Leveraging Blockchain and Artificial Intelligence for Enhanced Copyright Enforcement in South Africa

Author: Joseph JTR Mugauri (MGRJOS008)

Minor Dissertation as a prerequisite for completion of the LLM in Intellectual Property Law

Supervisor: Prof Caroline Ncube

Word Count: 22, 647

Research dissertation presented for the approval of Senate in fulfilment of part of the requirements for the LLM in Intellectual Property Law in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of LLM in Intellectual Property Law dissertations, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations.

Signature: Signed by candidate

Date: 22 August 2024

ACKNOWLEDGEMENTS

First and foremost, I would like to express my heartfelt gratitude to my supervisor, Prof. Caroline Ncube. Your patience, guidance, and unwavering support throughout the dissertation have been invaluable. You challenged me to push the boundaries of my research and helped shape this work into what it is today. For that, I am deeply grateful. I also want to take a moment to acknowledge and thank myself. This journey was difficult, and I worked tirelessly to reach this point. The late nights, moments of self-doubt, and perseverance paid off, and I am proud of my progress. To my father, Joseph Mugauri, thank you for always being there for me. Your encouragement, belief in me, and unwavering support throughout this journey have meant the world to me. You were my rock during this process, and I am forever grateful. To my mother, Tukisayi Mugauri, thank you for your prayers that kept me safe and sane throughout this journey. Your love and spiritual support sustained me through the toughest times, and I am blessed to have had you by my side. Finally, I extend my gratitude to everyone who supported me in one way or another during this dissertation process. Your contributions, no matter how big or small, have helped me reach this milestone, and I am truly thankful for that.

Table of Contents

Chapter 1: Introduction

1.1.Introductory remarks

The Fourth Industrial Revolution has pushed South Africa into a perpetual technological transformation that inspired increased human interactions with blockchain and artificial intelligence (AI) for personal or commercial purposes. These technological advances move at the speed of light purposefully to supplement that which goes beyond human abilities, maximising efficiency, profits, accuracy, productivity, and surveillance. Although doubt hovered above the incorporation of blockchain and AI technology within our daily activities, they seem to have shut their naysayers down, proving their worthiness whenever in use.[1] For example, the use of chatbots, which is are applications powered by generative AI and used by various businesses that can have automated conversations with more than one human being simultaneously to assist with queries,[2] and smart contracts, which are blockchain-based programs used to automate the execution of a contract, upon fulfilment of conditions at the exclusion of a middleman.[3]

According to Gulyaeva and Lovells, technological advances exacerbated vulnerabilities in people's copyrights and infringements in the digital space.[4] This makes digital copyright infringement a nightmare for rights holders as it intercepts how they exploit their works. For example, websites facilitate movie or music copyright infringement by making available copyright-protected works to the public for free, without a license from the copyright holder. A report by the US Chamber of Commerce's Global Innovation Policy Centre in 2019 indicated that digital copyright infringement of videos cost the entertainment industry an estimated amount of up to $71 billion every year, reducing the revenue by 11% to 24%, resulting in approximately 230,000 to 560,000 jobs lost impacting the growth of the economy.[5] Pam and Mantu add that copyright infringement negatively impacts economic development, highlighting that copyright infringement has a negative economic effect.[6] To dispute this stance, Snelling highlights that not every instance of copyright infringement

---

[1] Roman V Yampolskiy 'AI Risk Skepticism' 2021; Oluwaseun David Adepoju, Bosun Tijani & Steven Karera 'Artificial Intelligence Skepticism in Career Domains' (2024) 15 *International Journal for Digital Society* 1880–8; Kent Anderson 'Can Blockchain Withstand Skepticism? An Inquiry' (2018) 38 *Information Services & Use* 1–6.

[2] Aishwarya Gupta et al. 'Introduction to AI Chatbots'(2020) 9 (7) *International Journal of Engineering Research* 255-258.

[3] Charlotte Ene 'Smart Contracts - The New Form of The Legal Agreements' (2020) 14 *Proceedings of The International Conference on Business Excellence* 1206–10.

[4] Natalia Gulyaeva And Hogan Lovells 'Intellectual Property Law in The Digital Society: Challenges and Opportunities' available at *https://www.expertguides.com/articles/intellectual-property-law-in-the-digital-society-challenges-and-opportunities/arcpwtmm* accessed on 26 March.

[5] David Blackburn, Jeffrey A. Eisenach, David Harrison Jr 'Impacts of Digital Piracy on the U.S. Economy' (2019) *US Chamber of Commerce* 1-16.

[6] Adamu Audu Pam & John Ishaku Mantu 'Copyrights Infringement and Its Impacts on Developing Economies' 2018.

equates to a lost sale because some individuals who engage in piracy might not have purchased the content if it was not free.[7] Although Karanganis appreciates the importance of studies on the economic effects of copyright infringement, he highlights how they raise methodological challenges supporting Snelling. He denotes that determining substitution effects in piracy, which is the likelihood that a pirated copy replaces a legal sale, is challenging. This complexity arises because the assessment depends on understanding the effects of price and income. These effects influence whether a consumer who pirated content would have bought it at the legal cost. Additionally, it is crucial to consider the countervailing benefits of piracy to both the industry and consumers in any economic impact model. He encouraged viewing piracy as an integral part of the economy rather than merely a negative factor.

As it stands, copyright law in South Africa has faced some backlash from academics, calling it obsolete as it fails to address copyright issues that arise in the digital sphere.[8] The reason may be that the legislation was enacted 46 years ago. Hence, some of the current technology was outside the minds of the legislators when they drafted it, thus making it inadequate to tackle copyright infringement issues caused by modern technology.[9] Although amendments covering this gap are underway, the process takes years. Hence, copyright owners seek private enforcement measures that leverage technology to control digital copyright infringement.[10]

Over the years, copyright owners have utilised access control, copy control and algorithmic measures to mitigate the proliferation of infringement. Still, with technological progression, users have been devising new methods to circumvent the protection measures and gain free access to the works, thus weakening them. However, suppose the same technology can be used to circumvent, it can also be used to protect, so employing blockchain and AI as countermeasures to enforce copyright is reasonable as it can mitigate the problem. Although it must also be noted that the issue will still not be extinguished, the severity of the acts will be reduced. For instance, some companies like Google have already started watermarking content using AI.[11] So it is not a question of applicability but how the technology can be leveraged to enforce copyright in the digital space.

---

[7] Alexander Peter Snelling *Digital Piracy: How the media industry is being transformed* (Universidad Politecnica De Valencia, 2013) at 10.
[8] Klaus D Beiter et al 'Copyright Reform in South Africa: Two Joint Academic Opinions on the Copyright Amendment Bill [B13B-2017]' (2022) 25 *PELJ*.
[9] 'Report on The South African Open Copyright Review' at 1 available *at https://ip-unit.org/wp-content/uploads/2010/07/opencopyrightreport1.pdf* accessed on 20 July 2024.
[10] Coenraad Visser 'Technological Protection Measures: South Africa Goes Overbroad' (2006) 7 *SAJIC* 54-63.
[11] The Verge 'Google's invisible AI watermark will help identify generative text and video' available at *https://www.theverge.com/2024/5/14/24155927/google-ai-synthid-watermark-text-video-io* accessed on May 19 2024.

Despite the benefits like blockchain's immutability or secure nature and AI's self-learning technology, which can help enforce copyright against digital infringements, the two technologies have their limitations, for example, those relating to data privacy, security, and copyright ownership. Additionally, blockchain has a carbon footprint caused by its energy-intensive process of verifying transactions that pose environmental risks[12], which is further explained in Chapter Three. AI can perpetrate privacy violations, misinformation, or political manipulation. Without a specific legal instrument governing blockchain and AI, bad actors may exploit this to the detriment of copyright holders or good users. So, regulations are necessary to ensure a fair playing field for consumers and owners. The good news is that the European Union and Nigeria have already taken strides to regulate AI and blockchain by introducing legislation, so a blueprint is already available. [13] However, when South Africa decides to regulate it, context must be a determining factor. Despite these concerns, blockchain and AI are helpful and possess features that copyright holders may leverage to mitigate the ever-growing problem of digital copyright infringement. Consequently, this dissertation aims to provide the various ways AI and blockchain technology can bolster copyright enforcement mechanisms in South Africa.

1.2.Justification and Impact

Considering the expanding digital landscape and the proliferation of copyright-protected online content, there is a pressing need to enhance copyright enforcement mechanisms in South Africa. The current copyright enforcement system faces significant challenges in effectively protecting works, resulting in widespread infringement of creators' rights. This dissertation addresses these shortcomings by exploring the potential of AI and blockchain technology separately in bolstering copyright enforcement measures. By exploring AI and blockchain technology, the study aims to identify innovative approaches that can augment current enforcement strategies and mitigate the inadequacies of the existing copyright enforcement system in South Africa. Through comprehensive analysis and investigation, this research aims to provide valuable insights and practical recommendations for stakeholders. So, to fulfil the objectives of this dissertation, a list of research questions will be outlined below.

---

[12] Surajit Mandal 'Blockchain Technology and Its Effect on Environment: A Comparative Study Between Proof-Of-Work and Proof-of- Stake' (2023) 7 *International Journal of Rural Development, Environment and Health Research* 1–6.

[13] European Union Artificial Intelligence Act 2024 available *at https://artificialintelligenceact.eu/ai-act-explorer/* accessed on 20 July 2024; Nigeria National Blockchain Policy available at *https://nitda.gov.ng/wp-content/uploads/2023/05/National-Blockchain-Policy.pdf* accessed on 20 July 2024.

1.3.Research Questions

To achieve the objectives of this dissertation, the questions below will be answered:

(i) How does South Africa's current copyright legal framework address digital copyright infringement?

This research question examines the effectiveness of South Africa's current copyright legal framework in addressing digital copyright infringement. It aims to analyse the Copyright Act and the current enforcement mechanisms, assessing their adequacy in protecting intellectual property rights in the digital environment.

(ii) What are the inadequacies of the current copyright enforcement system in South Africa, and what are their implications?

Succeeding the first question, this one seeks to identify the shortcomings within South Africa's copyright enforcement system and understand their implications. It involves critically evaluating the system's deficiencies and how these inadequacies impact copyright protection and enforcement.

(iii) How can AI and blockchain technology be leveraged to enhance copyright enforcement mechanisms in South Africa, and what are these technologies' potential benefits and limitations?

Following the identification of the shortcomings of the enforcement mechanisms, this question explores how AI and blockchain technologies can enhance them in South Africa. It aims to investigate the integration of these technologies to improve the detection and prevention of copyright infringement, as well as their benefits and limitations.

(iv) Which recommendations can be provided to ensure the successful implementation of AI and blockchain in copyright enforcement?

Conclusively, this last question provides recommendations for successfully implementing AI and blockchain technologies in copyright enforcement. It involves suggesting legal, technical, and organisational frameworks necessary for effective integration and strategies to overcome potential barriers and ensure sustainable and aligned advancements in South Africa's copyright protection regime.

1.4.Methodology and Scope

This dissertation comprises desktop research, which employs a conceptual legal research methodology. It focuses on existing literature and legislation deliberating on blockchain, AI, and the South African copyright legal framework. It analyses the current enforcement measures against the

various forms of digital copyright infringement to unearth the inadequacies of the enforcement mechanisms. After identifying the inadequacies, this dissertation will discuss AI and blockchain, then table the various ways the two technologies can be utilised to enforce copyright, consider the benefits and limitations of implementing the technology, and provide recommendations. It relies on the existing academic literature and use cases.

