of literature, art, or music for a specific period of time. Thus, electronic book theft refers to the illegal downloading and dissemination of protected books (Sahni & Gupta, 2019).

An annual $315 million in US book sales were lost to e-book piracy in 2017, according to a poll of consumers conducted by Nielsen (Digimarc & Nielsen 2019). The Global Innovation Policy Center of the Chamber of Commerce found that digital piracy had a negative effect on employment prospects in their paper titled "Effect of Digital Video Piracy on the US Economy." It has an effect on a nation's GDP (Blackburn et al., 2019). Piracy costs the United States economy between $47.5 billion and $115.3 billion annually and costs the country between 230,000 and 560,000 jobs annually. Moreover, digital piracy is estimated to cost the United States $30 billion per year. According to the data provided by a variety of industries, piracy is one of the leading contributors to the revenue decline of diverse publishing organizations.

In Nigeria, e-book piracy is widespread and garners considerable attention. Several publishing industry insiders have acknowledged that pirates have successfully gained control of between 40 and 50 percent of the industry (Ahmadu, 2018). In addition, Longman has lost between $1.5 and $2 million, or 50% of its potential annual revenue, due to book piracy (Obidiegwu, 2007). Research into book piracy in Nigeria has uncovered several factors contributing to the growth of the black market in the country, including the high cost of original books, the desire for quick financial gain, and the scarcity of original books (Ahmadu, 2018).

The circumstance in Kenya is identical. Kenya consistently expands its higher education and local publishing sectors. Nonetheless, widespread e-book piracy has decreased illiteracy rates in Kenya and elsewhere, and the publishing industry faces numerous challenges that, if not

addressed, could be detrimental to the industry. The Kenyan publishing industry faces a significant challenge in the form of electronic book piracy. Numerous Kenyans, particularly students in higher education institutions, favor counterfeit books over authentic ones. Students and teachers rely extensively on photocopying as a result of the proximity of several photocopy shops to educational institutions. This practice is damaging to the publishing sector, as millions of Kenyan shillings are wasted due to piracy and the illegal duplication of affordable editions.

NFTs, or non-fungible tokens, are digital assets that stand in for real-world things like artwork, collectibles, and in-game items. They are typically digitized with smart contracts and traded electronically with digital currencies. Because the technology is based on blockchain technology, it is suitable for uniquely identifying something or someone. Therefore, a creator can easily prove ownership, earn royalties each time a successful purchase is made, have full history traceability, have convenient interoperability, and track digital copies online. NFT technology processes the technology that e-books could use to reduce piracy.

1.2 Problem Statement

The lack of adequate techniques to protect copyright poses a significant problem in Kenya, where two out of every ten books are counterfeit, resulting in substantial financial losses for publishers and authors amounting to Ksh. 1.25 billion annually (Igesha et al., 2016). Book piracy not only deprives the government of tax revenue but also creates trade barriers for legitimate copyright businesses (Begum & Sharma, 2018). Moreover, it instills fear among aspiring authors, discouraging them from creating new works due to the imminent threat of piracy. This pervasive issue not only undermines the development and preservation of cultural heritage but also contributes to the erosion of law and order in society, tarnishing the country's international image. To address this problem, there is a need for effective techniques, such as a blockchain tool, to detect and mitigate e-book piracy. Such a tool would provide local and foreign publishers, as well as authors, with the means to protect, detect, track, and authenticate their publications, ensuring fair compensation for their creative efforts (Zhixuan Zhou et al., 2022).

1.3 General Objective

The general objective of the study is to establish a tool that detects and mitigates e-book piracy in the education sector in Kenya.

1.4 Specific Objectives

i. To identify the factors that contribute to e-book piracy.
ii. To investigate existing techniques used to detect and mitigate e-book piracy.
iii. To analyze the challenges in the existing models used in e-book piracy mitigation and prevention.
iv. To develop a prototype of a blockchain tool that detects and mitigates e-Book piracy.

1.5 Research Questions

i. What are the factors that contribute to e-book piracy?
ii. What are the existing techniques used to detect and mitigate e-book piracy?
iii. What are the challenges with existing piracy detection and prevention models?
iv. How can a blockchain tool that detects and mitigates e-book piracy be built?

1.6 Justification

Considerable efforts to find the right solution to detect and mitigate e-book piracy in Kenya have borne little fruit. Therefore, this research will be important in addressing the challenges of e- book piracy in Kenya with an NFT system that employs the beneficial characteristics of blockchain technology. The proposed solution will enable the creation of an immutable and tamper-proof record of digital content ownership and distribution. This is accomplished using smart contracts, which can be used to manage the rights and distribution of e-books securely and transparently. Furthermore, digital fingerprints or hashes can uniquely identify each digital copy of an e-book, allowing illegal copies to be tracked and traced.

Furthermore, the proposed solution will include blockchain-based payment systems for e- books, deterring piracy by making illegal copies more challenging to distribute. This is because such systems can ensure that only authorized parties can access and distribute e-books

and that payments are made to the proper copyright holders. According to Zhixuan Zhou, who conducted interviews with 15 NFT creators from 9 different countries, the positive comments revolved around the traits of NFTs. The main highlight is having proof of ownership, and a non-fungible aspect benefited the creators in gaining more followers, acquiring more funds, and protecting their work. Applying this technology to e-books will help publishers benefit from it (Zhixuan Zhou et al., 2022).

1.7 Scope and Limitations

The limitations of this research are discussed as follows. The study focused on Kenyan publishers, authors, and consumers in universities, especially at the graduate and doctoral levels. Furthermore, due to the broad reach, the findings depend on the accessibility of data regarding time and accessibility. Finally, the complexity of the architecture of this model may not allow the development of a simulation.

The research did not to cover the following problems, as they were considered outside the scope:

i. Physical book piracy detection and mitigation.
ii. Investigation of user acceptance of this model.

Chapter 2: Literature Review

2.1 Introduction

For the past decade, e-book piracy has been on the rise. The ease with which e-books can be pirated is one rationale for the increase in piracy. Because they are small digital files, compared to videos, they can be downloaded, shared, and reproduced quickly and easily. Furthermore, the high quality of digitally produced works makes it simple to make copies without sacrificing quality (Roncevic, 2019). Because pirated works are of the same quality as originals, they can be considered perfect digital reproductions.

This research discusses the empirical and theoretical literature surrounding the detection and mitigation of e-book piracy. Theoretical literature aims to give an in-depth look at the scope of e-book piracy to identify problems, actors, and processes that surround e-book piracy. At the same time, empirical literature provides the data needed to conclude the research problem. The chapter also discusses the various models and frameworks successfully applied in mitigating e-book piracy. Also, the research explores the multiple algorithms that are key in implementing e-book piracy mitigation systems. Lastly, the conceptual model summarizes how the proposed NFT- based e-book piracy detection and mitigation will work.

2.2 Empirical Literature

A digitally published book, also known as an e-book, electronic book, or e-book, can be read on electronic devices such as desktop computers, laptops, tablets, and smartphones. With the convenience of e-books, information is always within reach. Sixty percent of people polled in study conducted in the United Kingdom by the Joint Information Systems Committee (JISC, 2012) reported using e-books. The JISC survey also found that while libraries provided ebooks to 46% of respondents, 43% of respondents bought their most recent ebook online. The majority of respondents reported reading an e-book once every seven days or once every month.

It was also found that users read e-books more often for academic purposes than for leisure or education. Research by Statista (2022) indicates that e-books have gained popularity among Kenyan book readers. Twenty percent of Kenyan book readers say they read more electronic books than physical ones, and another 23 percent say they read about the same number of each. The number of self-published e-books has skyrocketed in the last decade, and with it, the demand for

e-books. Neyole (2014) researched e-book utilization among university students in two public institutions in Kenya. The research findings concluded that 71% of students and staff used e-books frequently. Statista (2022) states that the number of e-book readers is expected to amount to 4.5 million users by 2027 in Kenya.

2.2.1 Methods Employed to Reduce Piracy.

There have been substantial efforts made in recent years to combat multimedia piracy. E-books in multimedia PDFs have been the center of attention due to the large number of books shared across the internet. Qureshi & Jiménez (2022) define this process of protecting digital content as a measure to protect digital assets from unauthorized access by a user or group of users. The subsections below show the various techniques that have been widely used to address the issue of e-book piracy.

2.2.1.1 Encryption

Encryption is the process of converting plaintext messages into unreadable ciphertext, whereas decryption is the opposite procedure (Li, 2009). The following properties are anticipated to be offered by this method:

a) Confidentiality relates to only allowing authorized users to view or disclose data and preventing disclosure to unapproved parties or access.

b) Integrity is the term for safeguarding data from change or alteration, whether accidentally or knowingly.

c) Authenticity: This is the ability of the recipient of the data to identify its source.

The naive approach uses standard symmetric and asymmetric cryptographic methods to encrypt all of the media files, such as the Advanced Encryption Standard (AES), Rivest Cipher (RC5), Digital Signature Algorithm (DSA), and Rivest-Shamir-Adleman (RSA). Encryption has been applied heavily in mitigating e-book piracy by restricting access to a resource to only the user with the decryption key. (Chi et al., 2020) combined encryption with blockchain to securely deliver

downloaded content to the authorized. One of the significant benefits of encryption is that it guarantees the confidentiality and integrity of the data. However, security is still an issue since anyone with the decryption key can easily unlock the content.

2.2.1.2 Digital Rights Management (DRM)

Digital rights management (DRM) systems were created to restrict users' abilities to copy, print, or otherwise modify digital content once it has been supplied to them (Qureshi & Jiménez, 2022). A digital rights management (DRM) system will typically include tools for content protection, right creation, right enforcement, user identification, and usage monitoring.

Typically, a DRM framework involves the following three entities: the user, the licensed provider, and the content provider. In addition to managing encryption keys, the content provider also monitors production licenses. Instead, the license provider is responsible for issuing authorizations and keeping track of encryption keys for all content (DRM agents run on user's computers and determine who is authorized to access downloaded content). Digital rights management has been used to ensure that only the original purchaser of an E-book can read it. Digital rights management (DRM) has been shown to be effective at tracing content back to its rightful owner, which deters users from passing off copied works as their own and engaging in illegal file sharing. However, no mechanisms are provided to prevent the content from being illegally redistributed. A common DRM system architecture is shown in Figure 2.1.

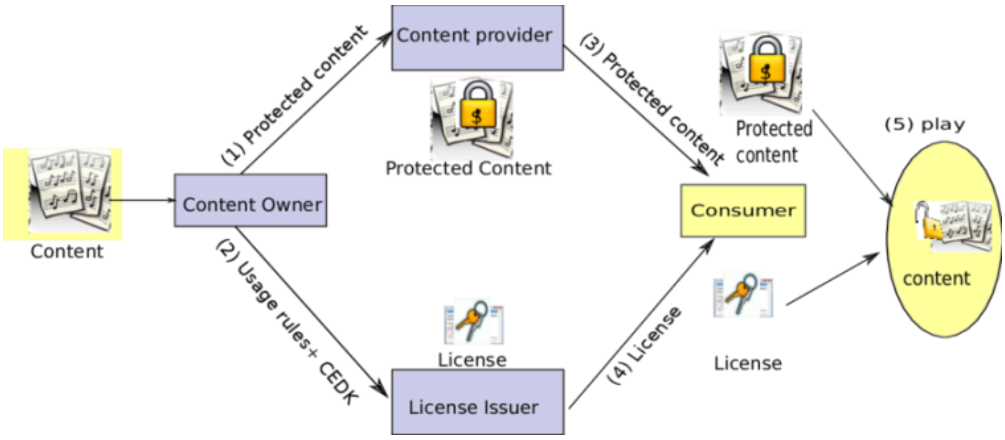

Figure 2.1: A Typical DRM System Architecture

(Gaber, 2013)

2.2.1.3 Digital Watermarking

When authorized users decrypt multimedia content, digital watermarking offers post-decryption security. By obscuring the identification data (watermark) in the original material (host signal), it subtly modifies it. The legitimacy of the carrier signal can later be confirmed, and ownership can be established using this information.

The first two steps of a digital watermarking system are watermark embedding and extracting. When making a watermarked password, the embedding process is used to add a watermark to the host signal. In contrast, the watermark is taken out of the altered or modified signal using the extraction algorithm. If the movement did not alter during transmission, the watermark remains and can be deleted. Unlike watermark detection, watermark extraction can show ownership. Throughout the embedding and extraction processes, a secret key is employed to prevent unauthorized access to the watermark (Qureshi & Jiménez, 2021).

Digital watermarking has been utilized successfully in numerous applications, including copyright protection, transaction tracking, content authentication, broadcast monitoring, copy control, device management, and heritage enhancement. Few watermarking techniques presented recently throughout the range of applications concentrate on creating watermarked audio and video content. Digital watermarking has a glaring flow with security. Malicious attackers or intentional attackers can detect the existence of embedded watermarks and extract or remove them. This is against the principle of allowing only authorized parties to access the watermark.

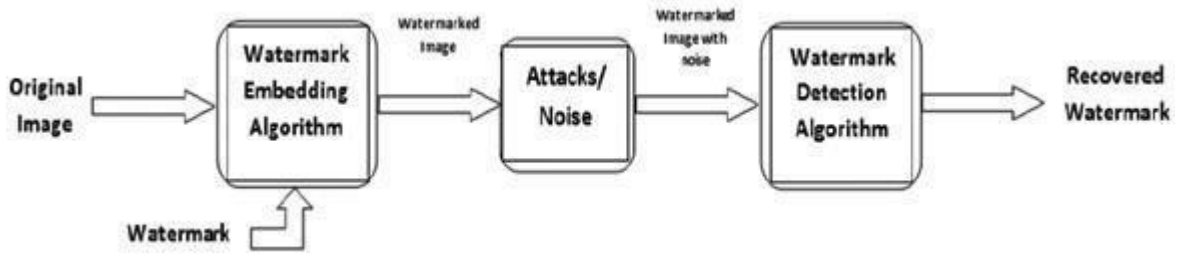

Figure 2.2: Stages of Digital Watermarking

(Kumar, 2016)

2.2.1.4 Multimedia Fingerprinting

Once an illegal copy has been found, the pirates can be tracked down using multimedia fingerprinting. For content to be traceable, a user-specific identifier, or fingerprint, is appended to multiple copies of the same file (Qureshi & Jiménez, 2022). Multimedia fingerprinting algorithms are a three-stage process that establishes a connection between the client and the content owner, allowing the latter to trace pirates using copies that were either stolen or obtained through coercion. Digital fingerprinting may be able to detect a single attacker, but a gang of dishonest customers can conduct catastrophic collusion strikes against the fingerprinting system. By comparing their versions, the colluders can try to pinpoint the spots that are transmitting the fingerprint signal, delete the relevant data, and then create a copy that cannot be linked to the originals.

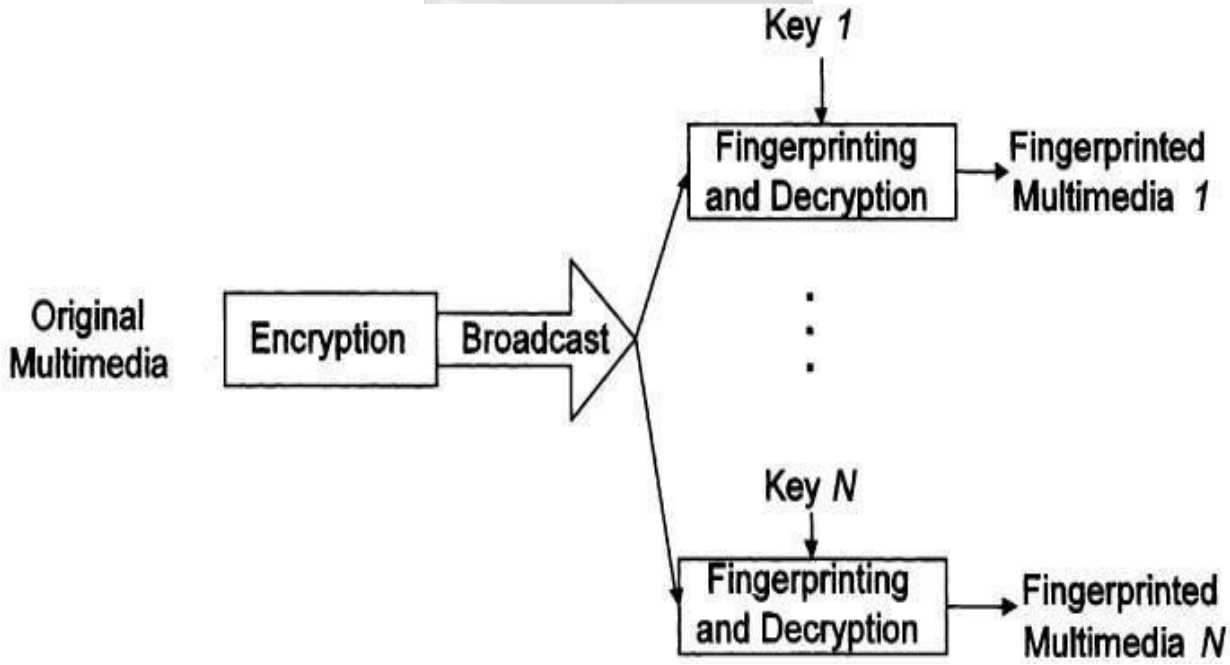

Figure 2.3: Overview of Multimedia Fingerprinting

(Luh & Kundur, n.d.)

Table 2.1: Summary of the methods employed to counter e-book piracy

Author	Method	Advantages	Limitations
Chi et al. (2020)	Encryption	- This method ensures the privacy, security, and originality of the digital books. - Lacks validation of the author	- Security is still an issue since anyone with the decryption key can easily unlock the content.
Qureshi & Jiménez (2019)	Digital Rights Management	- Powerful in revealing the rightful proprietor of a piece of content, which deters others from passing it off as their own and illegally disseminating or sharing it with others.	- It does not provide mechanisms for restricting the illegal redistribution of the content.
Qureshi & Jiménez (2019)	Digital Watermarking	-Suitable for identifying and verifying ownership of the content.	- Digital watermarking has an obvious correlation to security. Intentional or malicious attacks can detect the presence of embedded watermarks and extract or remove them.
Qureshi & Jiménez (2019)	Multimedia Fingerprinting	- Upon discovering an unlawful copy, multimedia fingerprinting can easily identify the pirates.	- Several unscrupulous buyers could band together to conduct potent collusion attacks against the fingerprinting system.

2.2.2 Blockchain Technologies in Piracy Mitigation

Both industry and academia have recently started looking into how they can use blockchain technology to better safeguard intellectual property. Data integrity, authenticity, tracing of piracy, and transparency are just some of the copyright protection issues that blockchain can solve, according to recent studies, along with the need for certificates attesting to ownership of the rights to the content in question and other similar issues. The following section provides a summary of the current blockchain-based piracy mitigation solutions and the key features and implementation details of each.

To protect the privacy and agency of its users, Vishwa & Hussain (2018) proposed a decentralized data management framework. Using blockchain technology, they proposed a protocol to seize control of the user's information. The user can manage his own media files with this protocol, eliminating the need to rely on an external source. The user can utilize the framework for data archiving, querying, sharing, and auditing. While there have been some encouraging developments in this system, it does not yet prevent the illegal copying of content, which is consistent with the findings of many other studies on the subject.

In their paper, Chi et al (2020) presented a secure and reliable blockchain-based real-time e-book market system, that allows users to publish autonomously and receive payment directly from readers, bypassing the need for a trusted third party. Blockchain was used in this research because it is a secure and efficient way to manage online payments and to maintain ownership rights to premium content. It provides several benefits, including the ability to confirm ownership of an e-book, the security of user information, the assurance that the buyer is who they say they are, the authenticity of the E-purchaser, the authenticity of the E-contents, the verifiability of direct payment transactions, and the prevention of e-book piracy and illegal distribution. Using elliptic curve cryptography, a book repository stores both the encrypted contents of published e-books and the book key. The proposed solution safeguards the confidentiality of e-book content by limiting access to it to verified buyers only. As a result of the consumer's ability to verify the authenticity of the e-book content prior to making a purchase, authors are also deterred from posting subpar content. Therefore, the proposed solution safeguards both the e-books and the rights of their buyers and authors. Yet, it can be difficult to gauge a book's and author's credibility, which may discourage honest writers from putting their works out there.

Peng et al (2019) presented an Ethereum-based digital copyright management system to facilitate direct interactions between content producers and consumers. Digital watermarking, ElGamal cryptography, a perceptual hash function, the smart contract, and IPFS are a just few of the technologies incorporated into the proposed system. According to the research, all the data that is supplied to the blockchain could benefit from being stored in a data lake, an off-chain centralized storage option. To protect user privacy and maintain data integrity, all data stored in the data lake is digitally signed and encrypted at rest. To ensure that only authorized parties have access to the stored data, the majority of nodes validate digital signatures and permissions. Users can rest assured that their information will remain private and under their control thanks to the decentralized data management framework. However, this is still just a proof of concept and hasn't been tried out in the real world. Since all media is encrypted with ElGamal, the method incurs a considerable additional burden. Both memory and processing power are heavily utilized.

P2P blockchain-based content distribution was proposed by Qureshi and Jiménez (2022). The proposed method employs the Inter Planetary File System (IPFS), a perceptual hash function, homomorphic and symmetric encryption schemes, a perceptual hash function for content authentication, a smart contract built on Ethereum for atomic payments, and collusion-resistant fingerprinting to ensure security. The proposed architecture considers the anonymity and security concerns of a fingerprinting protocol in a decentralized setting. However, this is just a proof of concept and has not been built and tested in the real world.

Table 2.1 compares various systems and applications developed using blockchain technology to help mitigate e-book piracy. The comparison is based on transaction types, a data automation approach, crypto currency, and content protection methods. The limitations of the systems are also highlighted to inform the reader of the gaps present in the current systems.

Table 2.2: Comparison of Existing Studies on E-book Mitigation

Author	Types of Transactions	Data Automation	Cryptocurrency	Content Protection Techniques	Limitations
Chie et al. (2030)	Hybrid	----	Customized coin	ECC-based Encryption	- It's platform dependent. - Lacks validation of the author
Mangipudi et al. (2019)	Hybrid	Smart Contract	Bitcoin	Watermarking	- Data can be easily compromised. - It is easy to copy and distribute books.
Peng et al. (2019)	Hybrid	dApp	Ethereum	Encryption and Watermarking	- Once the decryption key is obtained, the content cannot be protected from misuse or illegal Redistribution.
Qureshi & Jiménez (2019)	Hybrid	Smart Contract	Ethereum	Fingerprinting	- Data can be easily compromised - It is easy to copy and distribute books.
Qureshi & Jiménez (2019)	Hybrid	dApp	Ethereum	Encryption	-Data can be easily compromised. - It is easy to copy and distribute books.

2.3 Theoretical Literature

2.3.1 E-book Piracy

Creating and distributing copies of phonograms, books, music, paintings, architectural drawings, films, broadcasts, computer software, and other works for financial gain without the owner's consent is considered piracy. To "pirate" an electronic book means to steal a copy of it without the author's permission and distribute it online, either for free or for profit.

The following are entitled to copyright, as stated in the provisions of Section 22 of the Kenyan Copyright Act (2001): The written word, the sonic arts, the moving image, the recorded word, and the broadcast sphere all fall under this category (Kecobo 2020). This section details the various types of works that are protected by copyright law in Kenya, such as books, magazines, and scholarly articles. Without the permission of the authors, society can still gain access to knowledge and be rewarded for creative endeavors through the limited use of copyright-protected works. Among the statutory exemptions are research, private use, criticism or review, and news reporting (Kecobo 2020). The originator must recognize the restrictions.

2.3.2 Factors that Contribute to E-book Piracy in Kenya

Piracy is a major deterrent to creative output in any country. Sales in the publishing and book industries suffer as a result. According to Ahmadu's article, there is widespread piracy of books across a variety of genres, including those with educational, religious, commercial, recreational, and scholarly value. However, textbooks and other school-related materials are the most frequently pirated books, while novels, poetry collections, and dictionaries are the least (Ahmadu, 2018).

E-book piracy in developing countries like Nigeria is caused by a number of factors, including the high cost of books relative to average income, a lack of publishing materials like paper, machinery, ink, etc., and the immaturity of the publishing industry, which has led to an excessive reliance on the industrialized publishing sector to meet developing countries' educational and research needs (Nkiko, 2013).

Moreover, in Kenya, e-book piracy mainly occurs in primary, secondary, and tertiary institutions because local demands aren't satisfied. For instance, local readers need affordable books; taxes on purchases of (course) books need The limitations of the systems are also

highlighted to inform the reader of the gaps present in the current systems. to be reduced, and the government should opt to supply learning institutions with books. The supply side/publishers and authors have a challenge with technology. Because of the increased production due to the expanded market, the government misses checks that seal loopholes for counterfeits or copyright. Also, there is the challenge of misinformation and training on copyright and professionalism that contribute to piracy and corruption (Igesha et al., 2016).

2.3.3 Impacts of E-book Piracy

Piracy has grown considerably easier with the advancement of technology. In the past, people would photocopy books or journals and share them using the available transport media, such as water transport. Book prices dropped because shipping via sea was more cost-effective than alternative methods of transport. The internet's development has made it the quickest and most convenient method of communication. Many academic resources, including books, journals, papers, and research works, can be obtained without cost by scholars, but some of this information may be pirated. The limitations of the systems are also highlighted to inform the reader of the gaps present in the current systems. Today's readers are all about efficiency, so they look for ways to cut corners when gathering information. People like getting books on the internet to save time that would have otherwise been used to search for books in the market.

The impacts of e-book piracy on readers are; books have poor binding and print quality; some text is illegible and unfriendly to learners; some old editions are crammed into the supposed new edition (Mwale, 2022); when downloading on pirating sites, it may come with malware that corrupts devices; and last and importantly, the website/person giving off the free book can hack your machines and access your sensitive data, which is very dangerous (Roy, 2015). For publishing companies and authors, it increases unemployment; lowers income for the organization and author; lastly, discourages creativity. To the government, it denies revenue and reduces the nation's GDP.

2.4 Models and Frameworks for Detecting and Mitigating E-book Piracy

2.4.1 Content Distribution Framework

Li et al (2010) developed a content distribution framework for P2P networks that includes digital rights management (DRM). Using a network coding approach based on Lagrange polynomial interpolation ensured the security of the material's dissemination. A network peer that downloads sufficient coded bits not only reconstructs the related blocks using a finite field Gaussian elimination approach, but also makes copies of the coded bits contained inside these blocks, which it subsequently distributes to the other network peers. The distribution expense on the music source is significantly decreased, and the number of coded pieces within the network is significantly increased, hence eliminating the "last piece problem" that affects typical P2P systems.

The Digital Rights Management (DRM) subsystem generates an individual's digital fingerprint via the RSA public-key cryptosystem. A fingerprint is covertly embedded in the music file so that the music supplier may identify anyone who is involved in unlawful file sharing. The testing results verified the validity of the suggested system, demonstrating its capability to securely distribute enormous volumes of copyright-protected music content with no audible quality degradation.

Potentially more beneficial to users and content owners than monopoly platform offerings is the proposed digital content service model. By implementing the proposed solution, creators of digital media can license their work and recoup distribution costs without having to pay a cut to middlemen. Owners can promote their content in a number of different ways using the proposed system. For example, they may offer versions of their digital content that are restricted to a specific time frame, device, or transferable license number. The lack of middlemen will also benefit the users. Due to its self-decrypting encrypted format, this framework adds unnecessary friction to the process of transferring and storing digital data. There must be a reduction in these costs and an empirical evaluation of the content distribution framework proposed to safeguard digital content's intellectual property rights.

2.4.2 Hawk Framework

Kosba et al (2016) proposed the Hawk framework for preserving smart contracts of cryptography and privacy. A unique party known as the manager facilitates the implementation of Hawk contracts. The manager can access user input and keeps users' private information confidential. However, the manager is not to be compared to a reliable third party; even if the manager colludes with the parties or deviates from the procedure, this will not affect how the contract will be carried out. If a manager abandons the protocol, they risk financial penalties, and users are compensated as a result. Figure 2.3 shows the overview of the Hawk framework.

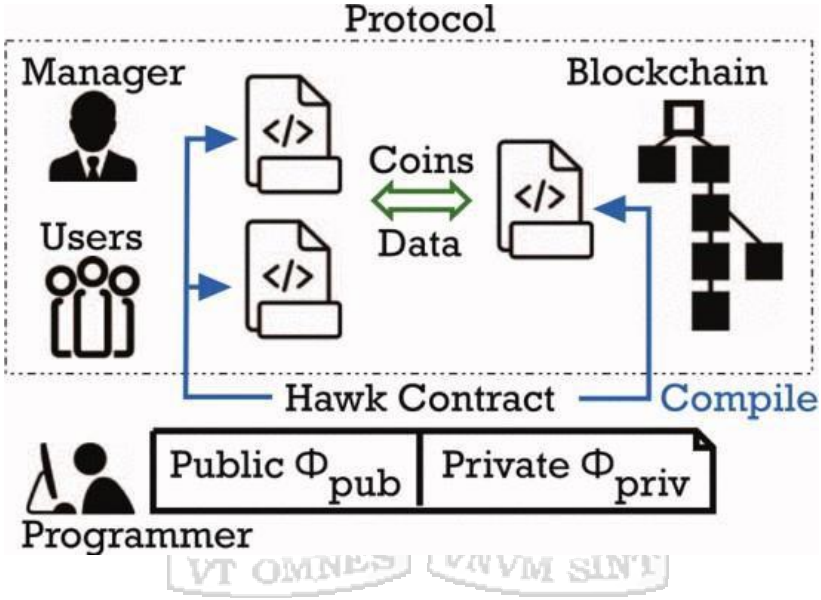

Figure 2.4: Overview of Hawk Framework

(Kosba et al.,2016)

Table 2.3: Models and frameworks developed to detect and mitigate e-book piracy

Author	Method	Advantages	Limitations
(Li et al., 2020)	Content Distribution Framework	- Allows the content owner to control how and where the content is distributed, making unauthorized copies more challenging to obtain and distribute. -Lacks validation of the author. - It protects the content during delivery with encryption and digital rights management (DRM) technologies, making it difficult for pirates to intercept and copy the content.	- Implementing and managing large and complex content distribution networks can be difficult.
(Kosba et al., 2019)	Hawk Framework	- To protect software applications from unauthorized access, Hawk Framework employs a combination of encryption and authentication. As a result, it is more difficult for pirates to crack the software and gain access to it without a valid license. - Hawk Framework is easily updated to adapt to new threats or changes in the software landscape, ensuring its effectiveness in preventing piracy.	- Hawk Framework can occasionally generate false alarms, such as labeling a licensed user as a pirate, which can cause the user inconvenience.

2.5 Architectures and Designs

There have been various architectures and designs that multiple researchers have used to design the mechanism to curb piracy, from e-books to a wide range of other applications.

2.5.1 Authorization Mechanism Based on Blockchain Architecture

Wang et al (2021) proposed a system architecture that allows traceability and authorization mechanisms for digital content. The architecture involves six parties, which are the: museum (M), Content Administrator (CM), Blockchain Center (BCC), Proxy (P), and Bank (B).

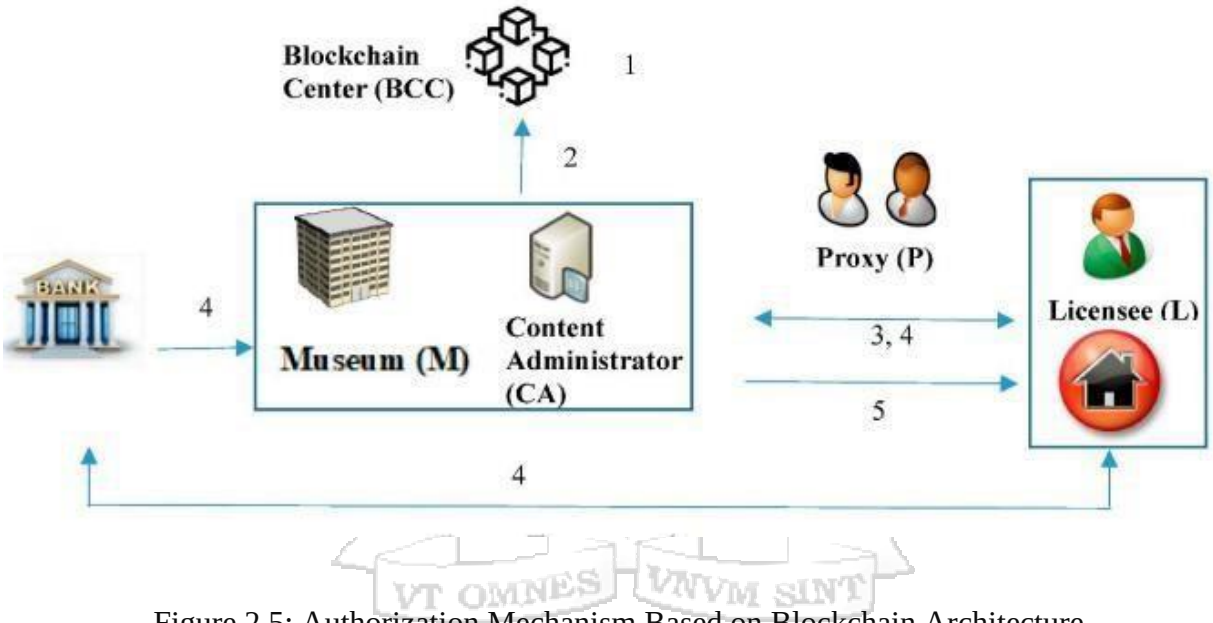

Figure 2.5: Authorization Mechanism Based on Blockchain Architecture

(Wang et al., 2021)

a) Museum (M): The content is owned by the museum. The museum is responsible for the collection of cultural artifacts as well as the creation and administration of the museum's digital material repository. The museum has organized and protected its digital content resources.

The CA is the cloud platform for the museum. It is responsible for analyzing the licensee's request to determine whether to "grant" access to the digital content resource.

c) Licensee (L): Individuals or organizations that wish to use the museum's digital content resource are required to pay a fee to the museum. This facility monitors the licensee's access information to the digital rights resource. The BCC accepts the parties' registration and provides

them with a pair of public and private keys as well as an identity certificate.

The proxy is a museum department. After CA verifies the licensee's identity, P supervises the cloud and grants the licensee access to the museum's digital content resource.

f) Bank (B): Bank has been authorized by a licensee to donate to the museum. The subsequent steps briefly illustrate the possibilities.

The proposed design utilizes distributed ledger technology. During the authentication and authorization process, a few essential pieces of data are stored and confirmed on the blockchain. The smart contract specifies the essential data in the blockchain. The smart contract structure of the proposed scheme is depicted in Figure 2.5.

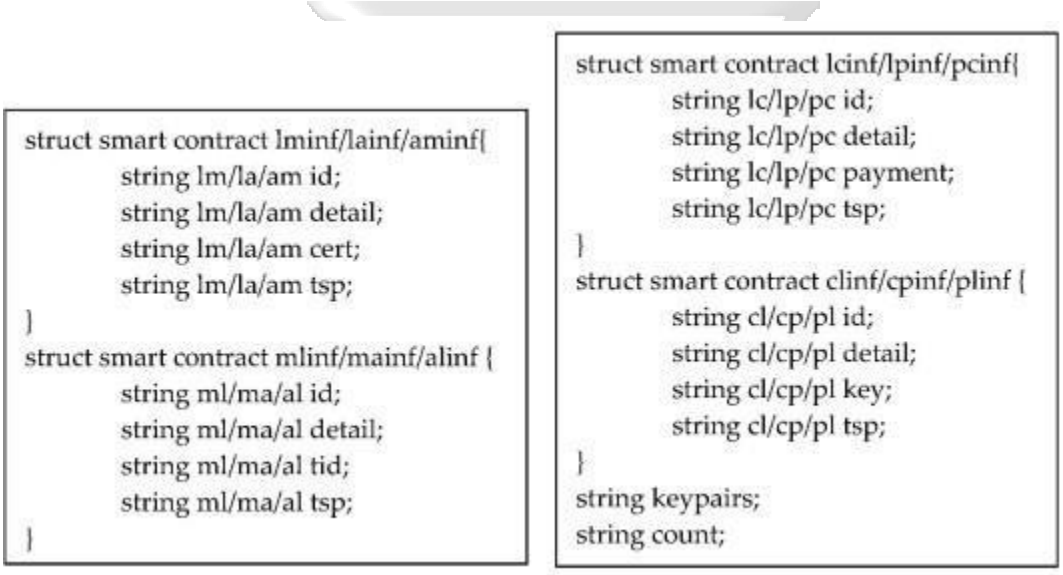

Figure 2.6: Smart Contract Overview

(Wang et al., 2021)

They generated key information that was stored in the Blockchain as part of the proposed smart contract. For the lm/la/am smart contract, they developed the id (identity), txn det, csr, and ts fields. During the setup phase, the blockchain hub also generates the public and private key pairs for each function. The major drawback of this architecture is its inability to deal with the illegal copying of content.

2.5.2 P2P DRM Architecture

The P2P DRM platform architecture proposed by Li et al (2010) consists of a master node (MP) and one or more peers. A program is executed on a secure system by each peer. The program enables content sharing and includes DRM protection in the files being shared. The proposed framework included three stages—distribution, FP generation, and FP embedding, protection, and checking—to make P2P DRM file sharing possible. Legal owners of content copies still have access to the master copy, so this architecture is only useful for tracing the movement of pirated materials, not stopping them from being distributed illegally.

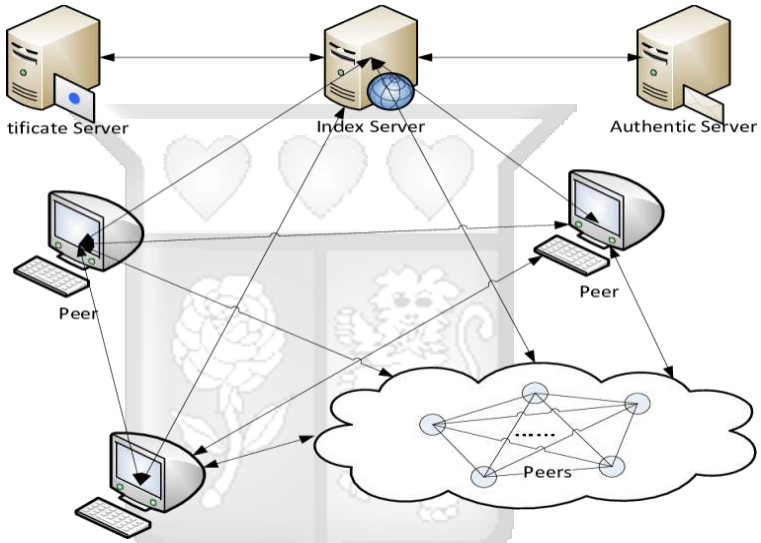

Figure 2.7: P2P Architecture
(Li et al., 2010)

There are a few drawbacks to DRM architecture. Even though the intended function of digital rights management (DRM) software is to prevent copying, some e-books are easily downloadable by unauthorized users. Further, screenshots of a DRM-protected book can be converted back to text using the same methods. Finally, it is possible to retype a publication that has been protected with DRM.

2.5.3 Scale Invariant Feature Transform (SIFT) Architecture

Srinivas et al (2012) Proposed a robust, efficient architecture for detecting software piracy. Simplified Invariant Feature Transform (SIFT) features are features extracted from images

to facilitate trustworthy matching between multiple perspectives of the same object. The extracted features are robust and unique to the image, regardless of scale or orientation. Figure 2.7 shows the architecture of the antipiracy software system. This architecture relies on the SIFT algorithm, which is known to be slow in operation and ineffective for low-powered devices.