1.5. Dissertation Structure

The organisation of chapters is as follows. Chapter 1 will lay the groundwork for the dissertation by giving an overview of what will be discussed. The chapter then delves into the problem statement, highlighting the escalating issue of digital infringements, the inadequacies of current enforcement mechanisms and the need to address them effectively. The significance of the problem is emphasised, underscoring the importance of exploring innovative solutions. Research questions are formulated to guide the investigation into evaluating the enforcement system and proposing viable alternatives.

The second chapter analyses the existing enforcement mechanisms employed to combat digital infringements. Legal frameworks and technological solutions are scrutinised, and the chapter elucidates their inadequacies in effectively addressing the challenges posed by digital copyright infringement. The need for a more robust and efficient enforcement system becomes evident through comprehensive analysis, setting the stage for the subsequent chapters.

Chapter 3 is a comprehensive primer on AI and blockchain technology, elucidating their fundamental features, functionalities, and applications. Readers gain insights into how AI algorithms and blockchain function through detailed exploration. The chapter provides examples of real-world implementations, showcasing the potential of these technologies to revolutionise enforcement mechanisms and mitigate digital infringements effectively.

Chapter 4 delves deeper into integrating AI and blockchain mechanisms for copyright enforcement. Various AI algorithms, including machine learning and deep learning, are discussed to depict their suitability in detecting and combating copyright infringements. Similarly, blockchain features such as immutable ledgers and smart contracts are explored for their potential to establish transparent and tamper-proof copyright enforcement systems. The chapter critically evaluates the benefits and challenges of utilising these technologies, providing a balanced perspective on their efficacy in addressing the shortcomings of current enforcement mechanisms.

The final chapter concludes by offering actionable recommendations to stakeholders based on the

findings and discussions presented in the preceding chapters, also drawing lessons from the European Union (EU), United Kingdom (UK), Malta and United Arab Emirates (UAE), providing vital insight for South Africa in developing balanced, forward-thinking regulatory systems that allow a progressive implementation of AI and blockchain in copyright enforcement. These jurisdictions have been chosen because they have influential regulatory approaches to AI and blockchain. The EU sets a global standard with its AI Act,[14] which prioritises strict risk-based regulation. The UK balances innovation and regulation through a pro-innovation approach that is sectoral. Malta is a pioneer in blockchain legislation, having developed a thorough legislative framework. The UAE demonstrates a dynamic, business-friendly regulatory model, establishing itself as a blockchain powerhouse. Drawing upon insights from the evaluation of enforcement mechanisms and the exploration of AI and blockchain technology, practical strategies are proposed to enhance copyright enforcement in the digital landscape. Considerations for stakeholders are outlined to facilitate the adoption and implementation of practical solutions.

[14] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmenised rules on artificial intelligence and amending Regulations (EC) No 300/2008. (EL) No 167/2013. (EU) No 168/2013. (ED) 2018/858, (RU) 2018/1139 and (FO) 2019/2144 and Direstives 2014/90/EU. (EL) 2016/797 and (BU) 2020/1828 (Artificia Intelligence Act) (Text with PEA relevance) PE/24/2024/REV/1 QJ1.. 2024/1689, 12.7.2024 ELI: http://data.europa.eu/eli/reg/2024/1689/oj

Chapter 2: Analysis of the Current Enforcement System of Copyright in South Africa

2.1.Introduction

The enforcement of intellectual property (IP) rights in the digital environment is a cause for concern.[1] Frustration may be the accurate term to describe the position of copyright holders who intend to enforce the protection of works they made available on the internet, and the growth of technology bore socio-economic fruits but eroded the ground on which IP rights holders exploit their works. The digital shift to online services such as peer-to-peer file sharing, online streaming and online marketplace places paved the way for users' unethical manipulation of technology, disrupting the owners' economic or moral exploitation of works. Illustratively, illegal media streaming takes place when copyright-protected media data is illegally transmitted or received for free to avoid paying for the streams,[2] and unlawful online file-sharing occurs when two or more computers form a network to illegally share copyright-protected files they are not authorised to share by the owner of the files.[3] In response to these and other online infringements, the copyright laws apply.

Although the Copyright Act facilitates the litigious route to enforce IP rights on the internet, it is less effective in preventing the occurrence of online infringements in the first place.[4] It is more reactionary than proactive, and as a result, rights holders resorted to other civil methods like technological protection measures (TPM), algorithmic enforcement, and take-down notices. These measures provide preventative actions rights holders can use to protect their work on the internet. TPMs have two types: access control and copy control.[5] The first ensures that it manages access to copyright works by blocking or limiting access unless an access key is provided.[6] Furthermore, copy control restricts any reproduction of the copyright-protected work.[7] Therefore, TPMs prevent the infringement from taking place in the first place by blocking access unless a key is bought and preventing reproduction.[8]

---

[1] M Jensen 'The Protection of Copyright Works on The Internet - An Overview' (2005) 38 *CILSA* 344-354.
[2] Damilola Ibosiola et al 'Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers' (2018) 12(1) *International AAAI Conference on Web and Social Media*.
[3] Sanjai Goel et al 'The Impact of Illegal Peer-to-Peer File Sharing on the Media Industry' (2010) 56 *California Management Review* 6-33.
[4] Caroline B Ncube 'Copyright Enforcement: The Graduated Response Takes Centre Stage' (2012) 24 (2) *South African Mercantile Law Journal* 133-147.
[5] Visser op cite note 10 CH1.
[6] Ibid.
[7] Ibid.
[8] Malebakeng Agnes Forere 'Keeping Up with The Developments in Technology: A Look into The Music Industry and The Copyright Laws in Southern Africa' (2019) 31 *IPLJ* 31-52.

Despite the use of these enforcement methods, achieving a balance between users and rights owners is a far-fetched reality. Users have been able to outmanoeuvre any form of protection measures. With the help of new technology, they continuously develop tools to circumvent TPMs and use virtual private network (VPN) technology to hide internet protocol addresses to avoid detection and evade liability. However, this does not rule out the intention to achieve the goal of IP laws; hence, to help enforce copyright on the internet, rights holders may use blockchain technology and AI.[9]

This chapter considers why the current copyright enforcement mechanisms are inadequate to address digital infringement. First, it will briefly outline infringement, the types of copyright infringement and their examples. Secondly, it discusses the current enforcement of the mechanism in South Africa. Lastly, an analysis of mechanisms to evoke the gap that renders the current enforcement measures of copyright inadequate in the digital space.

2.1.1. Copyright Infringement

2.1.1.1. Direct Infringement

Direct copyright infringement occurs when a person, who does not hold the owner's permission, performs or causes someone else to perform any of the acts exclusively reserved for the copyright holder. These acts such as reproducing, distributing, adapting, or publicly performing the work are enumerated in the Copyright Act.[10] It is important to note that infringement does not just arise due to the occurrence of the unauthorised acts stated above. Still, certain elements must be determined for reproduction, adaption, etc, to be deemed infringing. Under that, courts developed a test to determine whether copyright infringement by reproduction occurred, which will be expanded below.

2.1.1.2. The Objective Similarity

In South African copyright law, objective similarity is central to determining whether an alleged infringing work unlawfully reproduces or copies an original work. This concept does not require that the two works be identical in every respect; instead, it focuses on whether a reasonable, objective observer would recognise a similarity in the creative expression or the "substantial part" of the original work.[11] The test for objective similarity involves quantitative and qualitative assessments, ensuring that the copied material is not merely incidental or trivial but strikes at the heart of the work's creative essence. The judicial approach in South Africa emphasises that the measure of objective

[9] Custos 'Custos Use Case: Document Protection', *Custos Media Technologies* available at *https://www.custostech.com/blogchain/custos-use-case-document-protection/* accessed on 12 September 2022; Daniel Seng 'Detecting and Prosecuting IP Infringement with AI can the AI Genie Repulse the Forty Counterfeit Thieves of Alibaba?' 2019 *Artificial Intelligence and Intellectual Property* 292–320.
[10] S23(1) of the Copyright Act.
[11] *Moneyweb v Media 24 [2016] 3 All Sa 193 (GJ).*

similarity is not a rigid, numerical comparison of elements but a holistic analysis of the work's overall impression. Courts evaluate whether the alleged infringing work reproduces distinctive, novel, or striking elements of the original work that contribute significantly to its character.[12] This means that even if the allegedly copied elements constitute only a portion of the work, they may be considered sufficient to establish infringement if they are the "soul" or the most original parts. The focus is on the quality and significance of the reproduced material rather than solely on the quantity.

2.1.1.3.The substantial part

The term "substantial part" does not refer solely to the volume or quantity of the material copied but places significant emphasis on the qualitative importance of what has been taken. The copied segment must embody the original work's creative essence or distinctive character. In assessing what constitutes a "substantial part," South African courts have examined whether the copied elements are novel, striking, or central to the work's overall expression. For example, in *Galago Publishers v Erasmus,* the court analysed whether the defendant's work contained quantitatively significant elements and, more importantly, qualitatively central to the original work's identity.[13] The judgment clarified that even if only a portion of a work is reproduced, that portion might still be "substantial" if it captures the core creative contribution of the original. This approach protects the genuine creative contributions of authors without extending copyright to common or generic elements.

2.1.1.4.Causal connection

Equally important is establishing a causal link between the original work and the alleged infringing work. This element of the infringement analysis mandates a direct connection showing that the infringing work was derived from the original work rather than being the result of independent creation. The causal link goes beyond mere similarity; it requires evidence that the defendant had access to the original work and that the similarities can be traced back to that source. In the *Galago Publishers'* case, the court emphasised that a successful infringement claim must demonstrate that the distinctive features of the original were not coincidentally similar but were in fact reproduced in the infringing work.[14] By focusing on the necessity of a causal relationship, the ruling safeguarded against claims based on coincidental resemblances or using elements that were not uniquely original.

---

[12] Ibid.
[13] *Galago Publishers (Pty) Ltd and Another V Erasmus*
[1989] 1 All SA 431 (A).
[14] Ibid.

2.1.1.5.Indirect infringement

Indirect infringement occurs when a person, without the copyright owner's license and while the work remains protected, engages in commercial activities that facilitate or propagate an infringing copy, even though they may not have directly reproduced the work. Section 23(2) specifies that such infringement includes acts like importing an article into the Republic for any purpose other than strictly private and domestic use, and selling, letting, or offering for sale or hire any article that if produced domestically would have constituted a direct infringement.[15] Additionally, indirect infringement covers situations where someone distributes infringing copies to a degree that prejudicially affects the copyright owner's economic interests or where an individual knowingly acquires an article related to a computer program because its production was infringing. Central to establishing indirect infringement is the requirement of "guilty knowledge" – the infringer must be aware, or should reasonably be aware, that their actions are connected to an infringement, thereby enabling the economic exploitation of the copyrighted work without authorisation.[16]

2.1.1.6.Contributory Infringement

In copyright law, this type of infringement refers to holding a person legally accountable for directly infringing on a copyright and assisting, aiding, or abetting the infringement committed by another. Essentially, suppose copyright infringement is recognised as a delict, a wrongful act that causes harm. In that case, the liability of a party facilitating the infringement is determined under the broad principles of the Aquilian action. Under this common-law framework, liability is not limited to the direct perpetrator; those who contribute in any way to the commission of the infringement, even if they do not execute the infringing act themselves, can be held responsible for the damage caused. In such cases, the remedies available to a plaintiff, including damages and injunctive relief (an interdict), are the same as those for direct infringement.[17] Importantly, when a claim for contributory infringement is based on an award of damages, it is necessary to show some form of fault or knowledge on the part of the contributor.