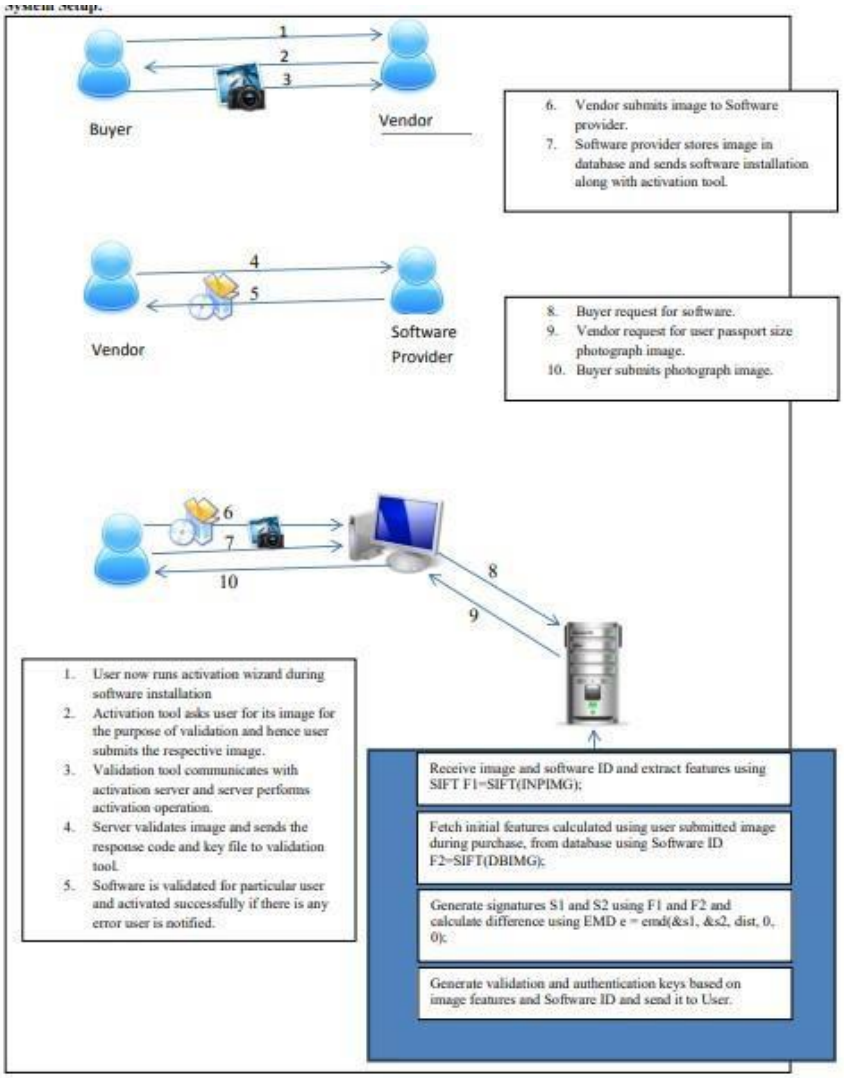

Figure 2.8: Overview of The Antipiracy Architecture

(Srinivas et al., 2012)

2.5.4 RobP2P Architecture

RobP2P, as presented by Elgazzar et al. (2013), is a reliable framework for building mobile P2P networks and efficiently managing their state. RobP2P is innovative because it presents a

protocol for selecting "super-peers" based on an aggregate utility function that takes into account the abilities and environments of the peers in question. Additionally, it provides a flexible plan by which super-peers can delegate authority to new or existing peers who are more capable of handling the workload. The simulation results demonstrated RobP2P's efficacy, resilience, and low-overhead traffic generation, all while preserving the integrity of the network's consistent state.

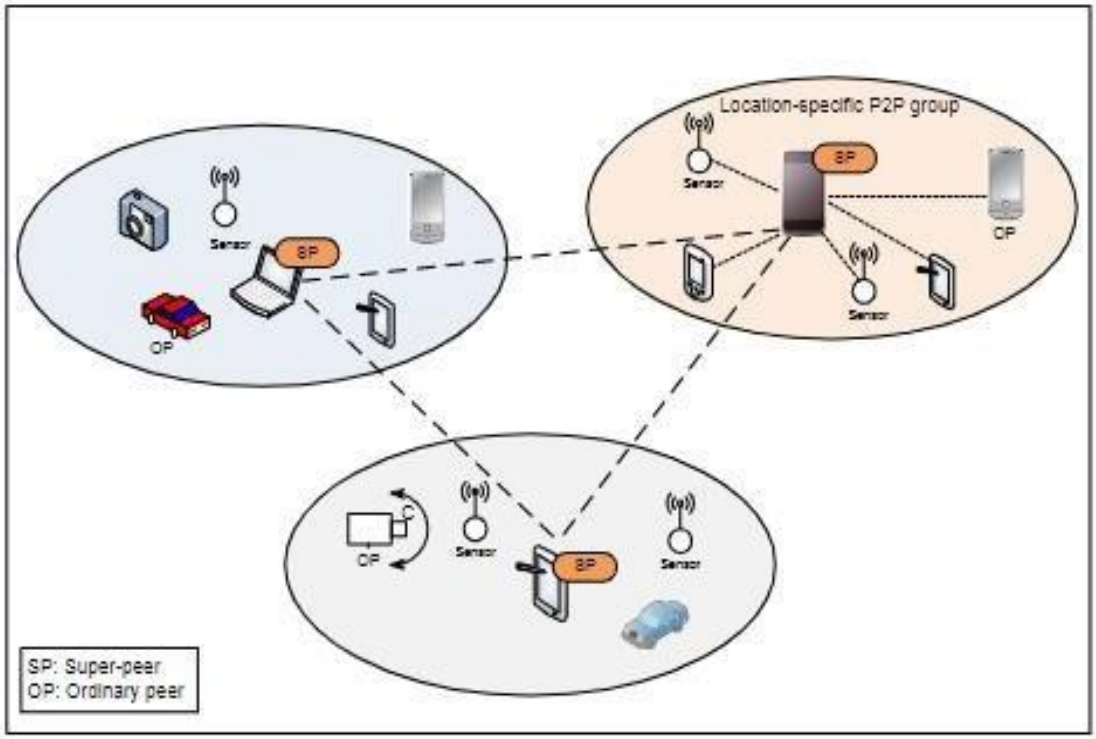

Figure 2.9: RobP2P Architecture

(Elgazzar et al., 2013)

Table 2.4: Architectures and designs adopted for e-book piracy detection and mitigation.

Author	Architecture	Advantages	Limitations
(Wang et al., 2021)	Authorization Mechanism Based on Blockchain Architecture	- Once the data for the book has been recorded, it cannot be changed or deleted, making it difficult for pirates to tamper with the record of ownership or distribution of the e- books. - Allows for a transparent record of all transactions, making it possible to trace the origin and distribution of digital assets.	- Struggles with high transaction volume and may be unable to handle the large number of transactions required for global digital asset distribution.
(Li et al., 2010)	P2P DRM architecture.	- Can handle many users and transactions, allowing for global distribution and protection of e- books.	- P2P networks rely on users to enforce copyright protections, which can limit copyright holders' ability to control the distribution and use of their content. - Different P2P networks may be unable to communicate with one another, posing challenges in tracking and enforcing copyright across multiple platforms.

Table 2.4: (continued).

(Srinivas et al., 2012)	Scale Invariant Feature Transform	- SIFT is resistant to changes in image scale, rotation, and viewpoint, allowing it to detect and prevent piracy even when the pirated copies differ from the original image. -SIFT can detect and prevent text and image piracy, making it a versatile tool for e-book protection.	- SIFT is an image-based algorithm, so it may not detect piracy in text-based e-books.
(Elgazzar et al., 2013)	RobP2P Architecture	- RobP2P reliably preserves network consistency with less overhead traffic and lower failure susceptibility.	- The architecture is vulnerable to hacking and other cyber-attacks, which could give pirates unauthorized access to e-books. - P2P networks may use a proprietary format to share e- books, which may not be compatible with other formats.

2.6 Algorithms

2.6.1 Elliptic Curve Digital Signature Algorithm (ECDSA)

Using Elliptic Curve Cryptography, the Elliptic Curve Digital Signature Algorithm (ECDSA) mimics the Digital Signature Algorithm (DSA) (ECC). The equation used in public key cryptography is very efficient (PKC). ECDSA is used in many different kinds of security systems and messaging apps, and it serves as the basis for Bitcoin's security.

TLS (Transport Layer Security), the successor to SSL, uses ECDSA to encrypt data sent between browsers and servers (SSL). The browser's display of a physical padlock indicates that

an encrypted connection has been established to the website in question using signed certificates issued with the ECDSA algorithm. The security provided by ECDSA is superior to that of RSA, despite the fact that its key lengths are shorter. A major distinction between the two algorithms is this; ECDSA was adopted by (Chi et al., 2020) when designing their e-book blockchain transaction system. The algorithm proved effective when combined with other digital protection mechanisms, such as watermarking. On the flip side, ECDSA lacks a security mechanism and can collapse the entire cryptosystem once the private key is leaked.

2.6.2 Douglas Peucker Algorithm

In order to protect against piracy, Ren et al. (2021) compressed data using the Douglas Peucker algorithm. This simplified Douglas-Peucker algorithm is depicted graphically in Figure 2.9. It's easy to calculate the distance from the starting and ending points of the curve to the line if you follow this simple procedure: (a) Draw a straight line between the two points. (b) Select the highest value and use it as the threshold. If more than one point exceeds the threshold, the one furthest from the line is retained. Otherwise, the points between the line's beginning and end will be rounded down, leaving only point four. To round off the remaining points, step (c) divides the known curve into two halves based on the reserved points and repeats steps (a) and (b) until no more points require rounding. Finally, the coordinates of the points along the curve that are accurate enough are found.

Compressed watermarks embedded in e-books to prevent piracy are generated by the Douglas Peucker algorithm, which is essential in the construction of zero watermarks. The watermark's robustness against attacks is enhanced, and the algorithm guarantees that watermark features are evenly distributed in space. Vector map data can also be compressed more tightly using this algorithm. Self-intersections along the recursive refinements of polylines encountered during compression severely hamper the effectiveness of this algorithm. The algorithm is also rather complicated, making it difficult to put into practice.

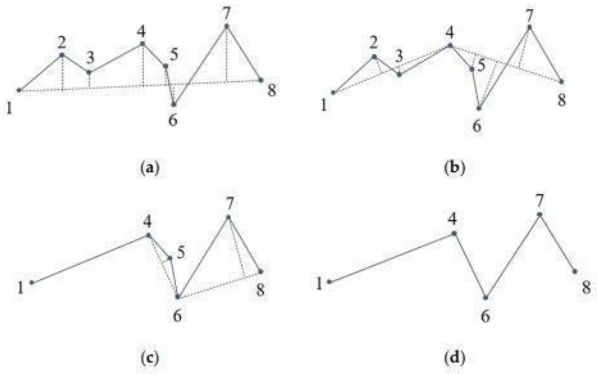

Figure 2.10: Douglas Peucker Algorithm Architecture

(Ren et al., 2021)

2.6.3 Zero Watermarking Algorithm

Watermarking algorithms have been used to protect digital assets on many occasions; proposed a way of embedding watermarking algorithms in digital content to protect it against piracy. The algorithm includes three steps: decomposing the cover image, embedding, and extraction. Figure 2.1 shows the overview of the watermarking algorithm.

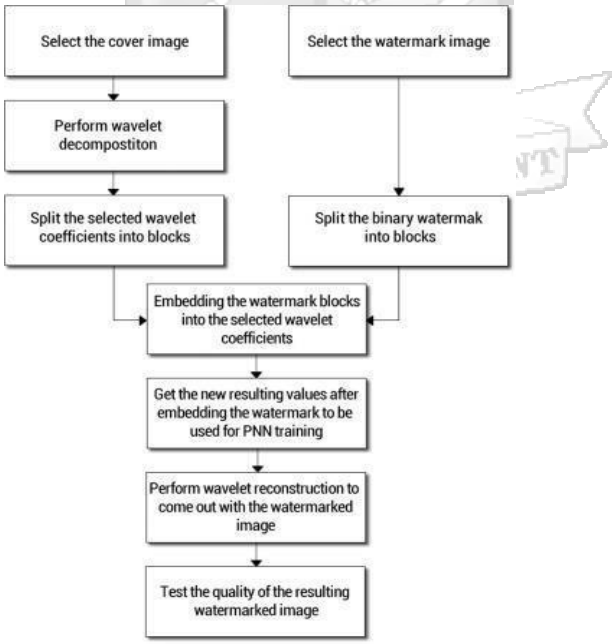

Figure 2.11: Watermarking Algorithm

(AL-Nabhani et al., 2015)

The original cover image is subjected to three layers of wavelet decomposition using the Haar filter wavelet technique. The Haar wavelet is renowned for its ease of use and calculation speed (AL-Nabhani et al., 2015). The DWT's two complementary filters split the signal into two signals—approximation and details. This procedure is known as analysis or decomposition. There won't be any information loss when the parts are put together to create the original signal. Reconstruction, or synthesis, is the name given to this. The underlying concept behind the usage of wavelets for picture watermarking is to carry out an analysis according to scale and time (ALNabhani et al., 2015).

Watermarking images with DWT is the simplest and most efficient method, as stated by Lin et al (2020). The most important part of DWT embedding, however, is selecting the DWT coefficients to be used and the location within those coefficients to embed the watermark. This algorithm has been applied in some of the studies successfully. It allows the detection of original content by embedding the watermark. However, illegal content distribution is a big challenge when using this algorithm alone because of its inability to exclusively protect the content from being copied.

2.6.4 Artificial Neural Network

The Study of the brain and nervous system serves as inspiration for artificial neural networks (Walczak & Cerpa, 2005). These networks mimic biological neural networks but use a more condensed set of ideas from brain systems. Specifically, ANN models are inspired by the way in which nerve and brain cells generate electrical impulses. Processing elements, also called neuronor or perceptrons, are the connecting pieces between various processors. Layers or vectors of neuron are typically used, with the output of one layer feeding into the input of the next layer, and so on. It is possible to model the synaptic connections between neurons in the brain by having a neuron communicate with all of the neurons in the layer below it, or with a subset of the neurons in that layer.

By simulating the electrical excitation of a nerve cell upon entering a neurode, weighted data signals are able to represent the movement of data within a network or the brain. As input

values are passed through a processing element, they are multiplied by a connection weight, wn,m, that is meant to mimic the strengthening of neural connections in the brain. To mimic the learning process, ANNs adjust the "weights" of their connections (Walczak & Cerpa, 2005). Artificial neural networks have been instrumental in improving the performance of conventional watermarking methods by learning the association between the watermark and the watermarked image (AL-Nabhani et al., 2015). Because of the many nodes that make up an ANN, a sizable amount of computing power is needed to train one. Furthermore, ANNs can overfit a smaller dataset, so large datasets are required for optimal performance.

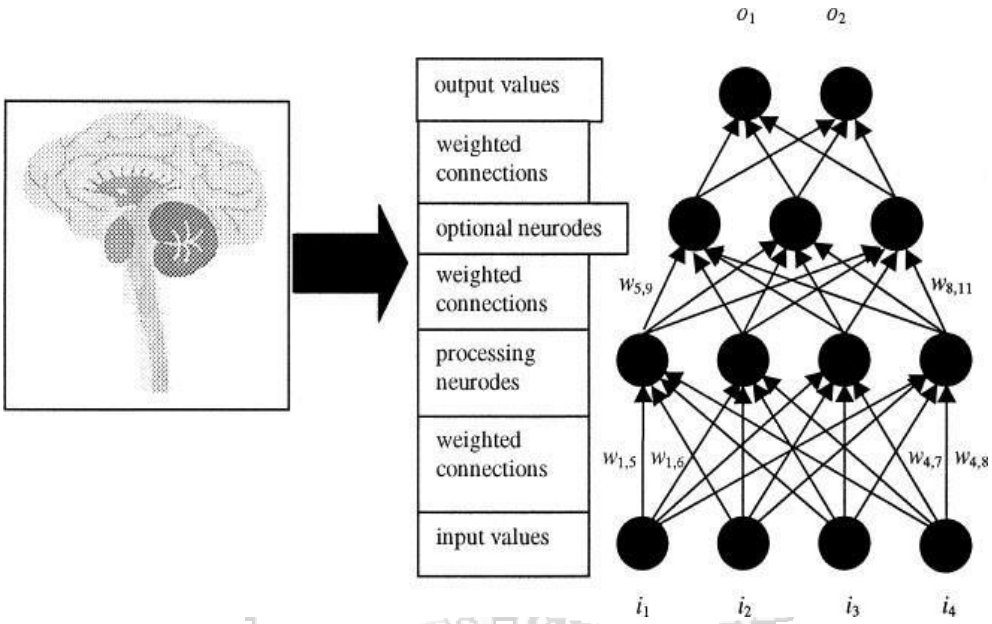

Figure 2.12: Artificial Neural Network Architecture

(Walczak & Cerpa, 2005)

Table 2.5: Architectures and designs adopted for e-book piracy detection and mitigation

Author	Algorithm	Advantages	Limitations
(Chi et al., 2020)	Elliptic Curve Digital Signature Algorithm (ECDSA)	- ECDSA ensures that digital signatures are secure, making it difficult for pirates to forge or tamper with them. - Because ECDSA is a computationally efficient algorithm, it can quickly create and verify digital signatures, making it useful for e-book piracy prevention and detection.	- ECDSA can only create digital signatures and cannot encrypt or decrypt the content, so other methods must be used to protect e-books from unauthorized access. - To create and verify digital signatures, ECDSA requires a public-private key pair, which necessitates a secure method of storing and managing the private key.
(Ren et al., 2021)	Douglas Peucker Algorithm.	- The Douglas Peucker Algorithm can simplify large datasets of points, which could help detect patterns in large e- book datasets.	- The algorithm cannot detect the exact copy of a document but rather simplifies a dataset, so it cannot identify the precise replica of a document. Still, it can detect if a document is similar to other documents.

Table 2.5: (continued).

(AL-Nabhani et al., 2015)	Zero Watermarking Algorithm	- Because the watermark is not visible to the naked eye, it does not affect the visual quality of the e-book, making it less likely that pirates will notice it. - Zero watermarking techniques are resistant to standard image processing operations such as cropping, scaling, and rotation, making it more difficult for pirates to remove or alter the watermark.	- Zero watermarking can be used to detect piracy, but it cannot prevent it. Pirates can remove or alter the watermark if the detection key is compromised, rendering it ineffective.
(AL-Nabhani et al., 2015).	Artificial Neural Network	- ANNs can process various types of data, including text, images, and audio, making them suitable for detecting e-book piracy.	- Although ANNs can detect piracy, they cannot prevent it.

2.6 Blockchain tool to Mitigate E-book Piracy

The blockchain tool designed to detect and mitigate e-book piracy uses smart contracts to streamline the publishing process for authors and consumers, as well as to provide robust

measures to prevent piracy. The following is a comprehensive explanation of how the tool works. Authors can publish their books using smart contracts, which are self-executing agreements that automatically enforce the terms and conditions specified by the authors. These contracts contain vital information including copyright ownership, licensing terms, and distribution regulations.

Every published book, along with details such as its author and publication date, are recorded on the blockchain. The immutability of the blockchain ensures that once information has been registered, it remains secure and unaltered. This establishes a transparent record of the book's existence and ownership, with no space for tampering. To authenticate an author's work, the blockchain instrument uses cryptographic techniques. By registering their books on the blockchain, authors establish proof of ownership and the precise time of creation, thereby bolstering their claims to copyright. This authentication mechanism serves as a deterrent to potential pirates, who will consider twice before infringing on copyrighted content.

The ability to provide traceability and accountability is a significant advantage of this blockchain-based utility. Due to the immutability of the blockchain, it is possible to trace the entire voyage of a book, from its initial publication to its subsequent transactions. This traceability facilitates the identification of any attempts at unauthorized distribution or piracy, making it simpler to hold responsible parties accountable. The developed tool offers several advantages over alternative methods of preventing piracy. Its utilization of smart contracts facilitates the publication process, ensuring clarity and adherence to the author's terms. The immutable and transparent record on the blockchain strengthens copyright protection and demonstrates ownership. Traceability and accountability provided by the blockchain tool serve as potent deterrents against piracy, making it the superior method for protecting authors and their creative works.

2.7 Conceptual Model

The components of the proposed NFT-based e-book transaction system are the user, service application, e-book content, digital coin, NFT, book repository, and P2P network. Users, who can be either writers or readers, have access to the system's services only via the service application, which is tailored software that executes the steps outlined in the proposed method

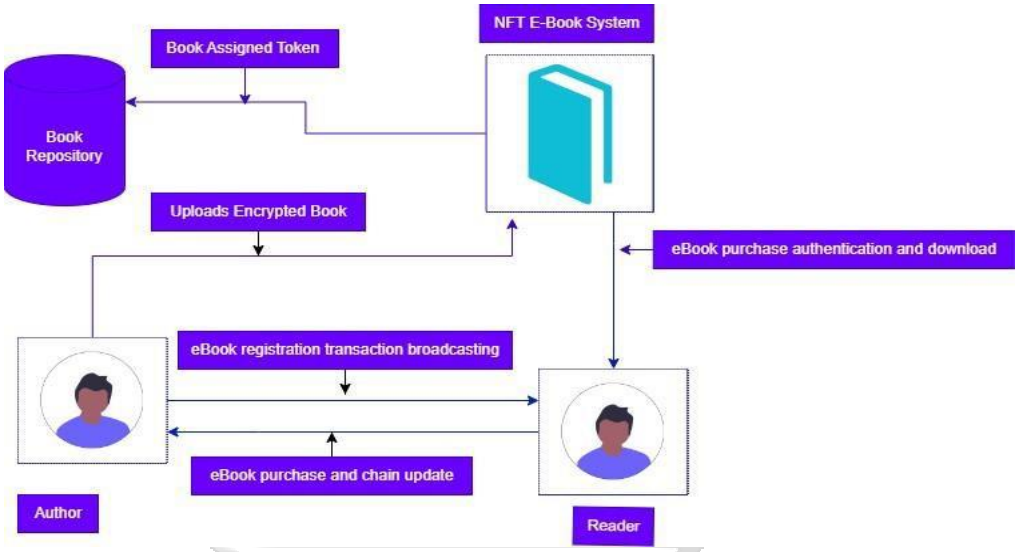

Figure 2.13: Conceptual Model

Chapter 3: Research Methodology

3.1 Introduction

Research is a methodical process that employs scientific methods to develop new knowledge that can be used to remedy a problem or improve an existing system (Bhaskar & Manjuladevi, 2016). This section explains the research methodology employed to construct the conceptual and theoretical frameworks. Further, it describes the study's target population and sample procedures. In addition, it describes the intended system development technique. In addition, it defines the scope of the project's research, data gathering, and data analysis methods. It also describes the methods utilized in system design and implementation. This section clarifies the exploitation and distribution of research findings. The chapter finishes with a discussion of the research's ethical requirements.

3.2 Research Design

The research design is the plan for how data will be gathered, analyzed, interpreted, and reported (Boru, 2018). It's a method for bridging the gap between theoretical questions and studies that can be conducted. What this means is that the study design specifies how the data will be collected, what methods will be employed, and how they will be applied to answering the research question. The study will adopt an exploratory research design to find meaningful insights into e-book piracy. This will be important in understanding the technologies used in typical e-book piracy mitigation systems and their associated limitations. The core features found will help form the basis that can be extended for the proposed system to be developed.

3.3 Target Population and Sampling

3.3.1 Target Population

In research, the term "target population" refers to the entire group or community that the researcher intends to study. After selecting a target population, a sampling frame is created (DJS Research, 2019). The target population for this study included authors and publishers in Kenya.

3.3.2 Sampling

Sampling is the selection of the group from which the researcher will collect data during the research. Voluntary response sampling were used during the research period. A convenience sample consists of the individuals who are most readily available to the researcher. There were 4 active publishers in Kenya and over 1000 authors according to (Publishers Global, n.d.). The sample size for this study was 100 authors and 2 publishers. This is due to geographical proximity, availability during this research period and a propensity to participate in the study.

3.4 Data collection and Analysis

3.4.1 Data Collection

The term "data collection" refers to the process of amassing information from all applicable sources in order to solve the research problem, conduct tests of the hypothesis, and assess the results (Dudovskiy, 2008). The data used in this study was gathered primarily through questionnaires and interviews. Interviews collected data on the respondents' views on the current system and its requirements. Questionnaires were used to gather requirements from users. The questions were structured differently for each focus group: authors and publishers.

3.4.2 Data Analysis

The process of data analysis entails the methodical use of statistical and/or logical methods for the purposes of describing, illustrating, summarizing, and evaluating information (Northern Illinois University, 2019). The data was analyzed in Microsoft Excel to help gain insights into the data. Descriptive and statistical analysis was used together to interpret and present the data. Lastly, graphs were used to visualize the results of the analysis.

3.5 Research Quality and Reliability

Research quality can be assessed by using the concepts of reliability and validity. A good indicator of a technique's or test's accuracy. The two main characteristics of any measurement are its reliability and validity (Middleton, 2019). The system's dependability was measured using test-retest consistency. Test-retest reliability shows the degree to which scores change from one

testing session to the next as a result of measurement mistakes (Mohajan, 2017). Reliability can be assessed by administering the same test twice to the same set of people at different time points (anywhere from a few weeks to a few months apart).

3.6 System Development Methodology

Due to time constraints, the Rapid Application Development (RAD) methodology was employed to create the proposed system. Each phase of RAD—Requirements planning, User design, Rapid Construction, and Cutover—is followed by the previous one.

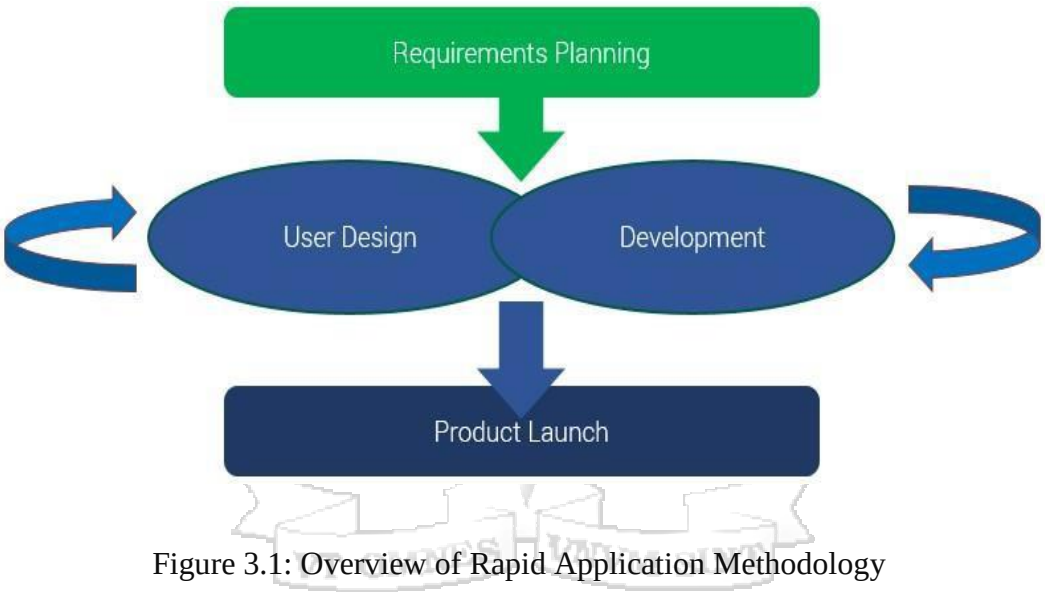

Figure 3.1: Overview of Rapid Application Methodology

(Filipets, 2015)

3.6.1 Requirements Planning

During this phase, the requirements for the proposed system will be defined. The objectives and expectations of the system were outlined, as well as the potential issues that must be addressed during the build to avoid expensive modifications in the future.

3.6.2 User Design

The user design was built during this phase through several prototype iterations. Target users of the proposed system were engaged during the process. All the bugs were fixed and worked out in an iterative approach to ensure there is no crack at the end of the design.

3.6.3 Rapid Construction

During this stage, the prototypes developed in the user design stage were implemented into a functional product. Program and application development and coding were part of the activities carried out during this stage. Lastly, unit, integration, and system testing followed successful development. Various technologies were employed during the implementation of the proposed system. They include Next Js, Tailwind CSS, Polygon, Vercel, Hardhat, MetaMask, and Alchemy.

3.6.4 Cutover

In this stage, the complete system for preventing e-book theft is put into action. The process involved transferring data, running tests, switching to the new system, and instructing the intended users on how to use it.

3.7 Utilization and Dissemination of Research Results

Dealing with e-book piracy is necessary for pushing humanity forward. This research results will come in handy to publishers, authors, and other players in the e-book industry. Authors can publish their books and get paid directly without involving a third party. This eliminates the possibility of authors not getting enough revenue while at the same time guaranteeing the security of the transactions. The research was disseminated in research journals and other publications for public scrutiny.

3.8 Ethical Considerations / Issues

Research ethics should inform every step of the research process (Bhandari, 2021). The researcher adhered to research principles and use ethical research methods and procedures. In addition, the researcher assured participants of confidentiality, anonymity, and how the research results were intended to be used.

Chapter 4: System Analysis and Design

4.1 Introduction

System design requires a certain procedure that entails an exhaustive description of the system's structure, components, and interface in order to suit the needs of the users and bridge the gap between prior designs. This section details the prototype development process and the functional and nonfunctional system requirements. The layered system architecture, use case diagram, and system sequence diagram all represent high-level system architecture and design.

4.2 Requirements Analysis

The requirements for the blockchain mitigation tool were gathered mainly through questionnaires sent to the relevant stakeholders. The list included a random sample of authors, publishers, and book readers. The data was then analyzed to aid in coming up with functional and non-functional requirements.

A questionnaire was utilized as a data collection method to gather requirements for the development of an NFT-based e-book marketplace. The primary objective of the questionnaire was to identify the desired features for the marketplace. A total of 20 responses were obtained from participants. In the questionnaire, respondents were presented with a list of features and were asked to indicate their preferred ones. The results were then compiled and displayed in a chart format to visualize the preferences of the respondents. Most of the participants expressed a preference for features related to easy payments and secure transactions, indicating the significance of these aspects in their decision-making process. Figure 4.1 shows the features most readers were interested in. Also, Figure 4.2 shows the results concerns the readers had regarding the technology.

Additionally, interviews were conducted with authors to gather further insights and perspectives. The findings from these interviews are included in the appendix section, providing additional valuable information to inform the development of the NFT-based e-book marketplace.

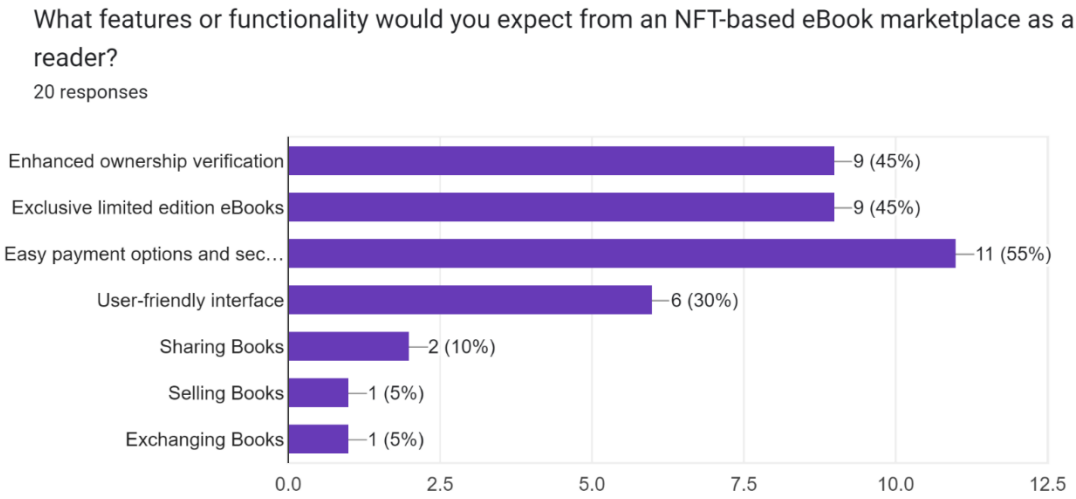

Figure 4.1: Features most Favoured

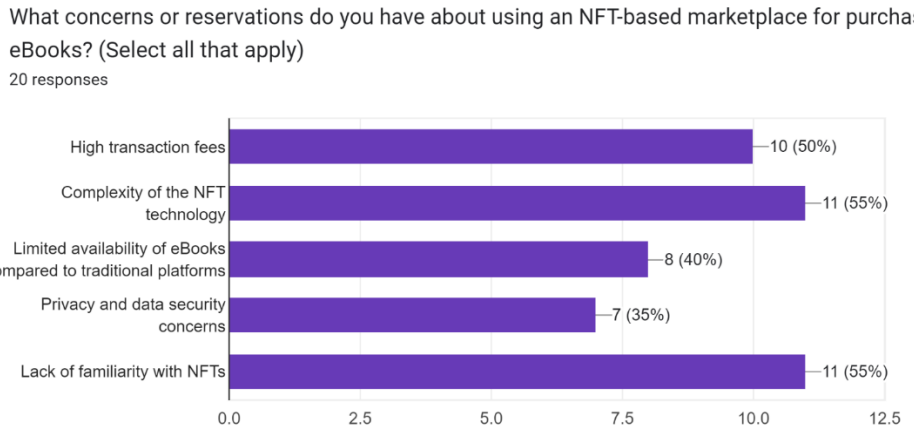

Figure 4.2: Concerns with Technology

4.2.1 Functional Requirements

Functional requirements define the function of a system or its component, where a function is defined as a specification of input-output behavior. The following is a list of the proposed tool's functional requirements.

The system should:

i). Allow the users to register.

ii). Allow the registered user to login.

iii). Allow the user (the author) to publish books.

iv). Allow the user (the reader) to purchase books.

v). Assign each book a unique token.

vi). Allow users to log out of the system.

4.2.2 Non-Functional Requirements

Nonfunctional Requirements (NFRs) are system characteristics that describe characteristics such as security, dependability, performance, maintainability, scalability, and usability. They serve as limits or restrictions on the architecture of the system across all backlogs. These are the non-functional requirements:

i). Security Requirement

The system should allow only authorized users to access the resources. The system should also withstand any external threats.

ii). Availability Requirement

The system should always be available to users whenever they need to upload and purchase books.

iii). Usability Requirement

The system is intended to be used by people from diverse backgrounds; hence, it should be user-friendly. It should require only a minimum guide for users of the system to navigate through it.

iv). Data Integrity Requirement

The system will guarantee data precision, consistency, and exhaustiveness. Whenever applicable, the system must track all events via audit logs and enforce approval checks for system event completion.

v). Adaptability Requirement

The system should adapt gradually even as the number of transactions and users increases over time.

4.3 System Architecture

The system architecture depicts the major system components while describing each component's services. To achieve the research aims, the proposed solution relies on blockchain

technologies. Figure 4.3 shows the proposed NFT-Based E-book Piracy Detection and Mitigation System's detailed architecture. The proposed tool allows authors to publish books and readers to buy and sell books in the system, guaranteeing authors of their share. The purchase details are then recorded in a public ledger for cross-checking whenever a new transaction is initiated. The platform will be built on the Ethereum blockchain to facilitate the different transactions of the system.

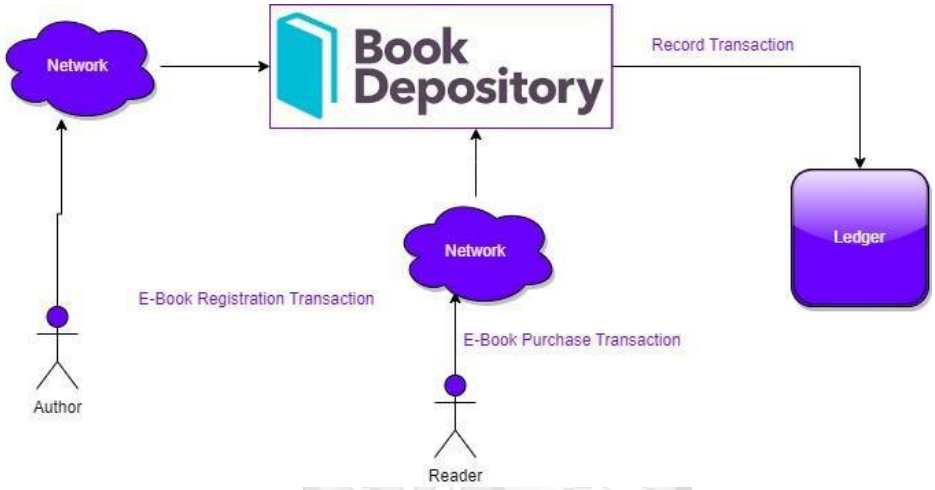

Figure 4.3: System Architecture

4.4 System Design

A system's design is an in-depth explanation of its intended operation. System designs that are most pertinent to the goals at hand were developed through a combination of user-specific needs and ideas from the researcher. The study's system design utilized Object-Oriented Analysis and Design (OOAD) techniques. OOAD is an approach to software engineering that emphasizes modeling a system as a collection of interacting objects, each with its own data and behavior. This method emphasizes the identification of objects and their relationships, as well as the encapsulation of data and functionality within those objects.

During the phase of system design, the researcher utilized OOAD techniques to analyze the system's requirements, identify the system's key objects, and define their attributes and behaviors. Additionally, the researcher modeled the interactions between objects, such as message transmission and

cooperation. The design process included the creation of class diagrams to depict the system's structure, the specification of object relationships and associations, and the definition of each class's methods and properties. Additionally, the team utilized use case diagrams to illustrate the efficacy of the system from the perspective of various actors or users.

By employing OOAD principles, the system design ensured the software solution's modularity, reusability, and maintainability. This strategy facilitated the development of a well-structured and robust system that addressed the project's requirements effectively. Use cases, system sequences, and class diagrams are only some of the UML diagrammatic representations that were put to use during the design process to provide a clear image of the system's inner workings. The execution of the system was aided by the illustrations and descriptions of the design that follow.

4.4.1 Use Case Diagram

The purpose of the use case diagram is to provide a visual representation of the system's features, including details about the participants and the outcomes that are expected. The interaction between actors and system processes is illustrated in Figure 4.4.

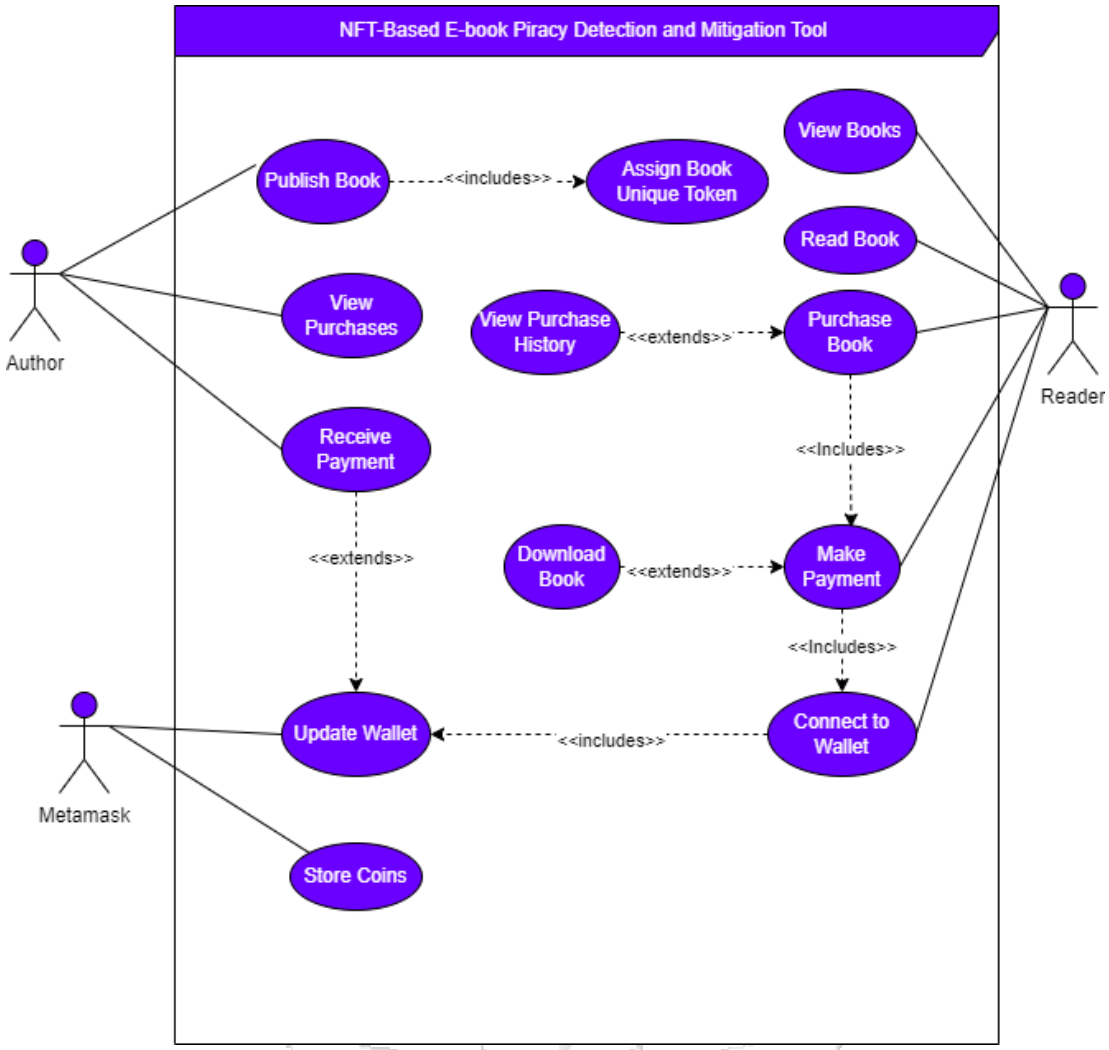

Figure 4.4: Use Case Diagram

4.4.2 Class Diagram

A class diagram represents a system's classes, attributes, methods, and object relationships. Figure 4.5 depicts a class diagram for the proposed tool with four classes: users, purchases, books, and payments.