Contributory infringement becomes particularly relevant in internet service providers (ISPs), where questions arise over whether these intermediaries should be treated as neutral conduits or entities that actively facilitate infringing activities. While some argue that ISPs merely provide the technical means for content distribution without curating or altering the data thus acting like "postmen" others contend that if they knowingly assist in transmitting or storing infringing content, they should bear

[15] Copyright Act 98 of 1978.
[16] Klopper et al *Intellectual Property Law In South Africa* 2 ed (2016).
[17] Ibid.

some liability.[18] Under the principles of contributory infringement, if an ISP is found to have the requisite knowledge of infringement and has taken steps that assist or enable the infringement, it might be held liable as seen in the *Napster* case where *Napster* was held liable for aiding copyright infringement through their file sharing platform.[19] This potential liability highlights the delicate balance the courts must strike between protecting the rights of copyright owners and ensuring that the infrastructure providers who facilitate communication on the Internet are not unduly burdened with liability.

2.2. Types of copyright infringements

2.2.1. Unauthorised Reproduction

Unauthorised reproduction is copying-protected works without the owner's permission. To define the term reproduction, in *Blind SA v Minister of Trade, Industry and Competition* the court reiterated Professor Dean explaining that "reproduction" under the Copyright Act is defined broadly enough to encompass the conversion of a work into another accessible format without altering its fundamental content or ideological essence. According to the court's interpretation, reproduction covers any mechanical process that produces an exact copy of the original work, even if the work is transformed into a different medium, such as converting text into braille.[20] In this context, format shifting does not involve any creative input or modification that would alter the work's substance; it merely presents the same work in a new form. In the digital space, if a musician releases a new album on various streaming platforms, then a user downloads the album illegally from a torrent site. So, by downloading and permanently storing in any storage device, a reproduction of the protected works is created as they would have reproduced the exact copy of the original work.[21] Section 23(1) of the Copyright Act provides that reproducing copyright-protected works without authorisation is a direct infringement.[22] Therefore, unauthorised reproduction falls under direct infringement as it is the direct copying of works.

2.2.2. Unauthorised Distribution

Unauthorised distribution of works is dispensing copyright-protected material without permission from the owner. According to s23(1), distribution is regarded as a direct infringement of copyright.[23]

---

[18] Ibid.
[19] *A&M Records, Inc. v. Napster Inc* 239 F.3d 1004 (9th Cir. 2001).
[20] Blind SA v Ministry of Trade, Industry and Competition and Others (14996/21) [2021] ZAGPPHC 871; 2021 BIP 14 (GP)
[21] Mengna Liang 'Copyright issues related to reproduction rights arising from streaming' (2020) 23(5-6) *Journal of World Intellect Property* 798-814.
[22] s 23(1) of the Copyright Act 98 of 1978.
[23] Ibid.

For example, when a movie is released in theatres, and then someone illegally records the film using a hidden camera. This person then uploads the entire movie to a file-sharing website, making it available for download to anyone with the link. This action constitutes unauthorised copyright distribution, as the individual has no legal right to distribute the movie. Distribution embodies selling, sharing, importing, and exporting unauthorised copies of copyright-protected works.

2.2.3. Unauthorised Performance

Performance of a copyright-protected work becomes unauthorised and a copyright infringement when one broadcasts or communicates to the public the copyright-protected work without the owner's permission. Unauthorised performance commonly occurs when one publicly performs copyright-protected works such as songs, plays, musicals and concerts without authorisation from the works' owner.[13] Section 1 defines performance broadly to include any visual or acoustic presentation of a work, whether via a loudspeaker, radio, television, or even during a live lecture or sermon, thereby ensuring that virtually any public or private presentation falls under the protection of copyright.[24] However, the Act expressly excludes the act of broadcasting or transmitting a work in a diffusion service from being classified as a performance. This distinction is pivotal because it separates traditional live or recorded presentations from modern digital broadcasting methods, which are subject to different enforcement mechanisms and regulatory challenges.

In *Southern African Music Rights Organisation Ltd v Svenmill* Berman AJ clarified that "performance" under the Copyright Act encompasses any visual or acoustic presentation of a work such as that delivered via loudspeakers, radio, or television while specifically excluding acts of broadcasting, rebroadcasting, or transmitting via a diffusion service. Berman AJ explained that although the defendant's music was originally received as a broadcast from the South African Broadcasting Corporation, its subsequent relay through extension speakers in a private factory setting did not qualify as a diffusion service. Instead, by playing the music for its 400 employees during working hours, the defendant was engaging in an acoustic presentation that is unmistakably defined as a performance under Section 1 of the Act.[25] Thus, the court held that the defendant's conduct constituted a public performance of the musical works, infringing the plaintiff's exclusive rights.

2.3.Examples of Copyright infringements

2.3.1. Peer to Peer File Sharing (P2P)

This is based on a computer network structure that allows participants to store information and

[24] Copyright Act 98 of 1978.
[25] *Southern African Music Rights Organisation Ltd v Svenmill Fabrics* (Pty) Ltd 1983 (1) SA 608 (C)

communicate with each other directly in the absence of a central server.[26] Additionally, programmers make the search function available, allowing users to locate any information they want without using the whole database.[27] For example, Napster, a pioneer of P2P file sharing, used a centralised cloud storage facility for users to store and search for files on the network. Moreover, the peers connect to a central database that permits them to publish any information about the content they want to share.[28] As a result, a user interested in this information uses the search mechanism to query the database and then secures the IP address and node, locating the content with the option to download it.[29] So, copyright infringement occurs when people start sharing content they are not authorised to share using the P2P system. Therefore, illegally downloading and uploading copyright-protected content results in an unauthorised reproduction and distribution of copyright.

In conclusion, peer-to-peer file sharing clearly falls under the category of a direct infringement that is, unauthorised reproduction and distribution of copyrighted works. By enabling users to download and upload content without the copyright owner's consent, P2P networks exemplified by platforms such as Napster circumvent traditional distribution channels, leading to widespread infringement. This mode of infringement reproduces and disseminates copyrighted material in a rapid, decentralised manner, challenging conventional enforcement measures. In the *Napster* case, the court ruled that P2P users were directly liable for infringing copyrights by sharing unauthorised content, while Napster was held responsible for facilitating the infringement by providing the platform that enabled such sharing.[30]

2.3.2. Bit torrent

It is a technology that uses the BitTorrent client software to allow users to upload and download files from multiple users instead of one.[31] For easy download, users split the files into smaller packets. In downloading the content, the user must obtain a torrent file from a BitTorrent index containing information about different file locations, enabling one to download files simultaneously from multiple users.[32] Pirates Bay is an example of a BitTorrent index that facilitates the unauthorised sharing of copyright-protected content. Consequently, direct copyright infringement, like unauthorised reproduction and distribution, occurs when copyright material is made available for

[26] OH Dean & Alison Dyer *Dean & Dyer: Introduction to Intellectual Property Law* 1 ed (2014) available at *https://search-ebscohost-com.ezproxy.uct.ac.za/login.aspx?direct=true&db=nlebk&AN=2175219&site=ehost-live* accessed on 20 July 2024.
[27] Goel op cite note 3 at 12.
[28] Ibid.
[29] Dean & Dyer op cite note 27.
[30] Napster case.
[31] Ibid.
[32] Ibid

download or uploaded without the copyright holder's permission.

2.3.3. Linking

It occurs when one creates a link from one page to another using a hypertext link. However, creating a link does not guarantee the occurrence of copyright infringement because the words used in the link are not sufficient to constitute a work along with the Uniform Resource Locator. The copyright infringement from linking is quite complex to decipher in that one must have provided a link that bypasses the home page, taking the user straight to internal pages.[33] The technical explanation for the infringement denotes altering the website sequence in which its owner may have intended the website to appear.[34] Furthermore, via linking, owners of content experience bypassing paywalls, users gaining access without paying for the license and allowing competitors to misuse their work.

Conclusively, linking falls under the category of indirect copyright infringement. Although creating a hypertext link on its own does not constitute infringement, liability arises when the link is structured to bypass the website's homepage and direct users straight to internal pages thereby altering the intended sequence and economic environment of the site. Such linking effectively circumvents paywalls and license controls, enabling unauthorised access to copyrighted content and causing economic harm to the rights holder. This nuanced form of infringement is not about copying the content itself, but about facilitating access in a manner that undermines the copyright owner's control.

2.3.4. Framing

When an operator of a website includes a large part of another operator's website on theirs to look as if it is one website, framing occurs.[35] In that regard, the operator responsible for website hosting the frame provides a link by displaying the linked contents on their site, arguably preparing derivative work.[36] As a result, the frame that the secondary website operator wants visitors to use is distorted by framing because they would access the contents through the primary website.[37]

2.3.5. Illegal Streaming

Illegal streaming involves the unauthorised distribution or transmission of copyrighted content over

---

[33] Nicole M Bond 'Linking and Framing on The Internet: Liability Under Trademark And Copyright Law Note' (1998) 11 *Depaul Business Law Journal* 185–228.
[34] Ibid.
[35] Van Der Merwe *Information and Communications Technology Law* 2nd ed (2016) available at *https://search-ebscohost-com.ezproxy.uct.ac.za/login.aspx?direct=true&db=nlebk&AN=2139885&site=ehost-live* accessed on 20 July 2024.
[36] Bond op cite note 34.
[37] Ibid.

the Internet.[38] It typically occurs through websites or platforms that offer access to movies, TV shows, music, or other copyright-protected material without proper licensing or permissions from the copyright holders. Users access this content without paying for it or without the rights to do so, violating the exclusive rights of the copyright owners. As a result, illegal streaming is an example of the unauthorised distribution of copyright-protected content.

As a result of the above, each of these examples whether it is the decentralised file sharing seen in P2P networks or the multifaceted approach of BitTorrent, linking, framing, and illegal streaming demonstrates the increasingly sophisticated tactics that digital infringers employ. This evolution in infringing practices starkly contrasts with the enforcement measures currently in place, which remain anchored to traditional frameworks. The discrepancy is evident: while technology has enabled infringers to innovate and circumvent conventional safeguards, the enforcement mechanisms have not kept pace. This gap highlights a critical need to adopt more adaptive, technology-driven solutions, powered by AI and blockchain, to effectively protect copyright in the rapidly evolving digital landscape.

2.4.Current Enforcement Mechanisms

Enforcing copyright can be approached from a litigation standpoint. One can initiate court proceedings upon noticing that their rights are infringed by the other party and obtain relief. Civil remedies are actionable through s24 of the Copyright Act, which provides that a copyright holder can sue anyone who infringes their copyright for relief, such as an interdict, damages, accounts, or delivery of infringing copies or plates used or intended for infringing purposes.[39] Since copyright infringement falls within the bracket of delict, the principles of delictual liability do not change when one seeks an award of damages due to the infringement.[40]

2.4.1. Cease and Desist Letter

Copyright holders usually enforce their rights by sending cease and desist letters to the person infringing on their copyright, informing them to stop the copyright infringement act. This is usually the first point of enforcing their copyright against infringers. A cease-and-desist letter is a document drafted and sent to a third party by a copyright holder, demanding they discontinue activities that violate their copyright. It provides a key advantage of swiftness by offering copyright holders a rapid,

[38] Tan Winsherly 'TV Broadcast Piracy Through Illegal Live Streaming Applications: Challenges and Legal Protection for Copyright Holders' 9 *Al-Adalah: Jurnal Hukum dan Politik Islam* 66-79.
[39] s24.
[40] Klopper et al *Law of Intellectual Property In South Africa* 2 ed (2016) available *at https://search-ebscohost-com.ezproxy.uct.ac.za/login.aspx?direct=true&db=nlebk&AN=2139897&site=ehost-live* accessed on 20 July 2024.

method to alert potential infringers and demand an immediate halt to unauthorised activities. This immediate action can prevent further economic loss and deter future violations without resorting to lengthy court proceedings if the alleged infringer ceases infringement upon receiving the letter.