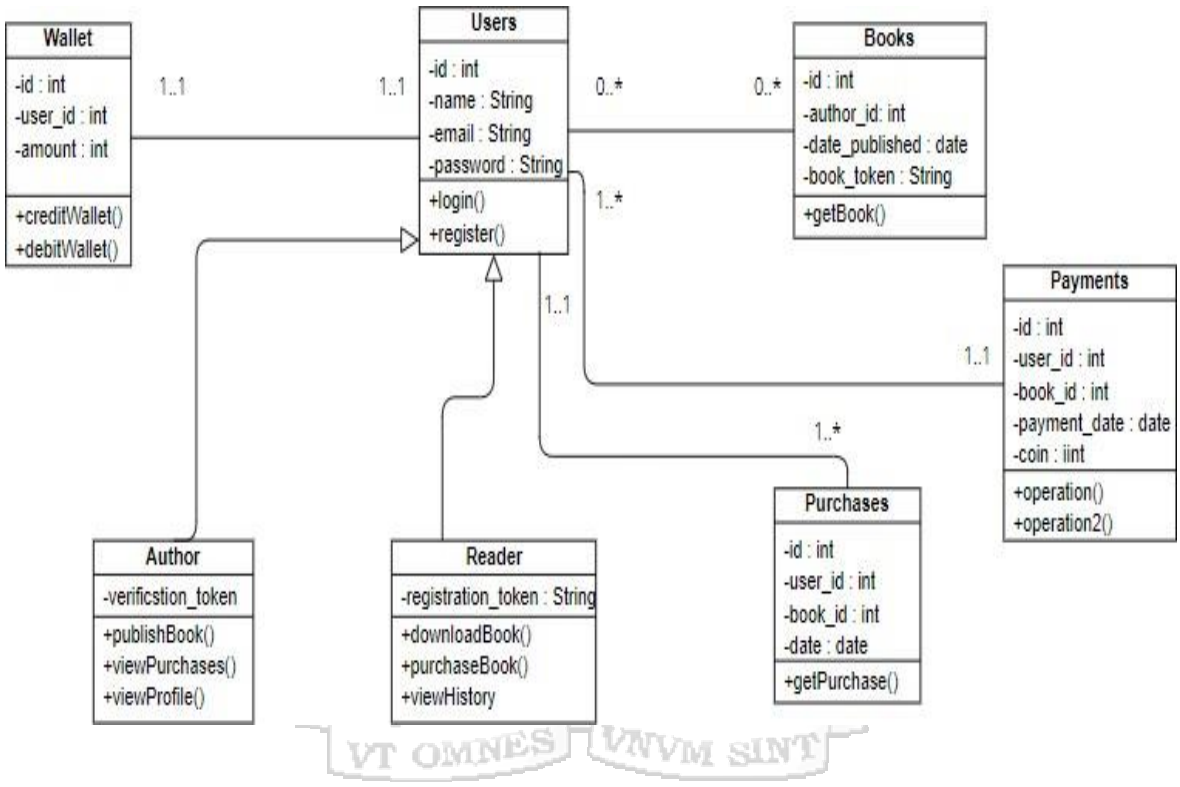

Figure 4.5: Class Diagram

4.4.3 Database Schema

A database schema is an abstract representation of the data stored in a database. As shown in Figure 4.6, there are five entities the: user, books, wallet, payments, and purchases. The attributes and various relationships surrounding these entities.

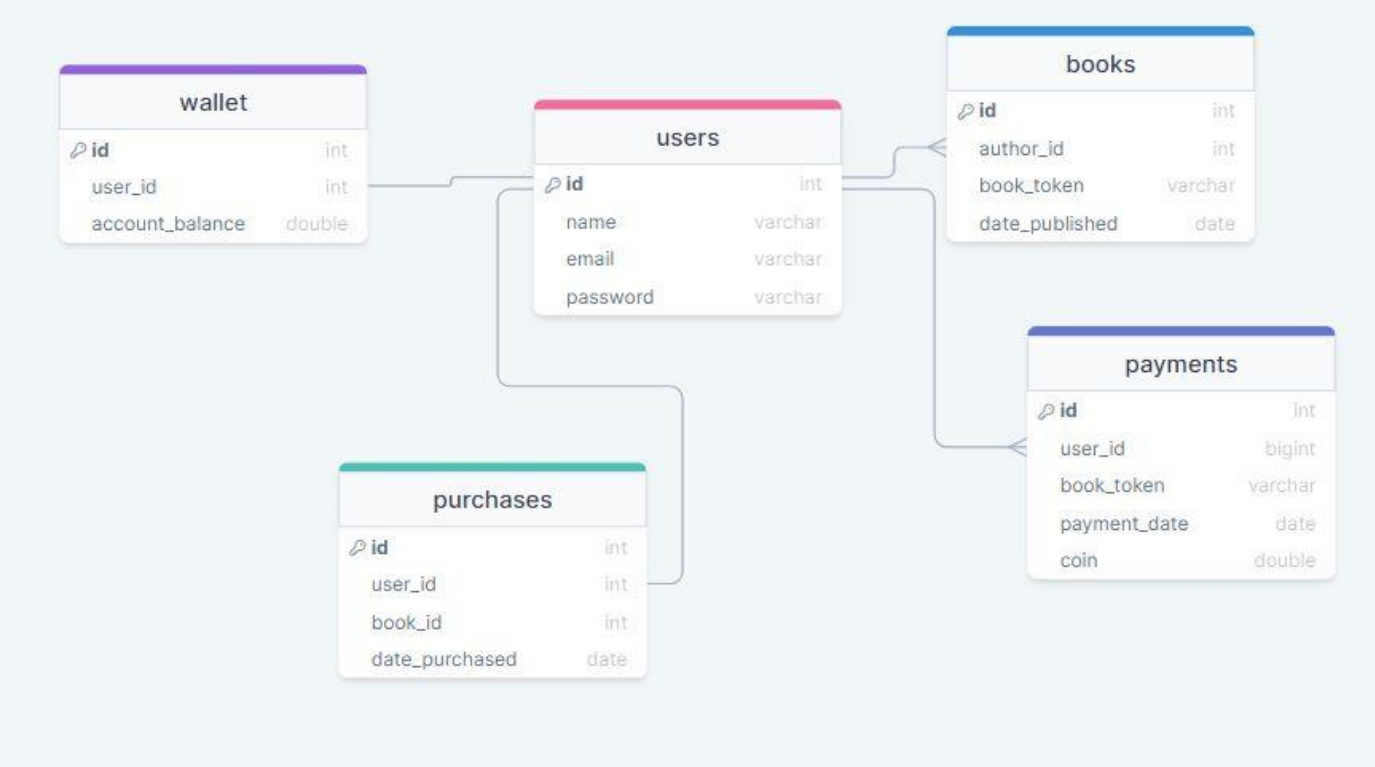

Figure 4.6: Database Schema

4.4.4 Sequence Diagram

The proposed system's general functionality is to allow users to publish books to reduce piracy. When a pirated copy is about to be published, the system should cross-check the existing transactions and update the status. The system sequence diagram in Figure 4.7 depicts the interactions between the system's various objects.

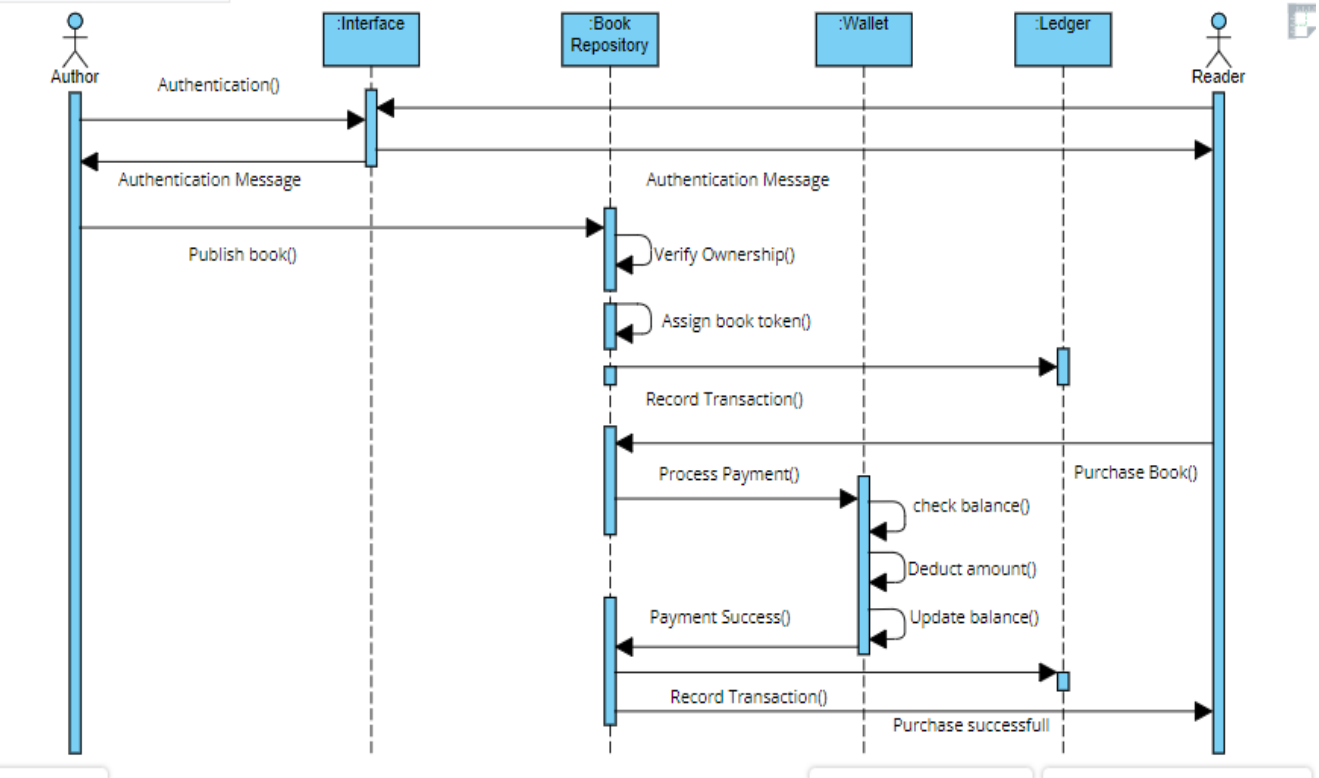

Figure 4.7: Sequence Diagram

4.4.5 Wireframes

4.4.5.1 Welcome Screen Wireframe

The welcome wireframe is the first screen the users will be able to see after loading the wireframe. It has an action button to take the user to the main features of the system, as shown in Figure 4.8.

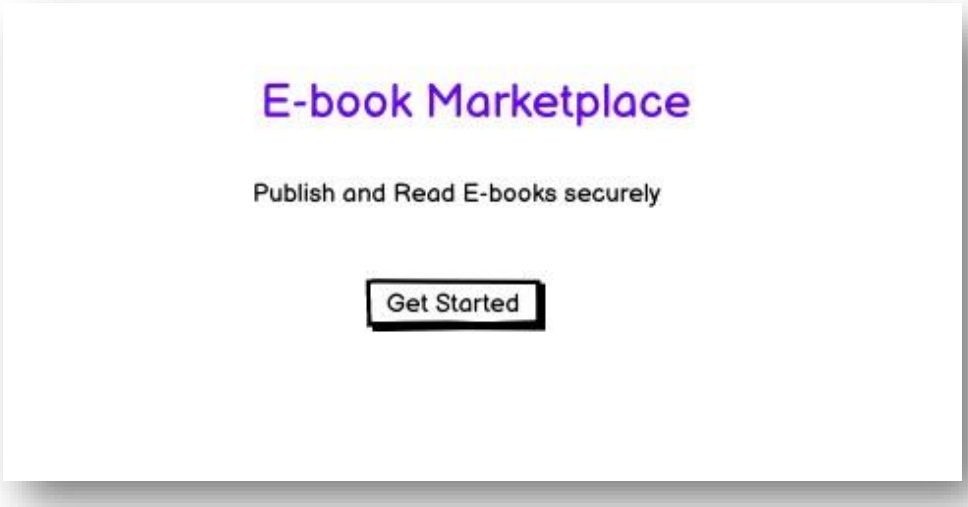

Figure 4.8: Welcome Wireframe

4.4.5.2 Login Wireframe

Users are required to login using their credentials to access the system. Username and password are collected for authentication purposes as depicted in Figure 4.9.

Figure 4.9: Login Wireframe

4.4.5.3 Register Wireframe

The registration wireframe is an easy-to-use user interface that enables users to establish

accounts by providing necessary data. Name, Mail, and Password are the three sections shown in the wireframe. The user can select the "Submit" button in the wireframe to finish the registration process. Overall, the platform's registration wireframe has been created to be simple and user-friendly, making it simple for new users to sign up for the service.

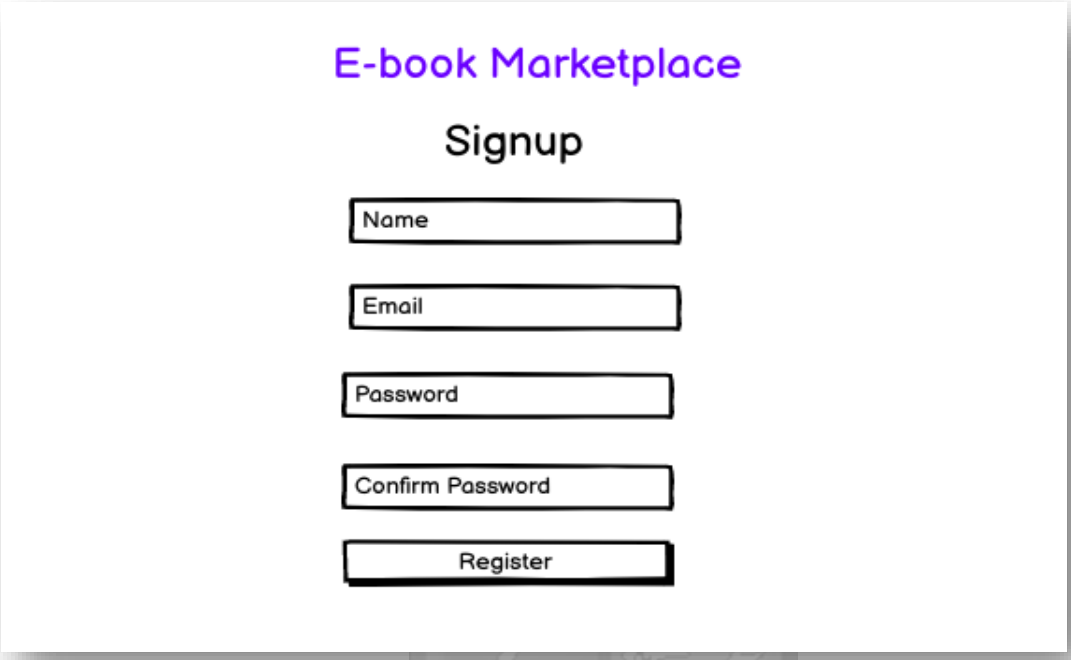

Figure 4.10: Register Wireframe

4.4.5.4 Books Dashboard Wireframe

The Books Dashboard Wireframe is a user interface that enables users to view a list of books with ease. The wireframe includes a list of books, with each book displayed as a distinct card with pertinent information including the title, author, and cover image. In addition, the

wireframe includes a search bar that enables users to locate specific titles rapidly. The Books Dashboard Wireframe is designed to be clean, straightforward, and user-friendly, allowing users to easily navigate and administer their book collection.

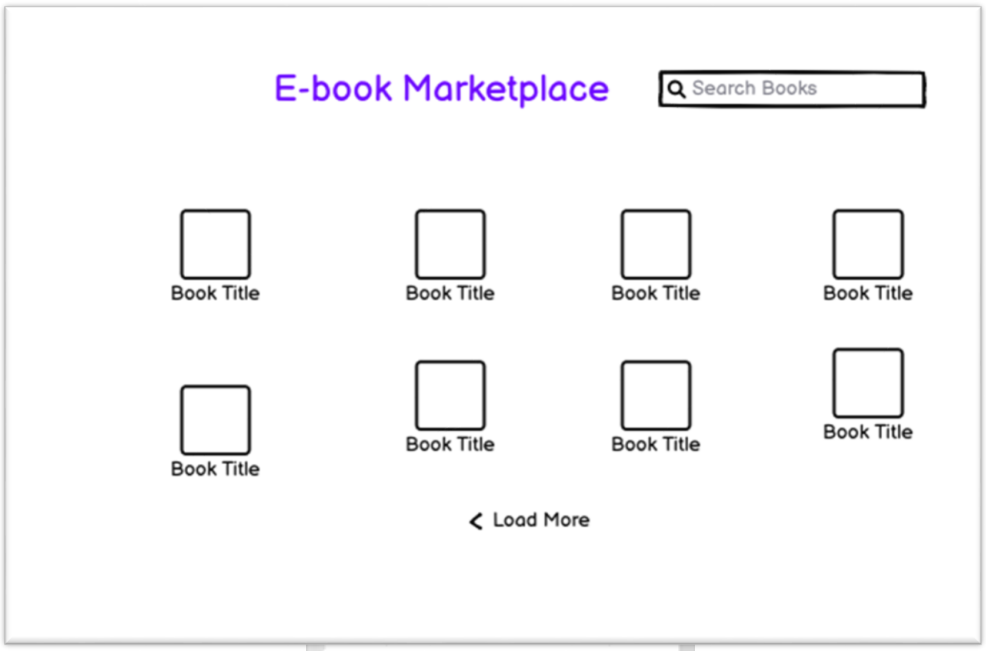

Figure 4.11: Dashboard Wireframe

4.4.5.5 Book Preview Marketplace

The Book Preview Wireframe is an interface intended to provide users with comprehensive information about a particular book. The wireframe contains an image of the book's cover as well as information about the book's title, author, and summary. Also included are the publication date, publisher, and genre of the book. In addition, the wireframe includes reviews and ratings from other users, allowing the user to gauge the book's popularity. The Books Preview Wireframe also contains a call-to-action button, such as "Purchase Book", that the user can click to purchase or submit the book to their shopping cart. The interface is designed to be visually enticing and simple to navigate, providing users with all the information they require to make an informed decision regarding the purchase of the book.

Figure 4.12: Book Preview Wireframe

4.4.4.6 Publish Book Wireframe.

The Books Publication Wireframe is a management and publication interface for authors. The wireframe contains a dashboard that enables users to upload and modify book manuscripts, cover images, and other relevant content.

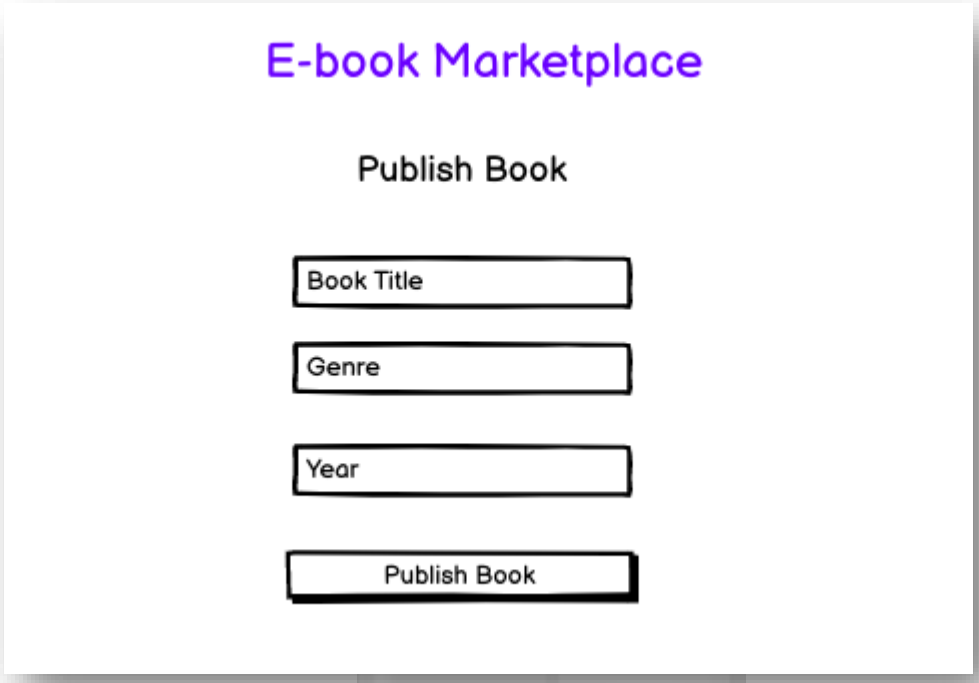

Figure 4.13: Publish Book Wireframe

Chapter 5: System Implementation and Testing

5.1 Introduction

System implementation shows how the system was built using various hardware and software platforms. The interfaces that users will interact with are also detailed. This section details the system's development process, including the steps of implementation and testing.

5.2 System Development Environment

Using Solidity, Next.js, and TypeScript, the built blockchain app is a decentralized application (DApp) focused on detecting and preventing e-book piracy. Using these technologies provides authors and publishers with a secure and transparent platform for protecting their intellectual property rights and preventing the unauthorized distribution of their works. The DApp employs a sophisticated algorithm to evaluate and compare the metadata of e-books in order to detect suspected cases of infringement. Once detected, the system activates a smart contract that enforces copyright protection and prevents the e-book's illicit distribution.

Next.js is utilized for the frontend development, giving authors and publishers a quick and responsive user experience for interacting with the DApp. TypeScript is utilized to provide type safety and enhance the overall quality of the codebase. MetaMask is a browser extension for interacting with the Ethereum blockchain that enables users to securely store and manage their digital assets. Ganache and Hardhat are utilized for local blockchain development and testing, while Alchemy provides the infrastructure for deploying the DApp to the Ethereum mainnet. Matic Tokens serve as the platform's native money, enabling users to transact quickly and cheaply inside the ecosystem. Writers and publishers can use Matic Tokens to pay for e-book piracy detection and prevention services, while users who attempt to distribute pirated e-books are punished by having their Matic Tokens revoked.

5.3 System Functionality Summary

A market for e-Books that utilizes NFT. Here, authors can publish their own books. Readers can purchase and sell books while rewarding the author for each exchange.

5.4 Fundamental System User Interfaces

5.4.1 Starting Hardhat Node

To start the local node, the command npx hardhat node is executed.

Figure 5.1: Local Node

5.4.2 Deploying Smart Contracts

in Figure 5.2.

Figure 5.2: Deploying smart contracts

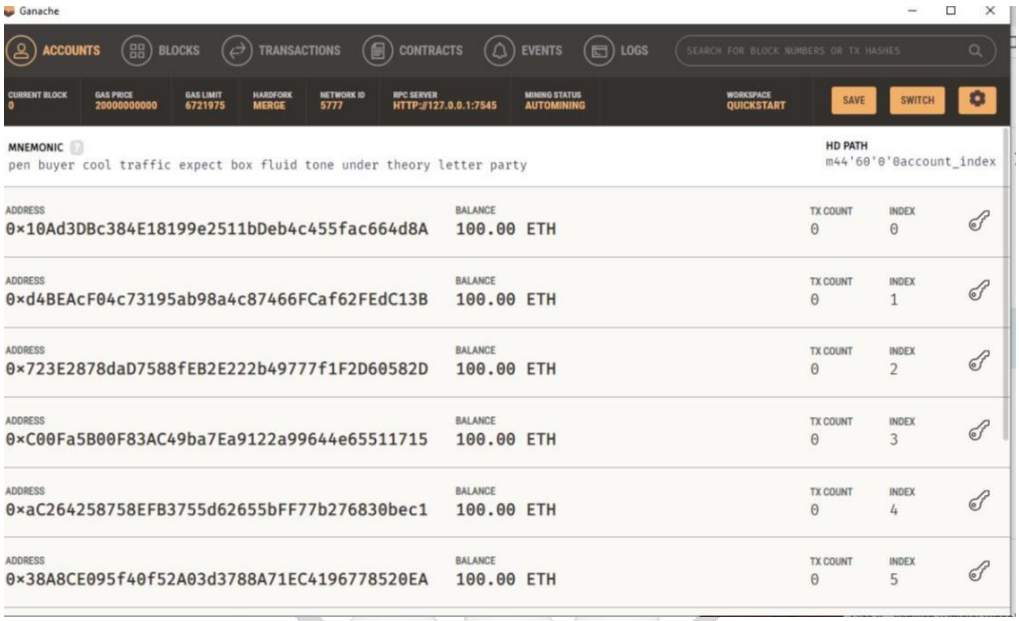

Figure 5.3: Starting Ganache

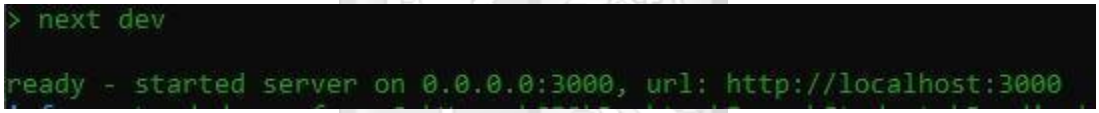

Figure 5.4: Starting the Next.js Local Server

Once the server has started, the home page is opened in a browser as Once the server has started, the home page is opened in a browser, as shown in Figure 5.5. The user is required to connect to Metamask Wallet to access the dashboard, where they can purchase or sell books. Metamask is a popular browser extension that functions as a digital wallet for storing and managing cryptocurrencies like Ethereum (ETH) and ERC-20 tokens. It enables users to safely store their digital assets and connect with Ethereum blockchain-based decentralized apps. Metamask is primarily utilized as a bridge between a user's browser and the Ethereum blockchain. It allows users to connect to decentralized applications without needing to set up a separate wallet or node. Users may effortlessly manage their digital assets and connect with decentralized services such as decentralized exchanges, prediction markets, and gaming platforms using Metamask.

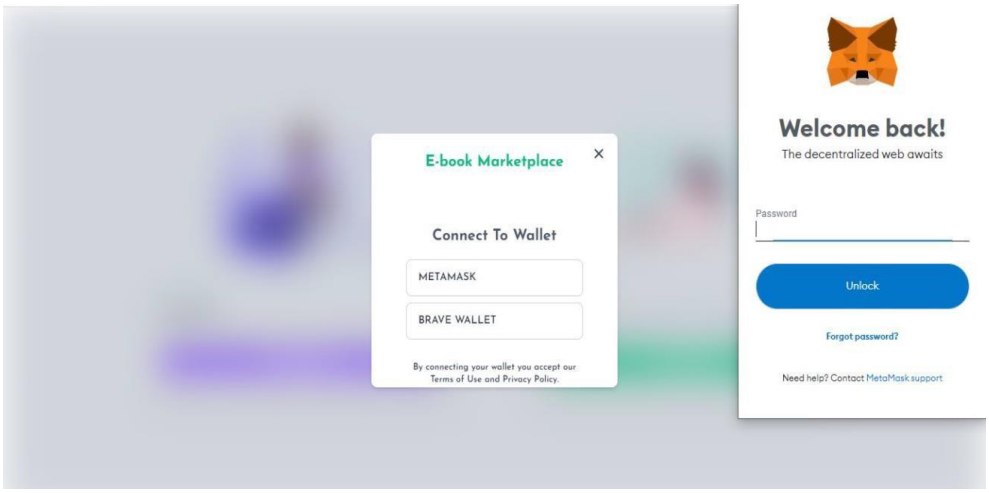

Figure 5.5: Verification Interface

5.4.3 Homepage

Figure 5.6 Once the wallet details have been added, the homepage presents the user with two options reader to access books and author to publish books.

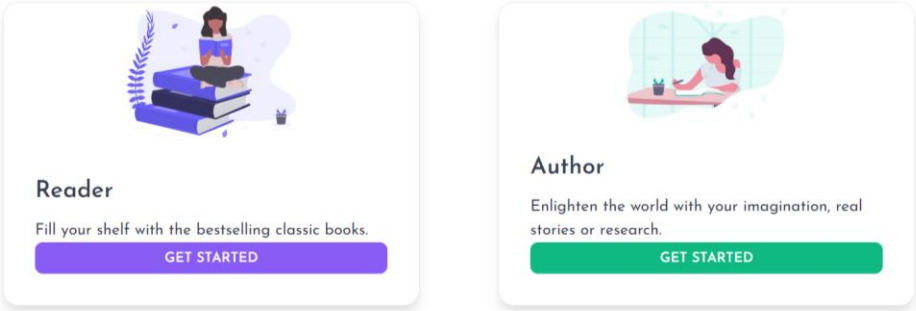

Figure 5.6: Homepage Interface

5.4.4 Adding Books to the Network

Figure 5.7: The author can add books through the author's dashboard by clicking on "New Book."

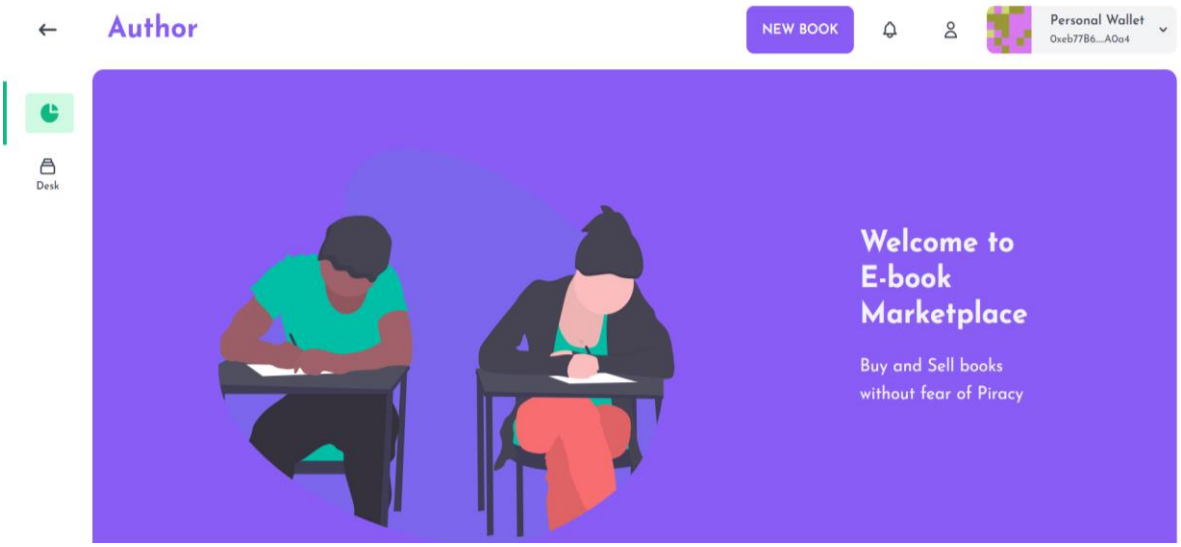

Figure 5.7: Authors Dashboard

By filling in the book details in Figure 5.8, the author can upload books, set the book's supply limit, and specify the cost in Matic.

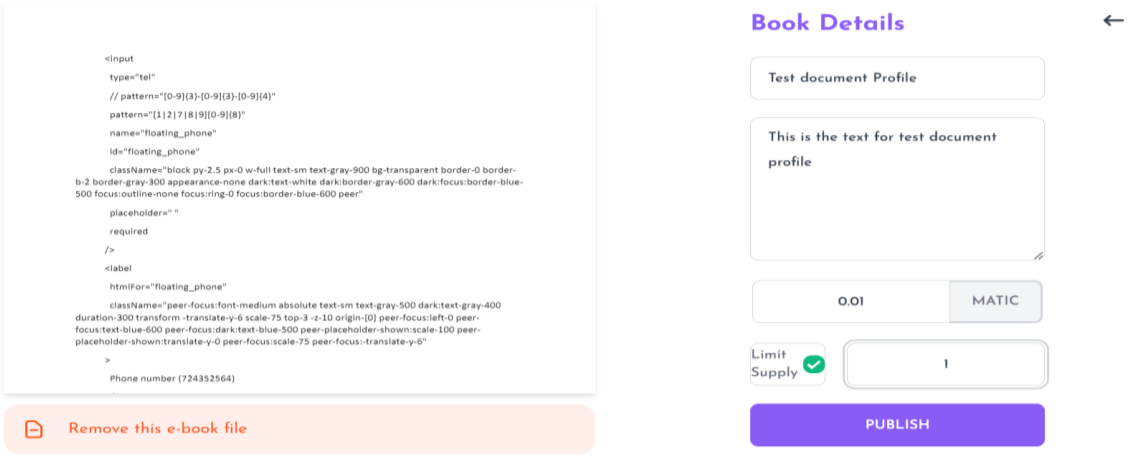

Figure 5.8: Adding Books to the Book Repository

Figure 5.9 show the Transaction Details of the book that has been uploaded tokenizing the book after the it has been placed in the repository.

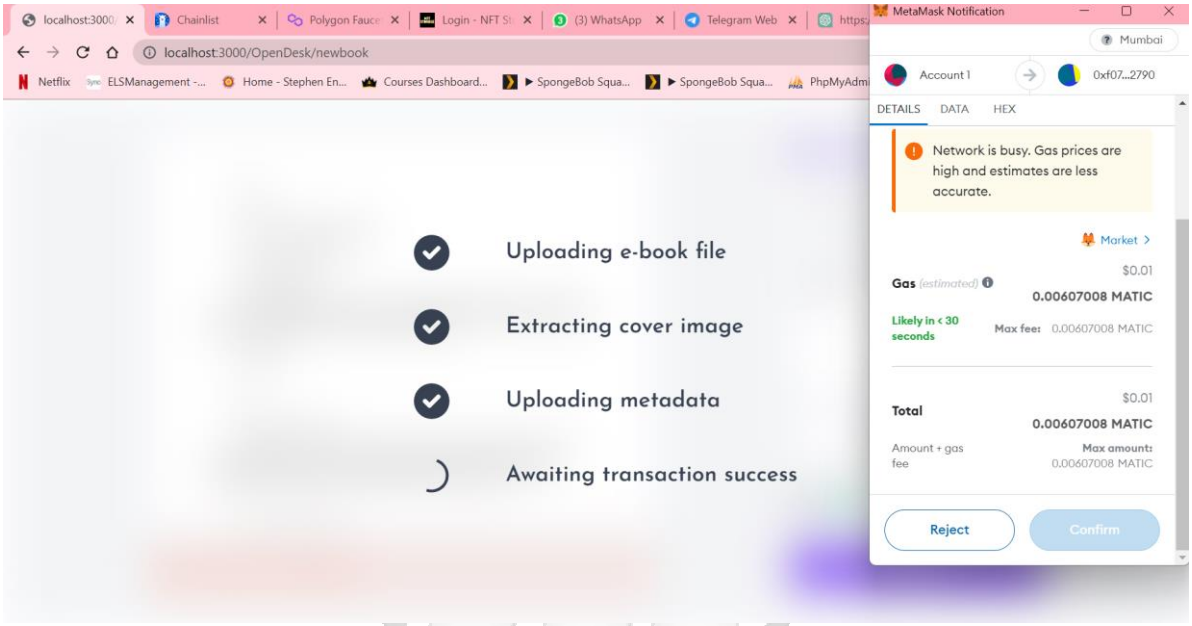

Figure 5.9: Transaction Confirmation

Figure 5.10: Once the user confirms the transaction the book is stored in repository and acquired a token number that uniquely identifies the book.

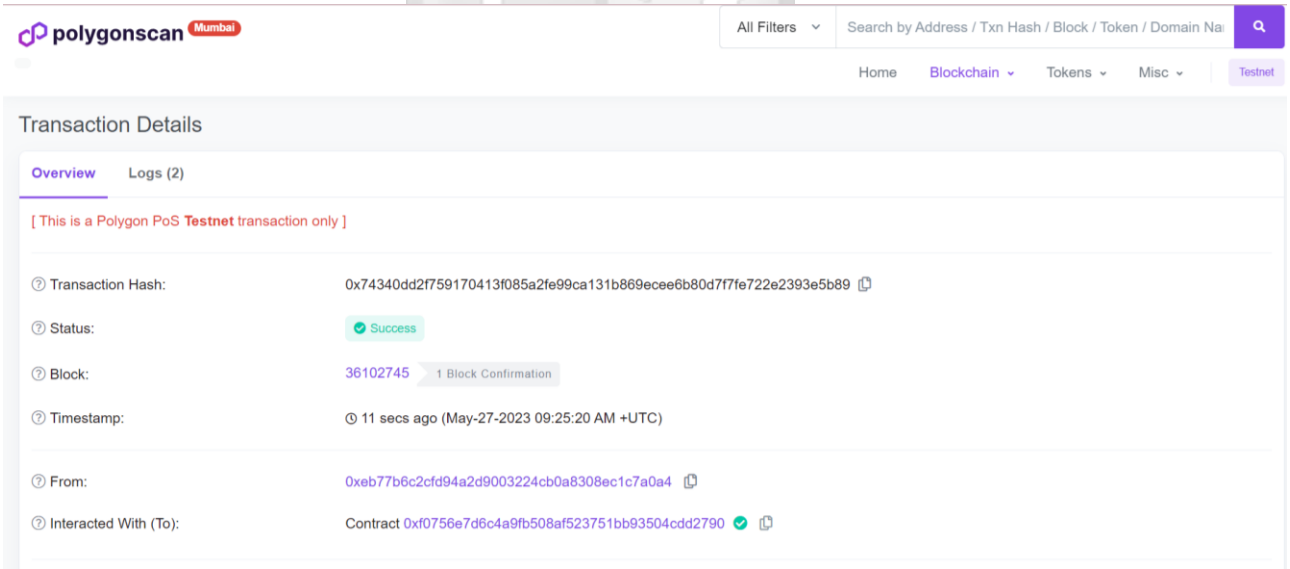

Figure 5.10: Transaction Detail

Figure 5.11: From the author's dashboard in Figure 5.8, the book is published and accessed through the "Desk" button. Here, it displays all the published book details, and

if the author wishes, they can enter a wallet address and create a voucher for readers to access the book for free.

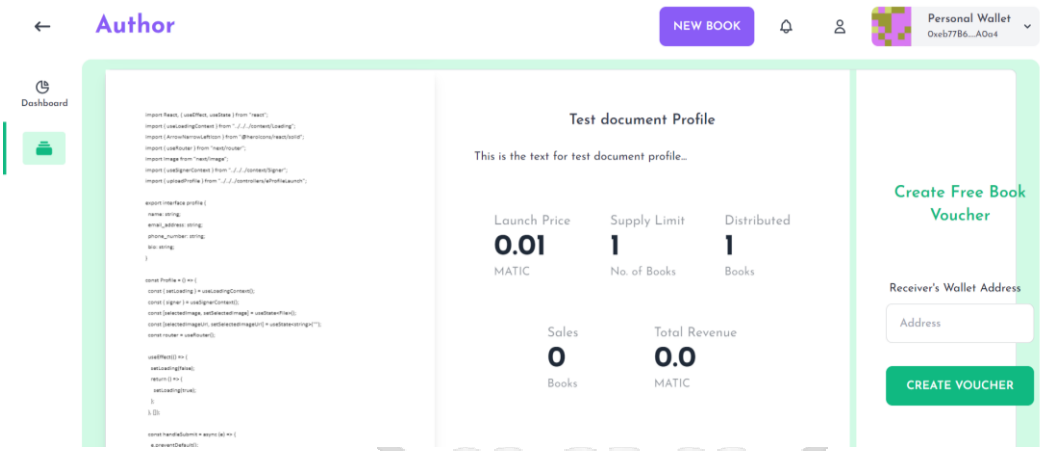

Figure 5.11: Published book

5.4.5 Purchasing Books

Readers can purchase books through the dashboard.

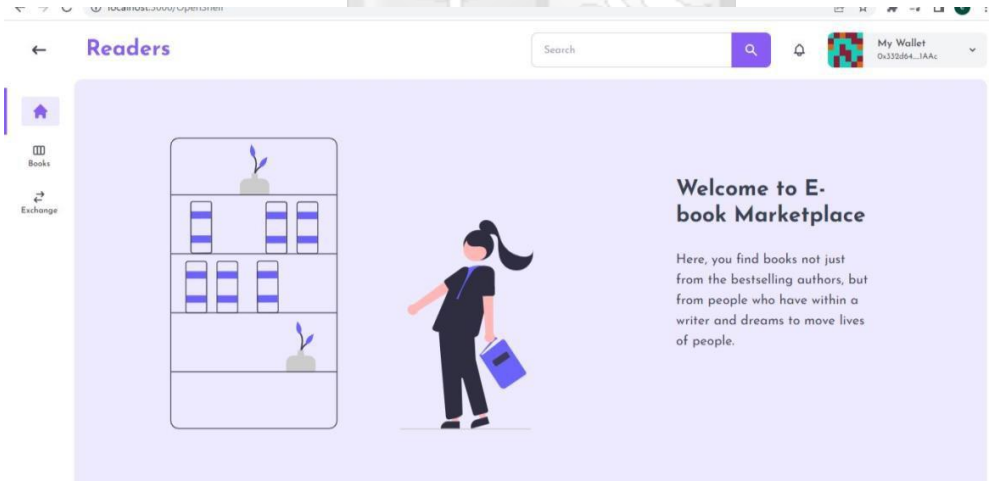

Figure 5.12: Readers Dashboard

Figure 5.13: The reader can access both the recently published books and the bestsellers. By reading the descriptions, the reader can decide which book to purchase in Figure 5.14 and Figure 5.15.

Figure 5.13: Readers Dashboard

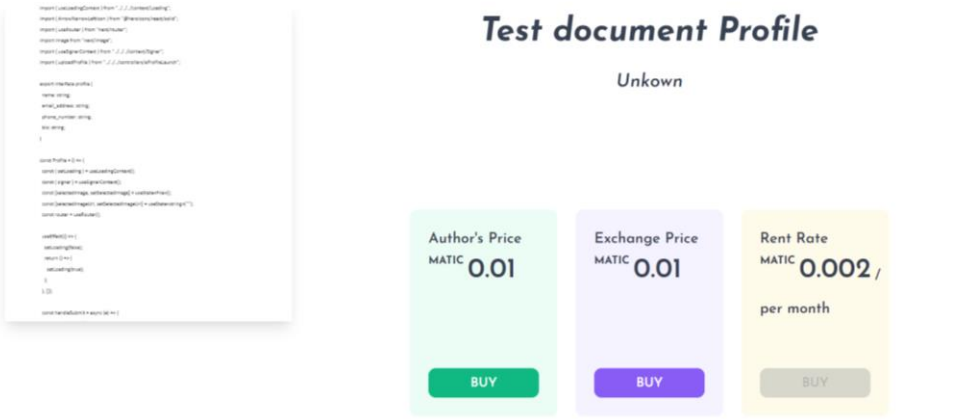

Figure 5.14: Purchasing book.