2.4.2. Damages

To claim damages, the fault must be proved on the part of the infringer. It must be evident that when the infringement was committed, the alleged infringer was aware that the works were copyright protected and that they were infringing the copyright in the work. As evidenced by s24(2), the plaintiff is not entitled to damages if the alleged infringer was unaware of the copyright protection in the work when the infringement occurred. The purpose of awarding damages is to compensate the proprietor for the patrimonial loss sustained through the infringement. For example, in *Moneyweb v Media 24*, the court held that Media 24 infringed the copyright when it published an article on the 16th of January 2013.[41] Moreover, it granted damages in favour of the applicant regarding one article whose copyright was infringed. Additionally, damages offer the benefit of compensation, a direct financial remedy for the harm sustained when infringement occurs, as demonstrated in *Moneyweb v Media24*.

2.4.3. Notional Royalties

A copyright holder may seek damages in lieu of damages in an amount calculated based on reasonable royalties. A reasonable royalty is an amount that would have been paid had the infringer bought a license to use the work. In claiming notional royalties, the claimant is not required to prove that there was actual damage when invoking s24(1B).[42] The appellant in *Feldman NO v. EMI Music Publishing SA* requested an order for damages equal to the royalties that would have been justifiably payable by a licensee of the copyright, and the SCA granted, indicating that the provision was inserted to cover such a contingency where the appellant claimed the respondent received royalties from acts of the infringement.[43] Notional royalties deliver efficiency by establishing a fee, based on what a license would have been, bypassing the need to prove actual economic loss.

2.4.4. Delivery Up

If the defendant still possesses the items they used to violate the plaintiff's copyright after the court issues an interdict prohibiting the defendant from doing so, a delivery up works as a mechanism to hinder the defendant from disregarding the interdict and committing further acts of infringement. [44] Resultantly, the plaintiff is granted permission to cease the goods the defendant was using to perform

---

[41] *Moneyweb* case.
[42] Klopper op cite note 41; *CCP Record Co* (Pty) Ltd *v Avalon Record Centre* 1989 (1) SA 445 (C). The judge awarded the plaintiff R3000 in additional damages.
[43] *Feldman No v Emi Music SA* (Pty) *Ltd* [2009] 4 All SA 307 (SCA).
[44] s24 (1).

acts of infringement. The purpose of a delivery up is to enhance the efficacy of the interdict by depriving the infringer of the means to perform acts of infringement. Delivery up orders ensure the removal of infringing materials, directly curtailing continued violations.

2.4.5. Criminal remedies

Apart from civil remedies, s27 of the Copyright Act criminalises acts of copyright infringement, providing the remedies under the provision. Section 27 states that anyone who engages in activities such as selling, distributing, exhibiting, importing, or possessing infringing copies of copyrighted works will be guilty of an offence. Additionally, causing a copyrighted work to be performed in public, rebroadcast or transmitted without permission, or distributing program-carrying signals without authorisation is also considered an offence.[45]

The penalties for these offences include fines and imprisonment, with the severity depending on the nature of the offence and whether it is a first conviction or not. For example, the Commercial Crimes Court convicted Majedien Norton of copyright infringement. It gave him a five-year suspended prison sentence without a fine. Norton uploaded a movie called Four Corners on the internet, sharing it with the public without the copyright holder's permission.[46] Resultantly, imprisonment and fines serve as alternatives to civil remedies which can be used to enforce copyright.

Sections 24 and 27 provide methods of enforcing copyright. Under s24 the copyright holder has the right to use civil remedies outline above which are provided for by the act to hold the infringer accountable. On the other hand, the state may invoke s27 to hold the alleged infringer accountable in a commercial crimes court as seen in the Four Corners case where Norton was sentenced to imprisonment. Finally, the advantage of criminal remedies is that they deter wilful infringement through fines or imprisonment.[47]

2.4.6. Technological Protection Measures (TPM)

TPMs are applications employed to control the public's interaction with digital content. They block unauthorised access to or use of digital content unless the content owner grants it.[48] Due to their vulnerability, international and national laws have been put in place to protect the circumvention of

---

[45] s31.
[46] Jan Vermeulen 'How SA's first online pirate was caught' available at *https://mybroadband.co.za/news/internet/103875-how-sas-first-online-pirate-was-caught.html* accessed on 13 September 2022.
[47] Vermeulen op cit note 47.
[48] Tobias Schonwetter & Caroline Ncube 'New Hope for Africa? Copyright And Access to Knowledge in The Digital Age' (2011) 13 *Info* 64–74.

TPMs by the public. As stated above, there are two types of TPMs, and the various examples of TPMs rights holders use to protect their digital works include password protection, dongles, online movie rental, secret handshakes, and watermarking.

2.4.6.1.Password Protection

Password protection is one of the standard methods of protecting digital content using TPMs. It protects various types of copyright works, from software to personal emails.[49] It controls access to copyright-protected material by requiring a user to enter a password first to gain access to the contents of the copyrighted material.[50] Illustratively, authors who publish e-books on a digital platform may invoke the platform to implement a password protection system to protect the content from unauthorised access and distribution. So, when a user purchases the e-book, they receive a unique password to open and read the file. Hence, it restricts unauthorised access and prevents unauthorised users from copying the copyrighted content.

2.4.6.2.Secret Handshakes

It includes a secret handshake protocol set between the authorised user application and the server to ensure content is only streamed directly to the authorised user application, preventing copying. Most secret handshakes involve the challenge-response sequence to authenticate the user.[51] The user will first initiate a connection by entering their details. After receiving the request from the user, the server will send a message containing the challenge, which takes the form of a number.[52] When the user gets the number, they are supposed to enter it, and then the server will compare the number entered by the user with the one stored in its system, and once the two correspond, the user is granted access.[53]

2.4.6.3.Online Movie Rental Protection

The technology allows users to rent movies online for a certain period, and then when a specific period lapses, the system automatically deletes the movie from the user's computer.[54] This protection is achieved through the Moving Picture Expert Group Rights Expression Language (MPEG REL), a rights expression language used to control the distribution and access to digital content.[55] It connects the XML reader and extra metadata to every file MPEG REL will control.[56] Although data can still be copied, once a specific period lapses, the movie is deleted from the system, and iTunes uses this

[49] Ryan Iwahashi 'How to Circumvent Technological Protection Measures Without Violating the DMCA: An Examination of Technological Protection Measures Under Current Legal Standards' (2011) 26 *Berkeley Technology Law Journal* 491-526.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] Ibid.

system.[57]

2.4.6.4.Watermarking

It is watermarking the act of adding an undetectable signal to the work created. As a result, each work produced is marked with a watermark, and each is unique such that whenever an illegal copy is in public, it can be traced back to the original one. Therefore, watermarking aims to help track unauthorised copies of one's works.[58]

In essence, TPMs offer substantial control over digital content. For instance, password protection provides robust security by ensuring only authorised users can access the content. Similarly, secret handshakes deliver precise authentication through challenge-response protocols that verify user legitimacy. At the same time, online movie rental protection enforces a strict time limit, automatically revoking access after the rental period lapses. Watermarking further enhances traceability, embedding unique identifiers into works to track and identify unauthorised copies.

2.4.7. Encryption

Encryption is converting data into a code to prevent unauthorised access. In the context of copyright content in the digital space, encryption serves as a TPM by encoding the content, making it unreadable without the decryption key. This helps safeguard copyright-protected material from being accessed, copied, or distributed without proper authorisation. Encryption ensures the integrity and confidentiality of digital content, deterring copyright infringement and unauthorised use, thereby preserving the rights of content creators and owners in the digital realm. Encryption is key in ensuring confidentiality by converting content into a secure code that remains inaccessible without the proper decryption key.

2.4.8. Take Down Notice

A take-down notice is a procedure outlined in the Electronic Communication and Transactions Act (ECTA) in which a person makes an internet service provider (ISP) aware of any content that infringes their rights and requests them to take it down immediately.[59] In essence, intermediaries like ISPs must comply with the take-down notice once they know it; otherwise, they will be held liable. In notifying the intermediaries, s77 of the ECTA requires an individual to address the complaint of unlawful activity in writing. It must include their full names, signatures, identification of the infringed right, identification of the material infringing the right, etc.[60] The Take Down Notice mechanism offers

[57] Ibid.
[58] Ibid.
[59] s77 of the Electronic Communications and Transactions Act 25 of 2002.
[60] Ibid.

swift responsiveness, compelling intermediaries to remove infringing content once notified.

2.4.9. Algorithmic Enforcement

The term "algorithmic enforcement" in the context of copyright refers to using technology and automated algorithms to track down and stop copyright violations online. Copyright owners and ISPs have looked for measures to protect IP and prevent the unauthorised use of copyright-protected works in response to the growth of digital content-sharing platforms and the simplicity with which copyright-protected products may be copied and distributed.

Automated notices sent by copyright holders based on internet monitoring systems represent the first wave of automated copyright enforcement.[61] The proliferation of illicit content online made it more challenging for humans to monitor it, which was a significant factor in introducing automated notices. The automated notification systems work by scouring the internet for unlawful content and notifying the relevant internet platforms to remove it.[62] Online platforms executed an automated removal in response to the notices due to the high volume of notices.

Voluntary filtering is the second wave of automated copyright enforcement. This technology compares all user-uploaded content with content for which copyright holders have requested protection.[63] The platforms allow the copyright holders to prohibit the content once the infringing content has been detected. For instance, a similar content screening method is used by YouTube, where each piece of content submitted by users is checked to see whether it matches any copyright-protected content and is rejected if it does.[64] In conclusion, copyright holders in South Africa utilise algorithmic enforcement as part of their digital copyright-enforcing tools to manage how the public interacts with their work without violating their rights.

Finally, Algorithmic enforcement bolsters efficiency by automating the detection and removal of unauthorised content across digital platforms, enabling copyright holders to manage large volumes of content with greater accuracy and speed.

2.5.Inadequacies Of the Current Enforcement Methods

The enforcement mechanisms outlined above are beset by more inefficiencies than efficiencies that create exploitable gaps, leaving rights holders at a disadvantage in the digital realm. Protracted legal

---

[61] Maria Lillã 'Virtues and Perils of Algorithmic Enforcement and Content Regulation in The Eu - A Toolkit for A Balanced Algorithmic Copyright Enforcement' (2019) 11(1) *Journal of Law, Technology & The Internet* 3-47.
[62] Ibid.
[63] Ibid.
[64] Joanne Gray & Nicolas Suzor 'Playing with machines: Using machine learning to understand automated copyright enforcement at scale' (2020) 7 (1) *Big Data & Society* 1-13.

proceedings and exorbitant litigation costs render the judicial route impractical for many, particularly independent artists and small companies. These actors are often forced to abandon legal action due to the financial and temporal burdens imposed by the traditional court system. Simultaneously, the rigidity of an outdated Copyright Act which has not kept pace with rapid technological advancements further exacerbates these challenges, as it fails to adequately address the nuances of digital infringement. This inflexibility, coupled with the system's inability to quickly update or incorporate modern enforcement tools, results in a fragmented and sluggish response to copyright violations. The enforcement gap is widened by circumvention tactics such as VPNs and brute-force attacks on TPMs, which enable infringers to bypass established safeguards with relative impunity. Such systemic shortcomings not only dilute the deterrent effect of copyright law but also embolden infringers to exploit these vulnerabilities, thereby undermining the overall integrity of the enforcement framework. Below is a discussion of these shortcomings indicating the gap they create in enforcement, which in turn is exploited by infringers.