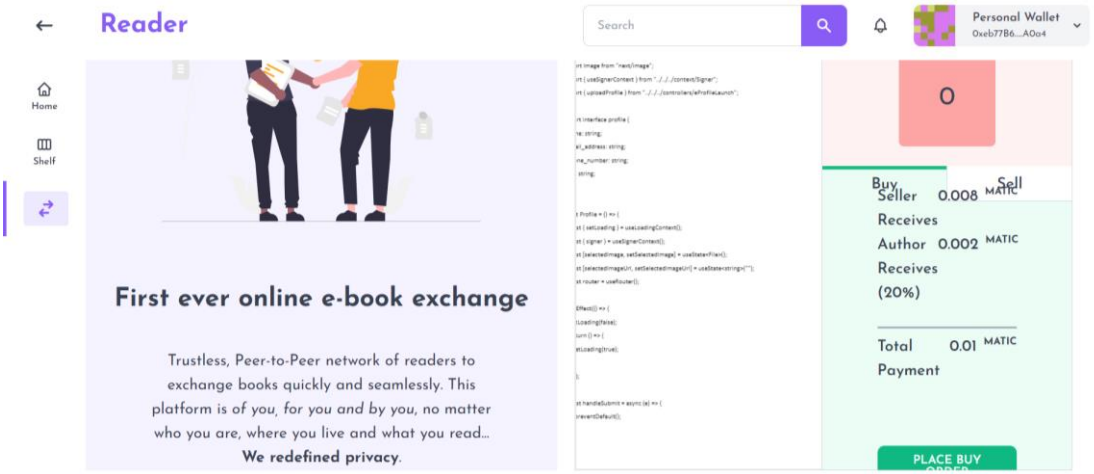

Figure 5.15: Place buy order page

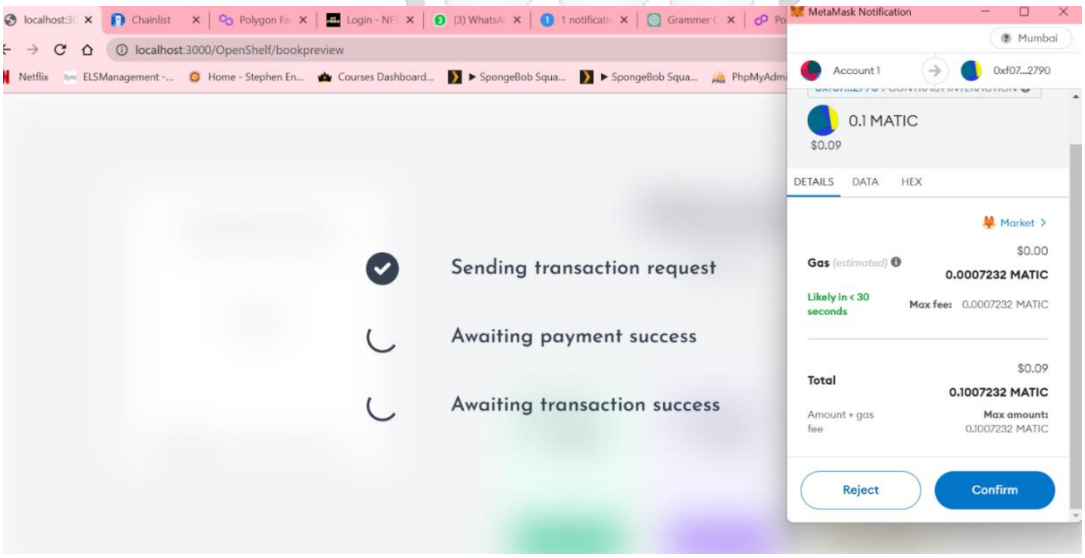

Figure 5.16: Transaction Confirmation

Figure 5.17: Once the user confirms the transaction the details of the purchase are recorded and the book is retrieved from the repository by its token number that uniquely identifies it.

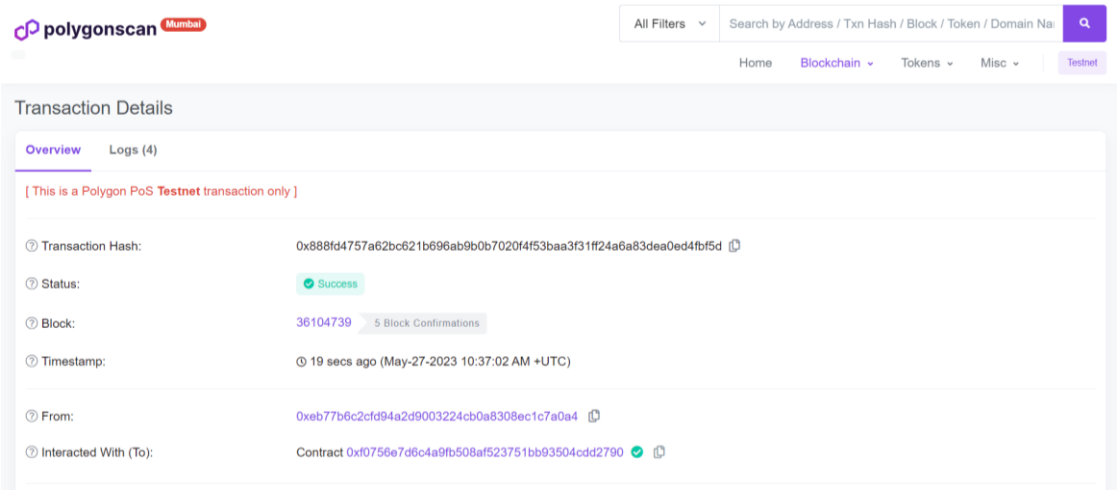

Figure 5.17: Transaction Detail

From Figure 5.13 once you select shelf, the purchased books are now stored in the shelf page in Figure 5.18 as owned books. The user can read, rent and distribute copies of books in Figure 5.19. The reader has follow the same process of placing the book on sale or rent and confirm the transaction.

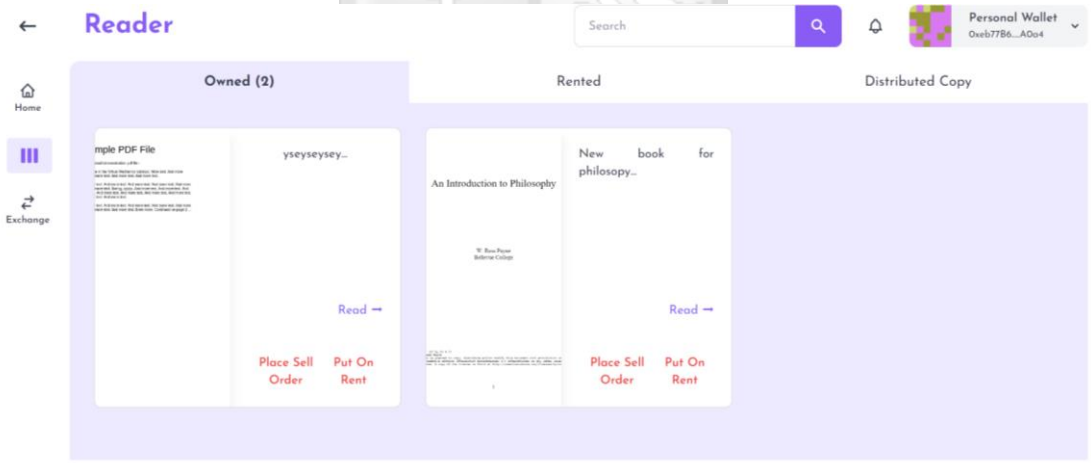

Figure 5.18: Transaction Detail

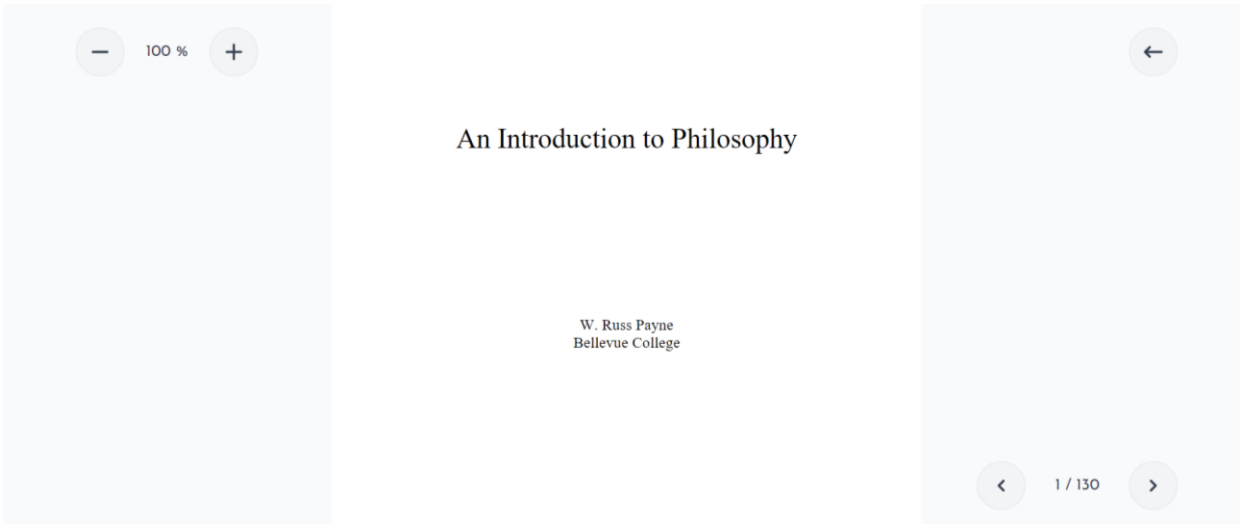

Figure 5.19: Purchased book page

5.5 System Testing

Testing was performed on the system to check if it met the functional requirements. Sections 5.5.1 and 5.5.2 detail the functional and compatibility tests performed on the blockchain application. Moreover, integration testing was also performed.

5.5.1 Functional Testing

Table 5.1: Summary of the Functional Tests Conducted

No	Test	Expected Results	Achieved Results
1	Blockchain Application Loading	The system is to be accessed via a web browser.	The system was successfully opened in a web browser.
2	Connecting to the Network	Metamask wallet users should be permitted access to the network.	An authorized user was able join to the blockchain business network successfully.
3	Publishing Books	A user should be able to publish books on the network.	A user should be able to publish books on the network.
4	Assigning Books unique tokens	The system should assign books Unique Tokens.	Tokens were assigned to books to verify ownership.
5	Purchasing Books	A user should be able to purchase books if they have enough funds.	Users with funds were able to purchase books.

5.5.2 Compatibility Testing

The program was built and hosted using a Windows-based operating system. Later, tests were conducted to ascertain how the program opened on the most recent versions of several web

browsers.

Table 5.2: Compatibility Test Outcomes

Browser Type	**Compatibility**
Internet Explorer	Yes
Google Chrome	Yes
Mozilla Chrome	Yes

Chapter 6: Discussion

6.1 Introduction

This research was aimed at identifying the factors that contribute to E-book piracy, analyzing the challenges in the existing models used in e-book piracy mitigation and prevention, investigating existing techniques used to detect and mitigate e-book piracy, and developing a prototype of a blockchain tool that detects and mitigates e-book piracy in Kenya. This section therefore discusses the achievements attained in relation to the research objectives.

6.2 Review of the Research Objectives for the Blockchain Application

Blockchain technology has the potential to revolutionize the way e-book piracy is tackled in Kenya. Research objectives of a blockchain application to end e-book piracy in Kenya are central to guiding the research process to the desired outcomes. A review of the research objectives highlights their relevance and importance in addressing the problem of e-book piracy in Kenya, as it was found that the high price of books compared to average income; scarcity of printing materials such as paper, machinery, ink, etc.; and finally the infantile state of the publishing industry, which has made developing countries overly dependent on their industrialized counterparts for their educational and research needs, are all factors that have contributed to e-book piracy.

The second objective of the research was to investigate existing techniques used to detect and mitigate e-book piracy. The blockchain's existing solutions include digital rights management (DRM) technology that allows publishers to encrypt their e-books and prevent unauthorized access or copying. This method helps prevent piracy by making it difficult for unauthorized use or copying of e-books. Another research objective is to explore the potential of blockchain technology to combat e-book piracy in Kenya.

This objective is crucial because it provides a framework for evaluating the applicability of blockchain technology to solving the problem of e-book piracy. Several studies had been conducted to address the problem of e-book piracy. (Chi et al., 2020) used encryption with

blockchain to provide downloaded content to authorized users in a secure manner. Encryption ensures the security and integrity of the data, which is one of its most significant advantages. But security remains a concern because anyone with the decryption key can simply access the data.

Also, digital rights management (DRM) systems have been developed to prohibit unauthorized duplication, printing, or modification of digital content after it has been supplied to a specific user (Qureshi & Jiménez, 202). Digital rights management (DRM) has been demonstrated to be successful at tracing content back to its legitimate owner, thereby discouraging users from passing off duplicated works as their own and engaging in illegal file sharing. Nevertheless, no procedures are provided to prevent unlawful redistribution of the content.

Blockchain technologies have also been explored by various researchers to address the e- book piracy problem. Peng et al. (2019) presented a digital copyright management system based on Ethereum. Many technologies, including digital watermarking, ElGamal cryptography, a perceptual hash function, smart contracts, and IPFS, were utilized by the proposed system. The research suggested adopting a data lake, an off-chain centralized storage solution, to store the transactional data of all the data given into the blockchain.

Vishwa and Hussain (2018) developed a system for decentralized data management. They developed a technique to gain control of the user's data using blockchain technology. This protocol allows the user to handle his own media files, reducing the need to rely on an external source. While there have been some positive advancements in this system, it does not yet prohibit the unauthorized copying of content, which is consistent with the findings of numerous other studies on the subject. By exploring the potential of blockchain technology, the researcher identified the strengths and weaknesses of the technology and was determined to apply it to combat e-book piracy in Kenya.

The third research objective was to analyze the challenges in the existing models used in e-book piracy mitigation and prevention. The methods employed to prevent piracy in digital content distribution have inherent weaknesses that hinder their effectiveness. Encryption, although widely used for securing digital content, faces a significant challenge if unauthorized individuals gain access to the decryption key, compromising the security of the content.

Digital Rights Management (DRM) systems, aimed at controlling content usage and distribution, often fall short in preventing unauthorized redistribution. Pirates continually find ways to bypass or circumvent DRM protections, rendering them ineffective in curbing piracy. Digital watermarking, another method used to embed unique identifiers into content, suffers from a critical security flaw. Malicious attackers or intentional infringers can detect and remove embedded watermarks, allowing them to freely distribute the content without proper authorization.

Similarly, multimedia fingerprinting, which involves creating unique signatures for digital content, faces weaknesses. Collusion attacks pose a significant challenge, as multiple unscrupulous buyers can collaborate to launch potent attacks against the fingerprinting system. This collusion makes it difficult to accurately track and prevent piracy. These weaknesses highlight the ongoing challenges in effectively preventing piracy in the digital realm. This formed the basis of the research which aimed to address these weaknesses and develop a more robust and secure method for protecting e-book piracy.

The fourth research objective was to develop a prototype of a blockchain tool that detects and mitigates e-Book piracy. In this study, an NFT-based e-book marketplace was developed using smart contracts, Solidity programming language, Next.js framework, and TypeScript. The researcher designed and built a blockchain application that functions as a decentralized application (DApp) with a specific focus on detecting and preventing e-book piracy. Smart contracts were utilized to create the foundation of the marketplace, enabling secure and automated transactions while ensuring the integrity of the e-book ownership and distribution. Solidity, a popular programming language for Ethereum-based smart contracts, was employed to write the code that governs the behavior of the smart contracts.

The Next.js framework, known for its capabilities in building server-side rendering and static site generation applications, provided a robust foundation for developing the user interface and front-end functionalities of the marketplace. TypeScript, a typed superset of JavaScript, was chosen to enhance code readability, maintainability, and scalability. Throughout the research study, the developed NFT-based e-book marketplace underwent rigorous testing to validate its functionality and effectiveness in detecting and preventing e-book piracy. The testing process

encompassed various scenarios and simulated attacks to ensure the system's resilience and security. By successfully developing the blockchain application, the research study contributes to the advancement of secure and decentralized solutions for the e-book industry. The implemented features and the testing phase demonstrate the viability and potential of using NFTs, smart contracts, and blockchain technology to combat e-book piracy effectively.

In conclusion, a review of the research objectives of the blockchain application to end e-book piracy in Kenya highlights their importance in solving the problem of e-book piracy. The objectives are to create a framework for studying the problem of e-book piracy, exploring the possibilities of blockchain technology, designing a blockchain-based solution, and evaluating its effectiveness. By achieving these goals, researchers can develop a blockchain-based solution that can effectively end e-book piracy in Kenya.

6.3 System Assessment

The prototype blockchain application built requires users to have access to the internet in order to use the system's features. The benefits and drawbacks of the application are briefly discussed below.

6.3.1 Advantages of the Developed Blockchain Solution

i. The application is compatible with all platforms, including browsers and operating systems.

ii. The security threat and unlawful redistribution disadvantages are eliminated.

iii. heightened record security relative to other systems due to the use of robust cryptographic techniques.

iv. The blockchain application enables immutability and provenance.

6.3.2 Disadvantages of the Developed Blockchain Solution

i. The application lacks a reporting option for counterfeit books.

ii. The blockchain application requires internet connectivity in order to function.

iii. The application does not address impersonation-related concerns.

iv. The application's scope is restricted to preventing e-book piracy.

Chapter 7: Conclusion and Recommendations

7.1 Conclusion

No country can prosper if invention and intellectual property are attacked and destroyed rather than safeguarded and appreciated. Kenya's copyright and anti-counterfeiting laws are clear and comprehensive, although they face challenges in practice. Copyright protection is important, but readers aren't always aware of why. Books and course materials purchased by parents are in high demand across all levels of education, but their exorbitant cost makes them out of reach for many pupils. Because of this, book piracy is possible. Pirates of books are free to meet consumer demand. As a result, the reading community in Kenya has reason to exert enormous pressure on the government. Kenya will gain international respect and economic rewards if it takes action to reduce book piracy.

Local demand side factors, such as providing cheaper books to local readers, lowering taxes on parental purchases of books/course books, and the government's decision to effectively supply schools with books, are necessary to eradicate the pirate problem. To meet the needs of the expanding industry, supply-side factors will need to be reined in, and technological advancements will need to be made to boost output and close any gaps in intellectual property protection. Kenya Copyright Board should enhance people, be professional so as to avoid corruption, and be swift in prosecuting piracy cases in order to improve the legal/legislative determinants.

To achieve this, the designed prototype is an effective and original solution to the issue of digital piracy. The developed tool provides a platform for authors and publishers to secure their intellectual property rights and prohibit unauthorized dissemination of their works by using the security and transparency of blockchain technology. Solidity, Next.js, and TypeScript are utilized to ensure that the project is created with modern and dependable technologies, while MetaMask, Ganache, Hardhat, Alchemy, and Matic Tokens provide a complete infrastructure for blockchain development and deployment.

With the E-book Piracy Detection and Prevention prototype, writers and publishers can rest easy knowing that their works are safeguarded against piracy, while users who seek to distribute illegal e-books are punished by having their Matic Tokens revoked. Overall, this study represents a substantial advance in the fight against digital piracy, and its effects will be felt for

years to come.

7.2 Recommendations

To promote the adoption of blockchain in securing e-books and protecting copyrights, the following recommendations are provided:

i). Right holders should utilize automated publishing methods, such as the E-book Piracy Detection and Prevention system powered by blockchain technology, to safeguard their copyright works. Copyright industry associations and societies should launch extensive campaigns through both print and digital media to raise awareness about the detrimental effects of piracy.

ii). Conduct lectures, seminars, workshops, and awareness events in educational institutions, including schools, colleges, and universities, to educate people on the importance of using automated publishing methods to combat piracy. Emphasize the long-term negative consequences of piracy for society, including the pirates themselves. Launch comprehensive media campaigns that highlight both moral responsibilities and copyright laws. Educate readers about the issues associated with pirated books, such as poor printing quality affecting eyesight and comprehension. Consider governmental support for campaigns to encourage reading.

iii). The Kenya Institute of Intellectual Property Rights (KIIPR) should offer regular courses and training programs on intellectual property rights (IPR) for various stakeholders, including copyright product creators and sellers, industry associations, law enforcement agencies, and the general public. Foster close collaboration between KIIPR, the government, and copyright industry groups to provide policy advice.

iv). Encourage the registration of copyright works to enhance protection. Continuously improve the E-book Piracy Detection and Prevention Tool, potentially by leveraging machine learning techniques to enhance the accuracy and reliability of the algorithm used to identify pirates. This requires a larger dataset of e-books and metadata to train the algorithm

effectively.

v). Copyright owners should implement a corporate license system for their software products. The government should establish mechanisms to ensure compliance with copyright laws, addressing concerns regarding corruption within law enforcement agencies and sluggish court proceedings. Efficient and vigilant officials, along with swift and stringent judicial processes, can act as effective deterrents against copyright infringement.

vi). Strengthen and support institutions involved in copyright protection. The Copyright Board of Kenya, operating under the Attorney General's Chambers, and the Anti-Counterfeit Agency established by the Anti-Counterfeit Act of 2008, play crucial roles in copyright enforcement. These entities should receive adequate funding from the government and be empowered with robust legislation to effectively carry out their mandates.