2.5.1. Lengthy and Costly Legal Proceedings

Litigious remedies, like suing copyright infringers can be time-consuming and expensive. Due to the significant costs, it may be difficult for smaller copyright holders or lone artists to file a lawsuit, making it difficult for them to safeguard their rights successfully. Klaaren reiterated Judge J Makume's words that South Africans fail to access justice due to the inability to afford lawyers, or if they can afford their funds, they run dry as the individual fails to sustain the costs of continued litigation.[65] The legal costs may include fixed fees levied by the state to the general populace for access to various public processes like filing paperwork in court, litigious tariffs governed by the rules board and taxed, and the largely unregulated tariffs levied by practitioners for legal services related to transactions and litigation.

As stated above, the high cost of legal proceedings makes it difficult for individuals or small companies to enforce their copyright through legal processes because of affordability issues, causing some to abandon this method and try other channels.[66] Furthermore, legal proceedings are time-consuming due to the court procedures that must be followed when initiating them. The stages of litigation include the exchange of pleadings, the pretrial preparation and the trial and enforcement. In approximation, this may take years to settle, and with costs piled up, the copyright holder might suffer a more extensive patrimonial loss than the one they suffered because of the infringement.

---

[65] Jonathan Klaaren 'What Does Justice Cost In South Africa? A Research Method Towards Affordable Legal Services' (2019) 35 *South African Journal on Human Rights* 1–14.
[66] Ibid.

As a result, online infringers frequently exploit the drawn-out, expensive litigation process, knowing that copyright holders are often dissuaded from pursuing enforcement due to high legal costs and prolonged court battles. For example, in the while the legal battle against Pirate Bay continued, the site did not shut down and copyright infringement continued as user continued to upload and download copyright protected content.[67] This highlights how the cumbersome nature of copyright litigation creates an opening for infringers to maintain unauthorised use while copyright holders hesitate to invest the significant resources needed for full legal recourse.

2.5.2. Slow Legislative Updates

The main piece of legislation enforcing copyright in South Africa is the Copyright Act of 1978. Given how quickly technology develops, this act needs to be revised to adequately solve the modern digital world's problems. Slow legislative revisions can make it difficult for enforcement to handle new issues effectively. Amending the Copyright Act has taken over a decade, beginning in 2009, and the draft amendments were published for commentary in 2015.[68] Since then, talks have been ongoing, and to date, the president has not signed the amendment bill into law. With enforcement being one of the issues that need to be addressed because of digital advancements, the slow legislative update of the Copyright Act makes it difficult for copyright holders to enforce their copyright in the digital age. For example, the current Copyright Act does not allow a wide range of works to be used, even if the use is non-infringing.[69] This means that even if the intention is good and the use is non-infringing, like research or education, the act will still be deemed infringing. Moreover, with data-reliant technology progressing, such a strict provision stifles innovation and development and defeats the whole IP purpose of finding a balance between consumers and creatives. The area of AI relies heavily on data to train its models. With the current fair dealing provision, researchers cannot use copyright-protected works to improve the technology further. As a result, slow legislative updates contribute to the copyright enforcement system's struggle to tackle digital copyright infringement.

2.5.3. Circumvention

Although the law criminalised the circumvention[70] of TPMs, more is needed to stop individuals from doing so, knowing they can succeed without detection by the copyright holders who put the measures in place. To illustrate, TPMs such as password protection are bypassed by using a brute-force attack.

---

[67] Karl Ritter 'Pirate Bay moves from Sweden to Norway, Spain' The Sunday Morning Herald available at https://www.smh.com.au/technology/pirate-bay-moves-from-sweden-to-norway-spain-20130227-2f4y1.html accessed 24 February 2025.
[68] Denise Rosemary Nicholson 'The Copyright Amendment Bill: Its Genesis and Passage Through Parliament' InfoJustice.org available at *https://infojustice.org/archives/41167* accessed 14 September 2022.
[69] s 12 of the Copyright Act.
[70] s7 of the Cybercrimes Act 19 2020.

It uses a trial-and-error method, guessing the login combination to a protected work until it attains the correct one.[71] Therefore, such a weakness plays a part in rendering the enforcement of copyright law inadequate because if users can still bypass measures to stop them from infringing the owner's rights, the measure is not fully serving its purpose.

Further examples include the use of VPNs to remain undetectable. This makes it hard for online service providers to track down the person responsible for the infringement so that they can block their internet protocol address from accessing digital content unauthorised. VPNs hide a person's internet protocol, so their internet activity cannot be tracked even by the ISPs.[72]

In conclusion, while the law criminalises the circumvention of TPMs, practical enforcement remains severely weakened because these safeguards are too easily bypassed. For example, infringers use brute-force attacks to overcome password protections and employ VPNs to hide their identities, enabling rapid and widespread unauthorised distribution of copyrighted material. Similarly, linking and framing techniques effectively sidestep TPMs by redirecting users to internal pages or embedding external content directly within a website, thus subverting intended access controls. Illegal streaming platforms further illustrate this vulnerability, as users exploit these technical loopholes to stream protected content without detection, undermining the system's deterrence capabilities. Ultimately, these circumvention methods not only allow infringers to evade detection and legal recourse but also exacerbate the scale of digital copyright infringement, highlighting an urgent need for more robust, adaptive enforcement solutions.

2.5.4. Accessibility Concerns

TPMs raise concerns about limiting access to information by failing to accommodate the non-infringing use of copyright material. The problems lie in the TPMs' failure to distinguish between uses for non-infringing purposes and infringing purposes.[73] TPMs block access, meaning that if one wants to use the protected works for educational purposes, they cannot because the TPMs cannot distinguish whether the use is for non-infringing purposes.[74] As a result, should one decide to circumvent the TPM for non-infringing purposes, the Cybercrimes Act criminalises the act despite the intention behind it because circumvention of TPMs is a violation distinct from copyright

[71] Iwahashi op cit note 49.
[72] Kasperskey 'Brute Force Attack: Definition and Examples', *Kaspersky.Com* available at *https://www.kaspersky.com/resource-center/definitions/brute-force-attack accessed* 10 July 2022.
[73] Schonwetter & Ncube op cite note 48.
[74] Ibid.

infringement.[75]

Section 12 of the Copyright Act outlines that some of the few non-infringing purposes for using copyright-protected works are for research or private study purposes[76]; therefore, using copyright-protected works for this purpose would not amount to an infringement and is not prohibited. However, usage and access are two different acts in which s12 provides exceptions for usage only. So, since no provision in operation permits the circumvention of TPMs for non-infringing uses of copyright-protected material, unlawfully accessing works remains a violation of the Cybercrimes Act, even if the purpose of the use is non-infringing.[77]

Although yet to be in operation, it must be noted that the Copyright Amendment Bill B13F 2017 (CAB) inserts sections 28O and 28P, which address the abovementioned issue. On the one hand, s28O prohibits the circumvention of TPMs.[78] Conversely, s28P provides the exceptions and limitations, which will be deliberated further. This section permits individuals to use TPM circumvention devices or services for lawful purposes, including those exceptions specified within the Act.[79] It also allows the sale, distribution, and possession of devices or data designed to bypass security measures, provided these actions enable lawful uses as described.
Additionally, when someone engages another person to assist in circumventing technological protections, they must keep detailed records of the assisting person's identity and the purpose of the circumvention. This ensures transparency and accountability while allowing circumvention for legitimate, legally permitted activities. Once the CAB comes into effect, users will be permitted to circumvent TPMs to legally access copyright-protected works for non-infringing purposes.

However, the Cybercrimes Act currently takes centre stage in regulating any act of circumvention of the TPMs to gain unauthorised access to protected works.[80] For this reason, the only lawful way to access copyrighted works protected by TPMs is through the owner. In conclusion, the failure to regulate the circumvention of TPMs to accommodate uses permitted by s 12 undermines the purpose of copyright law. Rights are not absolute and are subject to reasonable and justifiable limitations; however, in the case of TPMs, the public's rights are somehow negated.

[75] s7 of the Cybercrimes Act.
[76] s12 of the Copyright Act.
[77] s7
[78] s28O of the Copyright Amendment Bill B13F 2017.
[79] s28P.
[80] s7 of the Cybercrimes Act.

Conclusively, this over-blocking forces users, who may simply wish to access content lawfully, to resort to circumvention techniques, thereby triggering penalties under the Cybercrimes Act even when their intent is non-infringing. Such rigid enforcement exacerbates digital infringement scenarios: for example, the inability to access content through authorised channels drives users to bypass TPMs, which in turn fuels unauthorised distribution; similarly, linking and framing, which could be used to provide lawful access or enhance information dissemination, become contentious when TPMs prevent their proper use. Ultimately, until legislative updates like those proposed in sections 28O and 28P of the Copyright Amendment Bill are implemented, the current framework forces a situation where users access to information is unduly curtailed, inadvertently intensifying the cycle of infringement in the digital space.

2.5.5. Non-compliance

Enforcing IP rights by way of litigation may be faced with non-compliance. After the court orders the infringing party to cease their copyright-infringing activities, they may decide not to comply. As a result, this makes litigation a fruitless attempt because an online platform may choose to relocate to another jurisdiction and continue hosting unlawful content on its platform. Alternatively, the individual may use a VPN application to hide their internet protocol address and continue engaging in infringing content without being detected. To add, the affected party may contemplate invoking s77 of the ECTA to have the content taken down; however, because a VPN hides one's internet protocol address, it will be a futile exercise to identify the person's internet activity because even the ISP will not be able to locate it.[81] More so, an individual ordered to pay damages may contest, indicating that they do not have the money to pay for the damages.[82]

Non-compliance in the digital realm critically undermines copyright enforcement by rendering judicial orders ineffective, as infringers routinely evade penalties by relocating platforms across jurisdictions or using anonymising tools like VPNs. For example, in cases where courts have ordered the cessation of illegal streaming or unauthorised file sharing, infringers have simply shifted their online operations to regions with lax enforcement or concealed their identities, much like the widely reported phenomenon seen with platforms such as Pirate Bay.[83]

---

[81] VPN.com 'Can My Internet Provider See My VPN?' available at *https://www.vpn.com/faq/isp/* accessed 10 July 2022.
[82] Ncube op cite note 4.
[83] Ritter op cite note 68.

2.5.6. Algorithmic Bias

2.5.6.1.False Negative

False negatives occur when an algorithm fails to detect and flag infringing content. For example, algorithmic enforcement that detects pirate websites mainly does so by identifying advertising banners on the website.[84] However, infringers use specific static keywords in the web banners to bypass the algorithm detection, making it difficult for algorithmic systems to determine between a legitimate and a pirate website, and such instances fall under false negatives where the system fails to detect and flag the infringing content whereas it will be infringing.

2.5.6.2.False Positive

False positives occur when a system detects the presence of something which is not there. In algorithmic enforcement, a false positive emerges when the algorithmic system flags uploaded material as copyright-infringing content, which it is not.[85] Algorithmic bias may arise due to a mismatch between the intended target the algorithm should be predicting, and the biased proxy variable the algorithm is predicting. Furthermore, correcting algorithmic decision-making after flagging and filtering the wrong content is challenging because the system lacks accountability due to its opaqueness caused by the non-transparent complex code that even programmers fail to understand.[86] In a nutshell, algorithmic enforcement can produce biased results, such as false positives or negatives. This affects the accuracy of algorithmic enforcement as it can either fail to filter infringing content or non-infringing content.