7.3 Future Works

Future work will center on the tool's integration with existing Digital Rights Management (DRM) systems. Numerous publishers currently employ DRM to combat e-book piracy, but these systems can be costly and difficult to implement. A blockchain-based technology could provide an easier, more cost-effective approach to embedding DRM into e-book distribution, thereby minimizing the risk of piracy and boosting authors' and publishers' revenues.

References

Abrams, D. (2017, April 12). *Kenya Publishers and Copyright Board Complain of Textbook Piracy*. Publishing Perspectives. https://publishingperspectives.com/2017/04/kenyapublishers-textbook-piracy/

Ahmadu, I. (2018). Effects of book piracy on publishing in Nigeria. *Information Impact: Journal of Information and Knowledge Management, 8*(3), 103. https://doi.org/10.4314/iijikm.v8i3.9

AL-Nabhani, Y., Jalab, H. A., Wahid, A., & Noor, R. M. (2015). Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. *Journal of King Saud University - Computer and Information Sciences, 27*(4), 393–401. https://doi.org/10.1016/j.jksuci.2015.02.002

Ante, L. (2020). Smart Contracts on the Blockchain – A Bibliometric Analysis and Review. *Telematics and Informatics*, 101519. https://doi.org/10.1016/j.tele.2020.101519

Anyaegbu, M. I., Adafor, M. R., & Nneka, U. (2016, January). *Piracy and its Effect on The Book Industry in Delta State*. Research Gate. https://www.researchgate.net/publication/308880517_Piracy_and_its_Effect_on_The_Book_Industry_in_Delta_State

Begum, I., & Sharma, H. (2018). Piracy: A threat to Academicians and Publishers. *ResearchGate*. https://www.researchgate.net/publication/333507912_Piracy_A_threat_to_Academicians_and_Publishers

Bhandari, P. (2021, October 18). *A guide to ethical considerations in research*. Scribbr. https://www.scribbr.com/methodology/researchethics/#:~:text=considerations%20in%20r esearch%3F-

Bhaskar, Sb., & Manjuladevi, M. (2016). Methodology for research II. *Indian Journal of Anaesthesia, 60*(9), 646. https://doi.org/10.4103/0019-5049.190620

Blackburn, D., Jeffrey, A., Eisenach, & David, H. (2019). *Impacts Of Digital Video Piracy on The US Economy*. https://www.theglobalipcenter.com/wp-content/uploads/2019/06/DigitalVideo-Piracy.pdf

Boru, T. (2018, December). *(PDF) Chapter Five Research Design and Methodology 5.1. Introduction Citation: Lelissa TB (2018); Research Methodology; University of South Africa, PHD Thesis*. ResearchGate.

https://www.researchgate.net/publication/329715052_Chapter_Five_Research_Design_And_Methodology_51_Introduction_Citation_Lelissa_TB_2018_Research_Methodology_University_of_South_Africa_PHD_Thesis#:~:text=Research%20Design%20A%20research%20design

Chi, J., Lee, J., Kim, N., Choi, J., & Park, S. (2020). Secure and reliable blockchain-based e-book transaction system for self-published e-book trading. *PLOS ONE, 15*(2), e0228418. https://doi.org/10.1371/journal.pone.0228418

Corporation, D. (2017, March 14). *E-Book Piracy Costs Publishers $315 Million in Lost Sales*. Www.prnewswire.com. https://www.prnewswire.com/news-releases/e-book-piracy- costspublishers-315-million-in-lost-sales-300423534.html

DJS Research. (2019). *Target Population*. Djsresearch.co.uk. https://www.djsresearch.co.uk/glossary/item/Target-Population

Dudovskiy, J. (2008). *Data Collection Methods - Research-Methodology*. Research-Methodology. https://research-methodology.net/research-methods/data-collection/

Elgazzar, K., Ibrahim, W., Oteafy, S., & Hassanein, H. S. (2013). RobP2P: A Robust Architecture for Resource Sharing in Mobile Peer-to-Peer Networks. *Procedia Computer Science, 19*, 356–363. https://doi.org/10.1016/j.procs.2013.06.049

Filipets, V. (2015, July 10). *Rapid Application Development Model: definition and stages*. Theappsolutions.com; The App Solutions. https://theappsolutions.com/blog/development/rad-model/

Fisk, N. (2009, June 8). *Understanding Online Piracy: The Truth about Illegal File Sharing: The Truth about Illegal File Sharing*. Scholar.google.com.uy. https://scholar.google.com.uy/citations?view_op=view_citation&hl=pt-BR&user=UAwouhIAAAAJ&citation_for_view=UAwouhIAAAAJ:Y0pCki6q_DkC

Gaber, T. (2013). *A typical DRM system architecture*. Research Gate. https://www.researchgate.net/figure/A-typical-DRM-systemarchitecture_fig1_267981401

Igesha, P. M., Muia, D. D., & Maina, D. L. W. (2016). Determinants Of Book Piracy In Nairobi County. *American Journal of Public Policy and Administration*, *1*(1). https://doi.org/10.47672/ajppa.113

JISC. (2012). *Preparing for Effective Adoption and Use of E-books in Education*. https://purehost.bath.ac.uk/ws/portalfiles/portal/11154091/e-

books_in_education.pdf

Karaganis, J. (2011). Media Piracy in Emerging Economies. *Www.ssrc.org*. https://www.ssrc.org/publications/media-piracy-in-emerging-economies/

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. *2016 IEEE Symposium on Security and Privacy (SP)*. https://doi.org/10.1109/sp.2016.55

Kristiani, E., Lee, C.-F., Yang, C.-T., Huang, C.-Y., Tsan, Y.-T., & Chan, W.-C. (2020). Air quality monitoring and analysis with dynamic training using deep learning. *The Journal of Supercomputing*. https://doi.org/10.1007/s11227-020-03492-8

Kumar, H. B. B. (2016). Digital Image Watermarking – An Overview. *Oriental Journal of Computer Science and Technology, 9*(1), 07-11. http://www.computerscijournal.org/vol9no1/digital-image-watermarking-an-overview/

Li, J. (2008). On peer-to-peer (P2P) content delivery. *Peer-To-Peer Networking and Applications,* *1*(1), 45–63. https://doi.org/10.1007/s12083-007-0003-1

Li, J.-S., Hsieh, C.-J., & Hung, C.-F. (2010). A novel DRM framework for peer-to-peer music content delivery. *Journal of Systems and Software*, *83*(10), 1689–1700. https://doi.org/10.1016/j.jss.2010.04.071

Li, N. (2009). Data Encryption. *Encyclopedia of Database Systems*, 574–574. https://doi.org/10.1007/978-0-387-39940-9_98

Luh, W., & Kundur, D. (n.d.). Multimedia Fingerprinting. *Encyclopedia of Multimedia*, 524 533. https://doi.org/10.1007/0-387-30038-4_153

Mangipudi, E. V., Rao, K., Clark, J., & Kate, A. (2019). Towards Automatically Penalizing Multimedia Breaches (Extended Abstract). *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. https://doi.org/10.1109/eurospw.2019.00044

Middleton, F. (2019, July 3). *Reliability vs. Validity in Research | Differences, Types, and Examples*. Scribbr.https://www.scribbr.com/methodology/reliability-vsvalidity/#:~:text=Reliability%20and%20validity%20are%20concepts

Mohajan, H. (2017). *M P RA Two Criteria for Good Measurements in Research: Validity and Reliability Two Criteria for Good Measurements in Research: Validity and Reliability.* https://mpra.ub.uni-muenchen.de/83458/1/MPRA_paper_83458.pdf

Mwale, A. (2022, June 4). *Book piracy denies the publishing industry 40pc market share – Kenya News Agency*. Kenyanews.go.ke. https://www.kenyanews.go.ke/book-denies-publishingindustry-40pc-of-market-share/

Neyole, N. M. (2014, November). *A Study Of E-Books And C-Books Utilization By University Students And Faculties In Kenya.* https://www.researchgate.net/publication/280926228_A_Study_Of_E-Books_And_CBooks_Utilization_By_University_Students_And_Faculties_In_Kenya

Nkiko, C. (2014). Book Piracy in Nigeria: Issues and Strategies. *The Journal of Academic Librarianship*, *40*(3-4), 394–398. https://doi.org/10.1016/j.acalib.2013.09.005

Northern Illinois University. (2019). *Data Analysis*. Hhs.gov. https://ori.hhs.gov/education/products/n_illinois_u/datamanagement/datopic.html

Nyambala, J. A. (2015). *Growth In the Use Of E-Books Collection Among Undergraduate Students In Two Academic Libraries In Kenya*. Uonibi. http://erepository.uonbi.ac.ke/bitstream/handle/11295/94118/Nyambala,%20Joyce%20Apondi_Growth%20in%20use%20of%20ebooks%20collection%20among%20undergraduate%20students%20in%20two%20acade mic%20libraries%20in%20Kenya.pdf?sequence=3

Peng, W., Yi, L., Fang, L., XinHua, D., & Ping, C. (2019, December 1). *Secure and Traceable Copyright Management System Based on Blockchain*. IEEE Xplore. https://doi.org/10.1109/ICCC47050.2019.9064101

Publishers Global. (n.d.). *E-Book Publishers of Kenya - List of E-Book Publishing Companies of Kenya that publish E-Book | PublishersGlobal.com*. Www.publishersglobal.com. Retrieved March 9, 2023, from https://www.publishersglobal.com/directory/kenya/media/e-book-publishers.

Qureshi, A., & Jiménez, D. M. (2022, December 22). *Blockchain-Based Multimedia Content Protection: Review and Open Challenges*. Mdpi. https://www.mdpi.com/20763417/11/1/1/pdf

Rasure, E. (2021, August 26). *What is a Cryptocurrency Public Ledger?* Investopedia. https://www.investopedia.com/tech/what-cryptocurrency-publicledger/#:~:text=A%20blockchain%20is%20a%20form

Ren, N., Zhao, Y., Zhu, C., Zhou, Q., & Xu, D. (2021). Copyright Protection Based on Zero Watermarking and Blockchain for Vector Maps. *ISPRS International Journal of Geo-Information*, *10*(5), 294. https://doi.org/10.3390/ijgi10050294

Roncevic, M. (2019). Chapter 3. DRM and Consumers. *Library Technology Reports*, *56*(1), 13–23. https://journals.ala.org/index.php/ltr/article/view/7252/9928

Sahni, S. P., & Gupta, I. (2019). *Piracy in the Digital Era*. Springer Nature Singapore. https://doi.org/10.1007/978-981-13-7173-8

Saravanan, K. (2017). Systems Development Methodologies: Conceptual Study. *Indian J.Sci.Res*, *14*(1), 27–37. https://www.ijsr.in/upload/105047310905.pdf

Srinivas, B., Venkata, K., & Varma, P. S. (2012). *Download Limit Exceeded*. Citeseerx.ist.psu.edu. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.734.9852&rep=rep1&type=pdf statista. (2022). e-books - Kenya | Statista Market Forecast. Statista. https://www.statista.com/outlook/dmo/digital-media/epublishing/e-books/kenya Vishwa, A., & Hussain, F. K. (2018). *A Blockchain-based approach for multimedia privacy protection and provenance*. Research Gate. https://www.researchgate.net/publication/331421741_A_Blockchain_based_approach_for_multimedia_privacy_protection_and_provenance

Walczak, S., & Cerpa, N. (2005). Artificial Neural Network - an overview | ScienceDirect Topics. www.sciencedirect.com. https://www.sciencedirect.com/topics/computerscience/artificial-neural-networkWang, S., Zhang, Y., & Zhang, Y. (2018). A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems. *IEEE Access*, *6*, 38437– 38450. https://doi.org/10.1109/access.2018.2851611

Wang, X. (2019, November). *https://www.researchgate.net/publication/342660617_Research_on_ECDSA-Based_Signature_Algorithm_in_Blockchain*. Research Gate. https://www.researchgate.net/publication/342660617_Research_on_ECDSABased_Signature_Algorithm_in_Blockchain

Wang, Y.-C., Chen, C.-L., & Deng, Y.-Y. (2021). Authorization Mechanism Based on Blockchain Technology for Protecting Museum-Digital Property Rights. *Applied Sciences*, *11*(3), 1085. https://doi.org/10.3390/app11031085

Zyskind, G., Nathan, O., & Pentland, A. 'Sandy'. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE Security and Privacy Workshops*. https://doi.org/10.1109/spw.2015.27

Appendices

Appendix A: Ethical Review

Strathmore UNIVERSITY

14th March 2023

Ms Nzangi Joy Mwende,
joynzangi@gmail.com

Dear Ms Nzangi,

RE: A Blockchain Tool to Detect and Mitigate eBook Piracy in Kenya. A Case of Kenya

This is to inform you that SU-ISERC has reviewed and **approved** your above **SU- master's** research proposal. Your application reference number is **SU-ISERC1609/23.** The approval period is from **14th March 2023 to 13th March 2024.**

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-ISERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-ISERC within 48 hours of notification
iv. Any changes, anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-ISERC within 48 hours
v. Clearance for export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days upon completion of the study to SU-ISERC.

Prior to commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

for: **Dr Ben Ngoye,**
Secretary; SU-ISERC

Cc: Mr Ambrose Rachier,
Chairperson; SU-ISERC

STRATHMORE UNIVERSITY INSTITUTIONAL SCIENTIFIC AND ETHICAL REVIEW COMMITTEE
(SU-ISERC)
14-Mar-2023
Email:isercreview@strathmore.edu
P.O BOX 59857-00200
NAIROBI-KENYA

Ole Sangale Rd, Madaraka Estate, PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034000
Email admissions@strathmore.edu www.strathmore.edu

Appendix B: NACOSTI

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **627775**

Date of Issue: **04/April/2023**

RESEARCH LICENSE

This is to Certify that Miss.. Joy Mwende Nzangi of Strathmore University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: A BLOCKCHAIN TOOL TO DETECT AND MITIGATE E-BOOK PIRACY A CASE STUDY OF KENYA for the period ending : 04/April/2024.

License No: **NACOSTI/P/23/24872**

627775

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

Appendix C: Turnitin Report

ORIGINALITY REPORT

19%	16%	6%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	su-plus.strathmore.edu Internet Source	6%
2	www.mdpi.com Internet Source	2%
3	ir-library.ku.ac.ke Internet Source	1%
4	www.coursehero.com Internet Source	1%

Appendix D: Interview Questions

Interview Guide

In recent years, e-book piracy has emerged as a significant problem for authors and publishers, resulting in revenue loss and harm to the publishing industry as a whole. By providing a secure, decentralized platform for monitoring and validating e-book transactions, blockchain technology offers a promising solution to this problem. In this interview, we'll ask authors and publishers about their thoughts and expectations regarding the use of a blockchain-based tool to detect and combat e-book piracy. We hope to obtain valuable insight into how this technology can be implemented and integrated into existing e-book distribution systems in order to effectively combat e-book piracy and safeguard the interests of authors and publishers.

1) Have you ever come across any cases of e-book piracy? If so, could you explain how it affected your income and business?

2) How do you presently identify and deal with e-book piracy cases?

3) What do you think about e-book theft detection and mitigation using blockchain technology?

4) What potential advantages do you see for this blockchain tool in terms of helping writers and publishers recover lost income from e-book piracy?

5) What hopes do you have for the precision and potency of this blockchain tool in identifying and reducing e-book piracy?

6) Can you describe any concerns or potential drawbacks regarding the use of blockchain technology for the detection and prevention of e-book piracy?

7) What kind of assistance and instruction do you anticipate receiving in

Appendix E: Questionnaire

PUBLICATION INDUSTRY QUESTIONNAIRE

An investigation into the implementation of a blockchain tool to detect and mitigate eBook piracy in Kenya

Researcher and Confidentiality/Non-Disclosure Assurance

My name is Joy Nzangi, a Master of Science in Computing and Information Systems student at Strathmore University. I am conducting a study on A blockchain tool to detect and mitigate eBook piracy in Kenya. This is in partial fulfilment for the award of my master's degree.

The data and/or information collected shall be treated with utmost confidence and shall not be shared without your prior permission.

Research Objectives

- To identify the factors that contribute to E-book Piracy.
- To analyse the challenges in the existing models.
- To investigate existing techniques used to detect and mitigate E-book Piracy.
- To develop a prototype of a blockchain tool that detects and mitigates E-Book piracy.

Directions in responding to the Questionnaire:

- Please tick against response that apply to you in each question and give additional information where needed.

Correspondence/Inquiries:

Joy Mwende Nzangi (joy.nzangi@strathmore.edu)

Faculty of Information Technology, Strathmore University

P. O. Box 59857-00200 Nairobi, Kenya

Mobile: +254 (0) 726 709 538

Background Information

1. Have you ever had one of your ebooks pirated?

   a. Yes

   b. No

2. If yes, how did you first become aware of the piracy of your ebook?

   a. Through a search engine

   b. Through a friend or colleague

   c. Through social media

   d. Other (please specify) _____

3. In your opinion, what is the biggest challenge with stopping ebook piracy?

   a. Lack of effective technology solutions

   b. Difficulty in tracking down pirate websites

   c. Inadequate laws and regulations

   d. Ineffectiveness of current enforcement efforts

   e. Other (please specify) _____

eBook Piracy technology

4. Have you used any anti-piracy solutions to protect your ebooks? a. Yes b. No
5. If yes, which anti-piracy solutions have you used? a. DRM technology b. Watermarking c. Monitoring services d. Legal action e. Other (please specify) _____
6. In your opinion, how effective have these solutions been in preventing piracy of your ebooks?

   a. Very effective

   b. Somewhat effective

   c. Not very effective

   d. Not effective at all

7. Do you believe that current anti-piracy solutions do enough to protect authors' rights?

   a. Yes

   b. No

c. Somewhat

8. Are you satisfied with the level of support your publishing company or distributor provides in addressing piracy issues?

   a. Yes

   b. No

   c. Somewhat

9. What do you think needs to be done to address the issue of ebook piracy better?

   a. Improved technology solutions

   b. Better collaboration between authors, publishers, and technology companies c. Stronger laws and regulations

   d. Increased enforcement efforts

   e. Other (please specify) _____

The factors and impact of eBook Piracy

10. How do you think ebook piracy has impacted your sales and income as an author? a. Significantly decreased b. Slightly decreased c. No impact d. Increased (unlikely, but possible)

11. Have you noticed any differences in the level of piracy for ebooks in comparison to physical books?

    a. Yes

    b. No

12. How do you feel about offering your ebooks at a lower price to help combat piracy?

    a. Strongly in favor

    b. Somewhat in favor

    c. Neutral

    d. Somewhat against

    e. Strongly against

13. In your opinion, do you think ebook piracy is a larger problem for best-selling authors or for new and unknown authors?

    a. Best-selling authors

    b. New and unknown authors

    c. Both equally

14. Have you ever been approached by someone offering to sell your pirated ebook?
    a. Yes
    b. No
15. Have you or anyone you know ever purchased a pirated ebook?
    a. Yes
    b. No
16. How important do you think it is for individuals to support authors by only purchasing legitimate copies of ebooks?
    a. Extremely important
    b. Somewhat important
    c. Not very important
    d. Not important at all
17. Do you believe offering free ebook samples can help reduce piracy?
    a. Yes
    b. No
    c. Unsure
18. How do you think the rise of ebook readers and tablet devices has impacted the issue of ebook piracy?
    a. Significantly increased piracy
    b. Slightly increased piracy
    c. No impact
    d. Decreased piracy
19. Have you ever received any compensation for losses due to ebook piracy?
    a. Yes
    b. No
20. Do you believe that the publishing industry as a whole is doing enough to address the issue of ebook piracy?
    a. Yes
    b. No
    c. Somewhat
21. In your own words, how would you define ebook piracy and its impact on the publishing industry?

22. Do you have any suggestions for potential solutions to the issue of ebook piracy?

23. How do you think the issue of ebook piracy will evolve in the future, given advancements in technology and changes in consumer behavior?

24. How has your perspective on ebook piracy changed over time, if at all?

25. Can you describe a specific instance of ebook piracy that significantly impacted you or your work?