Resultantly, algorithmic enforcement, despite its potential, often falls short in effectively curbing digital copyright infringement due to its susceptibility to false negatives and false positives. False negatives allow infringing activities such as illegal streaming to persist undetected when infringers deliberately alter or obscure identifying markers, such as modifying web banners. This evasion enables unauthorised reproduction and distribution to continue unchecked. Conversely, false positives result in legitimate content being mistakenly flagged, which not only disrupts lawful activities but also creates a chilling effect on content sharing and user rights. In the context of illegal streaming, these enforcement flaws mean that infringing content might slip through undetected or, alternatively, legal content might be improperly taken down, thereby exacerbating the infringement landscape.

---

[84] Lelisa Adeba Jilcha & Jin Kwak 'Machine Learning-Based Advertisement Banner Identification Technique for Effective Piracy Website Detection Process' (2022) 71 *Computers, Materials & Continua* 2883–99.
[85] Cheng-Yuan Ho et al. 'Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems' (2012) 50 *IEEE Communications Magazine - IEEE Commun. Mag.* 146–54.
[86] Lillã op cite note 61.

To summarise the discussion above, linking enforcement shortcomings to infringement examples underscores a critical misalignment between rapid, cost-effective nature of digital infringement and the sluggish, expensive mechanisms currently in place to combat it. For instance, P2P networks and BitTorrent facilitate file sharing by leveraging the low cost and near-instantaneous speed of digital distribution, enabling vast amounts of copyrighted material to be shared quickly and anonymously. However, when such infringement occurs, pursuing legal remedies is time-consuming and prohibitively expensive factors that starkly contrast with the ease of digital replication. Similarly, methods such as linking and framing can bypass outdated TPMs, while modern algorithmic enforcement struggles with the inherent complexity of these methods, often resulting in false positives or negatives. This disparity between the high-speed, low-cost mechanisms employed by infringers and the slow, costly legal processes available to copyright holders creates significant gaps in protection, justifying the relevance of more agile and technologically advanced enforcement solutions leveraging AI and Blockchain.

2.6.Conclusion

First, the current copyright enforcement mechanisms must be improved to tackle online infringement. Although they have proven to be functional, they are struggling to cope with the occurrence of infringements taking place online, and as a result, this has left IP rights proprietors frustrated. Activities like circumvention continue to outmanoeuvre TPMs even if there are laws that criminalise them. Users have found a way to operate incognito such that they cannot be detected, making it challenging to track down those that circumvent the TPMs. Illustratively, the use of VPNs to access copyright-protected content. Users can sign into a VPN, which will hide their internet protocol address and internet activity from anyone, allowing them to access prohibited websites hosting illegal content. Furthermore, this prompts non-compliance because a person can have content taken down as per s77 of the ECTA act. Still, that content may resurface again, turning the scenario into a cat-and-mouse chase because the user knows the ISP cannot detect their online activity and IP address.

Lastly, a compelling argument exists for exploring alternative enforcement mechanisms that leverage advanced technologies such as blockchain and artificial intelligence. Blockchain technology promises an immutable, decentralised ledger that could revolutionise copyright addressing the evidentiary challenges and chain-of-custody issues plaguing traditional enforcement methods. Concurrently, AI can be harnessed to develop real-time monitoring systems capable of automatically detecting and flagging instances of infringement, reducing reliance on manual oversight and mitigating the delays associated with lengthy judicial processes. By integrating these technologies, the enforcement system could become more agile, cost-effective, and transparent, ultimately restoring the balance between

protecting intellectual property rights and facilitating legitimate access to creative works in the digital age.

Chapter 3: An Overview of Blockchain and Artificial Intelligence

3.1. Introduction

Various firms have begun integrating AI and blockchain for better and more accurate service delivery. In 2024, on the 18th of June, McKinsey & Co. announced a new AI platform designed to help enterprises develop, implement, scale, and manage generative AI solutions through a unified software-based approach.[1] Some firms stretch as far as entrusting AI, such as Hire Vue, with recruiting quality candidates through its algorithmic system, which matches keywords on a resume with those from the job description.[2]

Additionally, blockchain's high-level specs have proven helpful as companies like CUSTOS Media Technologies leverage Bitcoin to protect their software programs from copyright infringement.[3] Other firms use blockchain-based cryptocurrencies as payment, excluding intermediaries, while enhancing efficiency and transparency. These two technologies can address copyright law enforcement challenges currently haunting the South African IP system. The increased rate of such difficulties as circumvention, algorithm bias, and non-compliance could be on the brink of heavy reduction by including these two technologies in enforcing copyright.

Consequently, this chapter's primary objective is to provide a concise overview of blockchain and AI before outlining the various methods they can use to enhance copyright enforcement in chapter four.

3.2. Blockchain Technology

Blockchain technology has two types, namely, public and private. They mark the distinction between centralised and decentralised blockchain systems. A centralised blockchain system is a network of individuals whose identities are known and are the only ones allowed to post on the ledger. A decentralised blockchain system is an open network in which anyone can post and see the record of transactions taking place. So, a centralised system is controlled by a group of individuals, making it private, while a decentralised system is public. One of blockchain's best characteristics is the ability to authenticate transactions. This is achieved through two widely used consensus methods (although

---

[1] Duncan Riley 'McKinsey offering aims to bridge the gap from AI prototypes to *production' SiliconAngle* 'available at *https://siliconangle.com/2024/06/18/enhanced-mckinsey-offering-aims-bridge-gap-ai-prototypes-production/* accessed on 22 July 2024.

[2] Drew Harwell 'A Face-Scanning Algorithm Increasingly Decides Whether You Deserve The Job' *Washington Post* available at *https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/* accessed on 14 August.

[3] Tom Jackson 'SA Startup Custos Uses Bitcoin To Disrupt Media Piracy', *Disrupt Africa*, available at *https://disrupt-africa.com/2015/07/08/sa-startup-custos-uses-bitcoin-to-disrupt-digital-piracy/* accessed on 14 August 2022.

there are many more), namely proof of work and proof of stake, where entries into the blockchain are validated and marked as authentic.

Throughout this process, cryptography plays a crucial role by securing all the data against unauthorised access. Blockchain's structure comprises five layers that enable it to function fluidly, making it a comprehensive solution for everything from the backend administration to the front-end application development.[4] Each layer plays a crucial role in ensuring the successful functionality of blockchain. The layers include the application, contract, consensus, network, and data layers. Developers introduced blockchain in three phases, the successor being an upgrade of the predecessor. The first phase is crypto, followed by smart contracts, and the last is decentralised apps (DApps).[5] Without exhuming much, this section will discuss blockchain technology in detail.

3.2.1. Blockchain Layers

In blockchain technology, there must be a hardware layer first for the seamless flow of the network. The hardware layer includes the infrastructure, such as computers, servers, and mining equipment, for validating transactions and adding them to the chain.[6] The data layer stores all the transaction details in the blockchain. Information such as transaction details in the blockchain, the public key recipient and the private key sender form part of the information stored in the data layer.[7] In the data layer, we find the blocks containing the data connected sequentially where the previous block precedes the next block, and there is only one genesis block that connects going forward without a previous block.[8] The network layer follows the data, and it is responsible for all the communication that takes place in a blockchain. It enables transactions and the distribution of data throughout the whole blockchain system.[9]

After the layer responsible for data movement in the blockchain, there is another layer called the consensus layer. The consensus layer guarantees that every node on the network comes to a unanimous agreement concerning the validity of each transaction.[10] It is powered by various consensus methods, of which two are the most prominent ones, namely Proof of Work (PoW) and Proof of Stake (PoW). The application layer is the last, and it is the foundation for creating

[4] Changjing Wang et al 'A Review of Blockchain Layered Architecture and Technology Application Research' (2021) 26 *WUJNS* 415–28.
[5] S Sarmah 'Understanding Blockchain Technology' (2018) 8 *Scientific & Academic Publishing* 23–9.
[6] Wang et al, op cite note 4.
[7] Jared Newell et al 'A Generalised Logical Layered Architecture for Blockchain Technology' 2021.
[8] Ibid.
[9] Wang op cite note 4.
[10] Liu Chunhua 'The Overview of Blockchain Technology Foundation and Application Research' (2020) 2 *The Frontiers of Society, Science and Technology* 13-17.

decentralised applications, allowing users to interact with the blockchain. It embodies various applications, including smart contracts, d'Apps, and other applications designed to function on the blockchain network.[11]

3.2.2. Public blockchain

A public blockchain is a system of multiple nodes[12] joined together to perform transactions amongst each other.[13] Any individual can join the network and view the data or information regarding the transactions. The consensus[14] is implemented by all networks connected to the blockchain.[15] For this reason, a public blockchain is considered transparent by its users because any attempt to tamper with the registry will be easily identified with the record of transactions open to the public. In that regard, it being open to anyone who wants to join is what makes a public blockchain decentralised because no one can claim ownership of it to control it; the responsibility to maintain the blockchain solely rests on every node connected in the system.

The immutability aspect of a blockchain stems from its two consensus methods, proof of work/proof of stake, which are used to verify new entries to the public ledger. The complexity of the algorithms arguably renders it high-level challenging to alter the entries in the ledger because to change one entry, you will have to change all the previous entries, which requires vast amounts of computation power, and it must be verified by all the parties to the network which can be challenging to achieve.[16] As a result, the public blockchain's consensus method makes it highly secure.

In conclusion, a public blockchain is an open network not owned or controlled by a single person, organisation, or entity. Every node plays the same important role and verifies every entry or transaction into the public ledger based on every node's consensus.

3.2.3. Private Blockchain

Unlike public blockchains, private blockchains are centralised. It is a network of credible participants whose identities are known to the person or organisation controlling the system. They are sometimes referred to as permissioned blockchains, and they operate differently from public blockchains, where

---

[11] Newell op cite note 7.
[12] A node is one of the computers that run the blockchain's software to validate and store the complete history of transactions on the network.
[13] Realeboga Maboe *An Overview of Blockchain Technology in The South African Financial Industry* (published LLM thesis, Witswatersrand University, 2018) 34.
[14] A consensus is a system that validates a transaction and marks it as authentic.
[15] Maboe op cite note 13.
[16] Joao Pedro Quintais et al 'Blockchain and The Law: A Critical Evaluation' (2019) 2 *Stanford Journal of Blockchain Law & Policy* 28.

anyone can download the open software, form a node, and then start interacting with the blockchain. In a private blockchain, an intermediary oversees the blockchain and controls the access to the blockchain and the access rights each participant has.[17]

Private blockchain networks are easier to manage and control because they are relatively small. Verifying transactions is faster than the public blockchain because of the limited number of nodes allowed to join the blockchain.[18] The size of the private blockchain networks enables faster network latency. When fewer people log on to the blockchain, the nodes receive information faster, making transactions and verification efficient.[19]

Privacy is a crucial aspect that pushes entities toward a private blockchain instead of a public one. Having control of the blockchain guarantees privacy because entities in control can choose who gains access to the blockchain, every participant is trusted, and their identity is known to the entity in control.

3.2.4. Consensus Mechanisms

3.2.4.1. *Proof of Work*

The Proof of Work consensus mechanism is used in blockchain networks to verify transactions and add new blocks by having miners solve mathematical problems. Initially, this method was designed to fight against denial-of-service attacks and email abuses. However, it gained prominence when it was used to filter and block spam emails and was later employed in Bitcoin by Satoshi Nakamoto.[20] In PoW, two-party nodes play different but crucial roles in successfully streamlining the network. Some nodes are responsible for solving mathematical problems associated with creating new blocks, and they get rewarded in return.[21] Then, some nodes ensure that all transactions are validated and propagated by maintaining a copy of the entire blockchain and comparing the transactions to ensure authenticity, thus helping reach a consensus.[22]

---

[17] Bird & Bird 'Private Blockchain Briefing Note' available at *https://www.twobirds.com/-/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf* accessed on 14 August 2022.
[18] CNBC-TV18 'Private Blockchain And Their Use Cases' Cnbctv18.Com available at *https://www.cnbctv18.com/cryptocurrency/blockchain-private-and-their-use-cases-14166142.html* accessed on 14 August 2022.
[19] Coingeek 'Private Vs. Public Vs. Permissioned Blockchain: A Comparative Guide' Coingeek.com available at *https://coingeek.com/bitcoin101/private-vs-public-vs-permissioned-blockchain-a-comparative-guide/* accessed 14 August 2022.
[20] Ben Laurie & Richard Clayton 'Proof-Of-Work" Proves Not to Work' available *https://www.semanticscholar.org/paper/%5CProof-of-Work%22-Proves-Not-to-Work-Laurie-Clayton/1680d5a7eb20a9e09a56017bf254d7a8969ef692* accessed on 26 July 2023.
[21] Amitai Porat et al 'Blockchain Consensus: An Analysis of Proof-Of-Work and Its Applications' 2017.
[22] Ibid.

In the workflow process of a blockchain network, a user distributes their transaction onto the network. After that, the miners would collect this transaction into a block. Following that, the block resulting from the transaction carries a mathematical problem that must be solved before it can be added to the chain.[23] So, the term proof of work stems from this process because miners use their computers to try and solve this problem. The process requires a lot of computing power, and miners will be competing against each other to solve the mathematical problem. Once one miner solves it, they broadcast the solution to the entire network, and other nodes verify it.[24] If the solution is correct, the miner can add the block to the chain and receive a reward. Crypto assets are the primary users of the proof of work system, Bitcoin, to be specific, although there has been a shift to other consensus mechanisms like Proof of Stake.

The process outlined above is followed seamlessly, and as a reward, miners get crypto assets once they solve the mathematical problem. In the crypto community, PoW partly solved the double spending problem, and it is claimed so because it did not entirely eradicate the problem but reduced the odds of it happening. Bad actors can easily duplicate [25] digital currencies to spend more than they had, inflating the coins and making the currency unstable and worthless. So, proof of work mitigates this problem by encouraging miners to verify the authenticity of every new transaction before they are added to the blockchain ledger, with bitcoin incentives every time a new block is added to the chain.[25]

3.2.4.2.Benefits

High-level security is one characteristic that PoW is known for. By requiring miners to solve complex mathematical problems, a computationally intensive and time-consuming exercise, this consensus method makes it difficult for malicious parties to manipulate the system, resulting in the maintenance of a decentralised network.[26] Another merit found in PoW is the reduced risk of a single entity controlling the network, which enables miners to compete against each other in solving mathematical problems and rewarding them. Resistance to Sybil attacks is another merit attributed to PoW.[27] Sybil attacks occur where a user creates multiple fake identities to gain control over the blockchain network. So, using PoW would require the perpetrator to use a significant amount of computational power to

[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Arthur Gervais et al 'On the Security and Performance of Proof of Work Blockchains' 2016) *ACM Digital Library* 3–16.
[27] Roberto de Isidro & Erik Anderson 'Proof of Work Vs. Proof of Stake Eu Final' Global X October 5, 2022, available a*t https://globalxetfs.eu/content/files/proof-of-work-vs.-proof-of-stake-eu-final.pdf* accessed on 14 August 2022.

control most of the network, which is considered economically impractical.[28]

3.2.4.3.Challenges

PoW is known for consuming high energy. Solving mathematical problems requires very powerful computers to carry out the task, and such computers consume much electricity, overloading the electricity grid and increasing the demand for electricity production.[29] Now, if the source of electricity is renewable resources, carbon emissions will be increased. One bitcoin's carbon footprint is equivalent to driving a gas-powered vehicle for over 800km.[30] Another demerit that PoW has lies in the difficulties in quickly scaling to accommodate many transactions; for example, Bitcoin has a limited transaction throughput, leading to potential delays and higher fees during periods of high demand.[31]

3.2.4.4.*Proof of Stake*

Another consensus algorithm blockchain uses apart from PoW is PoS. It is used to achieve an agreement on the state of the ledger. Unlike PoW, which requires solving complex mathematical problems requiring massive computational power, PoS decides the creator of the next block based on the amount of cryptocurrency a participant holds and is willing to stake as collateral.[32]

To deliberate further, those participating in a PoS system must lock up their cryptocurrency as collateral, known as staking. Since the cryptocurrency that one can stake is sometimes proportional to the existing stake in the whole network, it then means that the more cryptocurrency a participant holds and is willing to lock up, the more their chances of being chosen to create the next block.[33] To prevent a single entity from consistently creating blocks, the PoS uses randomisation based on the amount of stake locked up as collateral.[34] The primary reason for locking up a stake as collateral is to prevent dishonest behaviour from the participants creating the blocks. As a result, should one participant become dishonest, they lose the locked stake. Like PoW, validators are rewarded for creating the blocks with a combination of transaction fees and minted crypto assets.

---

[28] Ibid.
[29] Zibin Zheng et al 'Blockchain Challenges and Opportunities: A Survey' (2018) 14 (4) *Int. J. Web and Grid Services* 352-371.
[30] Bit Wave 'Explained: Proof of Work Vs. Proof of Stake Carbon Footprint' available at *https://www.bitwave.io/blog/explained-proof-of-work-vs-proof-of-stake-carbon-footprint* accessed 12 March 2024.
[31] Finextra 'Blockchain and The Scalability Challenge: Solving the Blockchain Trilemma' available at *https://www.finextra.com/blogposting/24941/blockchain-and-the-scalability-challenge-solving-the-blockchain-trilemma* accessed on 12 March 2024.
[32] Cong T Nguyen et al 'Proof of Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities' (2019) 7 *IEEE Access* 85727–45.
[33] Ibid.
[34] Parma Bains 'Blockchain Consensus Mechanisms: A Primer for Supervisors' (2022) *IMF: Fintech Notes* at 10.

3.2.4.5.Benefits

One of PoS' merits is increased efficiency. While miners in PoW require a significant amount of computational power and energy to solve mathematical problems when selecting validators, PoS does not require that; it selects validators based on the stake they have locked up.[35] As a result, the requirement for intensive computing effort was removed. Additionally, PoS is seen as more secure against 51% attacks than PoW because to take over a network, a miner would have to purchase most of the crypto assets in circulation, which is prohibitively expensive, thus making the network more resilient to manipulation.[36] As a result, the network is more resilient to manipulation and attacks.

3.2.4.6.Challenges

Although the PoS uses a randomised method of selecting validators, it does not eliminate the fact that it is susceptible to wealth concentration.[37] This occurs when a group of participants with substantial holdings control a more significant portion of the network, and it has been argued that this could lead to an oligarchy in which the wealthy continue to amass wealth and possibly centralise power.[38]

PoS systems are vulnerable to long-range attacks. Such attacks occur when a hacker starts a fork from a point in the blockchain's past and tries to hold control over the current chain. Therefore, to reduce the risk, strategies such as checkpoints can be used to mitigate.[39]

3.2.5. Cryptography

Cryptography is referred to as a mathematical method of securing information and communication. This is made possible by converting data using cryptographic keys and algorithms into a format called ciphertext. [40] Cryptography guards against illegal access and tempering while retaining the information and maintaining the information's confidentiality, integrity, and authenticity. [41] It achieves this by making it difficult for hostile actors to decode the original content without the decryption key, paving the way for secure communication in an insecure environment.

To put the functionality of cryptography into a practical example, when one sends a friend a private

---

[35] Nguyen op cite note 32.
[36] Fredy Andres Aponte-Novoa et al 'The 51% Attack on Blockchains: A Mining Behavior Study' (2021) 9 *IEEE Access* 140549–64.
[37] Giulia Fanti et al. 'Compounding of Wealth in Proof-Of-Stake Cryptocurrencies' (2019) *Financial Cryptography and Data Security* 42–61.
[38] Ibid.
[39] Olanrewaju Sanda Et Al 'Long-Range Attack Detection on Permissionless Blockchains Using Deep Learning' (2023) 218 (1) *Expert Systems with Applications* 119606.
[40] Garry C Kessler 'An Overview of Cryptography' available *at https://core.ac.uk/reader/217173980* accessed 20 November 2023.
[41] Ibid.

message using the internet, there is a high chance that the message can be intercepted by anyone using the internet if cryptography is not used. However, if the message is encrypted, it becomes a code only their friend can open to read the contents with the correct key. It signifies sending a locked private letter; only the friend has the key to unlock the message. Moreover, should someone be able to intercept the message, cryptography will ensure that all they see is scrambled letters without the key.

Cryptography has numerous methods of securing communication and shielding data from unwanted access. In symmetric-key cryptography, the parties involved share a single key for encrypting and decrypting the communication.[42] On the contrary, asymmetric key crypto uses two mathematically related keys, a private key for decryption and a public one for encryption, eliminating the requirement for a shared secret and permitting secure communication.[43] Hash functions are essential for data integrity because they produce fixed-size outputs specific to each input. As a result, these cryptographic building blocks provide the basis for safe digital communication, ensuring sensitive data is authentic, confidential, and integrity across various uses.

3.2.6. Crypto Assets

Since the Bitcoin launch in 2009, crypto assets have revolutionised the financial industry. Although they are not a legal tender, they are a financial product as of 2022 in South Africa.[44] Large to small enterprises currently accept them as a form of payment, and because of their features, crypto-assets enhance transaction processes through their P2P mechanism.[45] Illustratively, at Waterzicht Breweries in Cape Town, you can purchase a pint of beer using crypto assets.[46] The Sun Exchange, a solar energy cell vendor, accepts Bitcoin payments.[47] In as much as South Africa is still in its infant stages of fully implementing crypto-assets as payment systems, there is notable progress due to private enterprises using them.

A crypto asset is a digital currency used for payments, and it is electronically stored in the blockchain and uses encryption to verify and monitor transactions. Crypto-assets like Ethereum and Bitcoin use blockchain technology to establish safe and open value exchange networks. [48] In contrast to conventional centralised systems managed by a central authority such as banks, blockchain functions

---

[42] Ibid.
[43] Ibid.
[44] Fasken 'Crypto Assets in South Africa are now legally recognised as Financial Products' available at *https://www.fasken.com/en/knowledge/2022/10/crypto-assets-in-south-africa-are-now-legally-recognised-as-financial-products* access on 14 August 2022.
[45] Staff Writer 'New Laws Coming For Cryptocurrency In South Africa' available at *https://businesstech.co.za/news/banking/605900/new-laws-coming-for-cryptocurrency-in-south-africa/* accessed on 14 August 2022.
[46] Team Luno 'Where to Spend Bitcoin In South Africa' available at *https://discover.luno.com/south-africa-pay-with-bitcoin/* accessed on 15 august 2022.
[47] Ibid.

as a decentralised and impenetrable platform through P2P networking.[48] An immutable chain is created when all the transactions are consolidated into blocks and connected using cryptographic hashes.[49] Consensus techniques like PoW and PoS are used by crypto-assets to verify transactions and protect the network.

These digital currencies make fast and international transactions possible, which lessen the need for intermediaries and promote financial inclusivity. Moreover, smart contracts self-executing code that automates contract terms are another feature that sets blockchain cryptocurrencies apart from other crypto-assets and increases their usefulness beyond straightforward transactions. Notwithstanding the potential for efficiency and innovation, scalability problems and regulatory worries continue to influence how blockchain and crypto-assets develop.

3.2.7. Smart Contracts

Smart contracts on the blockchain are self-executing contracts with the deal's terms directly encoded into the code. They are powered by a distributed, decentralised blockchain network that offers an impenetrable environment to tampering and trustless for carrying out contractual obligations.[50] In contrast to conventional contracts, which depend on intermediaries like banks, legal departments, or other parties to carry out agreements, smart contracts automate the fulfilment of predetermined terms without requiring intermediaries.[51] The outcomes of these contracts are recorded on the blockchain, guaranteeing transparency and immutability, and are carried out when specific predetermined conditions stated in the code are satisfied. Many blockchain platforms, including Ethereum, Binance Smart Chain, and others, support smart contracts, each with a different implementation. They are used in many different industries, such as finance, real estate, supply chain management, and more, where they simplify procedures, cut expenses, and improve the effectiveness and security of contractual relationships. Smart contracts are popular because they revolutionise traditional contract management and promote decentralised applications and ecosystems because of their automated and decentralised nature.

3.2.7.1.Lifecycle of a Smart Contract

In establishing smart contracts, parties first discuss and negotiate the rights, obligations, and limitations of contracts. An agreement can be reached after several rounds of deliberations and talks. Parties will be assisted in drafting a first contractual agreement by attorneys or counsellors. Then,

[48] Ujan Mukhopadhyay et al 'A Brief Survey of Cryptocurrency Systems' (2016) *14th Annual Conference on Privacy, Security and Trust* 745–52.
[49] Ibid.
[50] Ilya Sergey 'A Concurrent Perspective on Smart Contracts' (2017) *International Conference on Financial Cryptography and Data Security* 478-493.
[51] Mukhopadhyay et al, op cite note 48.

software developers transform this agreement written in regular languages into a smart contract using computer languages like declarative and logic-based rule languages. Design, implementation, and validation make up converting a smart contract, much like when creating computer software (i.e., testing).

3.2.7.2.Deployment

After validation, the certified smart contracts can be used on blockchain-based systems. Since blockchains are immutable, contracts placed there cannot be changed.[52] A new contract must be written for each amendment. All parties can access smart contracts using blockchains after they have been installed on those networks. Additionally, by freezing the respective digital wallets, the smart contract locks the digital assets of both parties involved.[53]

3.2.7.3.Execution

Following deployment, contractual provisions will be evaluated. The contractual procedures will be carried out automatically once the requirements are met. It is important to remember that a smart contract comprises several declarative assertions connected logically. The matching statement will automatically be carried out when a condition is met, which results in a transaction being carried out and verified by miners in the blockchains.[54]

3.2.7.4.Completion

Following the execution of a smart contract, the new states of all parties are updated. As a result, blockchains are used to store both the transactions that occur during the execution of smart contracts and the modified states. Throughout this time, the digital assets have been passed from one side to another (e.g., money transfer from the buyer to the supplier). As a result, the relevant parties' digital assets have been unlocked. The smart contract has now finished its whole life cycle.

3.2.8. Decentralised Applications

dApps, also known as blockchain decentralised applications, take advantage of the decentralisation principles inherent in blockchain technology to create a new paradigm for software development. Because dApps run on a decentralised computer network, they are free from censorship and a single point of failure (PoF).[55] dApps decentralise processing and storage across a network of nodes rather than relying on a central server, guaranteeing high security, transparency, and integrity. The decentralised code, called smart contracts, which are stored on the blockchain, is crucial to the

---

[52] Zibin Zheng et al 'An Overview on Smart Contracts: Challenges, Advances and Platforms' (2020) 105 *Future Generation Computer Systems* 475–91.
[53] Ibid.
[54]Ibid.
[55] Kaidong Wu et al 'A First Look at Blockchain-Based Decentralized Applications' (2021) 51 *Software: Practice and Experience* 2033–50.

functioning of decentralised applications.[56] Smart contracts increase user trust by eliminating intermediaries and automatically executing pre-defined terms and conditions; furthermore, the decentralised architecture of dApps minimises the risk of fraud, data breaches and unauthorised access.[57]

Numerous sectors, including healthcare, entertainment, finance, and supply chain management, are looking into integrating decentralised applications. For example, decentralised finance (DeFi) applications enable financial transactions without conventional intermediaries, giving users more control over their assets. Another type of dApps is non-fungible token (NFT) platforms, which allow the production and exchange of one-of-a-kind digital assets, transforming the gaming and art sectors.[58] Although the user interfaces of decentralised applications are like those of traditional applications, their underlying architecture fundamentally changes how data is stored, transactions are carried out, and trust is built.[59] Decentralised apps have the potential to completely change how people engage with digital systems as the ecosystem develops, promoting a more accessible, transparent, and inclusive internet.

3.3.Artificial Intelligence (AI)

Although no definition applies to all instances of AI, it can generally be summed up as the science and engineering of creating intelligent machines and computer programs capable of carrying out tasks that previously required human intelligence.[60] It involves employing computers to replicate or perform human-like behaviour or activities mimicking how human intelligence works.[61] AI possesses traits that allow machines to function without human involvement. Expert systems, natural language processing, speech recognition, and machine vision are some examples of specific AI applications. Learning, reasoning, and self-correction are the three cognitive abilities that AI programming typically emphasises. Having provided the above, artificial intelligence is understood to exist in 3 classes: narrow artificial intelligence, artificial general intelligence, and artificial superintelligence. Following the classes, only narrow artificial intelligence has been explored. It has the following sub-categories: machine learning, deep learning, expert systems, computer vision and natural language

---

[56] Kaidong Wu 'An Empirical Study of Blockchain-Based Decentralized Applications' (2019) *In Proceedings of ACM Conference 17.*

[57] Wei Cai et al 'Decentralized Applications: The Blockchain-Empowered Software System' (2018) 6 *IEEE Access* 53019–33.

[58] Douglas Axen 'What Are NFT dApps? In-Depth Guide to Decentralized Nft Apps', *Moralis Web3 | Enterprise-Grade Web3 Apis*, available at *https://moralis.io/what-are-nft-dapps-in-depth-guide-to-decentralized-nft-apps* accessed on 15 March 2024.

[59] Kaifeng Yue et al 'A Survey of Decentralizing Applications Via Blockchain: The 5g And Beyond Perspective' (2021) 23 *IEEE Communications Surveys & Tutorials* 2191–217.

[60] Stuart Roux 'Legal Regulation of Artificial Intelligence' (2020) 20 (4) Without Prejudice 48-49.

[61] Preeta Bhagattjee et al 'Regulating Artificial Intelligence from A Data Protection Perspective: Lessons from The EU' (2020) 20(11) *Without Prejudice* 9-10.

processing. Subsequently, this section provides an overview of artificial intelligence.

3.3.1. Types of AI

3.3.1.1. Artificial Narrow Intelligence

Among the three types of AI, artificial narrow intelligence (ANI), often called weak AI, is created and trained for specific or limited tasks. ANI lacks the cognitive ability and versatility associated with human intelligence to execute any task that falls outside their scope of functionality; however, they excel at accomplishing a task they are trained to carry out.[62] Google Assistant, Apple's Siri, or Amazon Alexa are examples of ANI, and these are restricted to voice-related tasks and any task outside to which they do not respond.[63] ANI is also used by streaming services such as Netflix and Amazon to examine user behaviour and preferences and make recommendations. As stated, ANI is task-specific, so one will find that it cannot do something other than suggest movie recommendations.[64] Another practical example of ANI is in autonomous vehicles such as Tesla vehicles.[65] They employ ANI designed and trained to control and navigate the vehicle, meaning they lack cognitive abilities to do anything more outside of driving tasks.

3.3.1.2. Artificial General Intelligence

Artificial General Intelligence (AGI) refers to highly autonomous systems designed and trained to outperform humans at most economically significant tasks.[66] AGI aims to have cognitive abilities comparable to human intelligence, and they would not need any programming for every task. Still, they could comprehend, learn and apply knowledge across various tasks.[67] It is argued that these systems still need to be created. As a result, there are no practical examples of them.

3.3.2. Machine Learning

Machine learning (ML) is a field of AI that focuses on building models and algorithms that make computers learn from data to make predictions and judgements. The primary goal of machine learning is to build systems that do not require extensive programming and are capable of learning and

---

[62] Rex Martinez 'Artificial Intelligence: Distinguishing Between Types & Definitions' (2019) 19 *Nevada Law Journal.*
[63] Indiaai 'What Is Narrow Ai?', *Indiaai*, available at https://indiaai.gov.in/article/what-is-narrow-ai accessed on 16 March 2024.
[64] Sunscrapers 'How Artificial Intelligence Is Changing the World?', Sunscrapers, available at https://sunscrapers.com/blog/how-artificial-intelligence-is-changing-the-world-real-world-examples-of-ai-in-action/ accessed on 16 March 2024.
[65] Bernard Marr 'How Tesla Is Using Artificial Intelligence to Create The Autonomous Cars Of The Future', *Bernard Marr*, available at *https://bernardmarr.com/how-tesla-is-using-artificial-intelligence-to-create-the-autonomous-cars-of-the-future/* accessed on 20 May 2024.
[66] Ben Goertzel 'Artificial General Intelligence: Concept, State of The Art, And Future Prospects' (2014) *Journal of Artificial General Intelligence* 1- 48.
[67] Ibid.

improving on their own.[68] Generally, for most systems to carry out tasks, they would have to be programmed by humans to give a desired output. However, machine learning systems do not solely rely on programming but use the data to discover relationships, patterns and insights that enable them to generate new data.[69] Various concepts compose machine learning, and these ensure its success. The first is training data, which contains examples of input-output pairs used to train the machine-learning models. Secondly, there are features and labels where the input data in a supervised learning scenario are linked to corresponding labels or results, giving the models the ability to predict or classify things. Thirdly, algorithms form part of concepts. These mathematical and statistical methods are used to train models depending on the learning task. Fourth, there is the training and testing phase, where a dataset is split into two parts that are a testing set used to assess the model's performance on untested data and a training set that is used to train a model, more so aiding in evaluating how well the model performs outside of the training set of data.

3.3.2.1.Types of Machine Learning

ML algorithms can be divided into multiple categories depending on the type of data and learning tasks involved. The primary categories include supervised, unsupervised, and reinforced learning, which will be discussed below.

3.3.2.2.Supervised Learning

In supervised learning, a model is trained on a labelled dataset that has labelled input values.[70] The model must learn a mapping between the inputs and outputs to make predictions or classifications of new unseen data. An example of supervised learning is email filtering, which classifies incoming emails as spam or legitimate. To achieve this, an AI model is trained on a labelled dataset containing examples of spam and legitimate emails.[71] As a result, the labels enabled it to differentiate such that when put in use, it could separate a spam email from a legitimate one.[72]

3.3.2.3.Unsupervised Learning

In unsupervised learning, models are trained on unlabelled data, allowing the system to search the data for relationships, patterns, or other features without human intervention.[73] One example is clustering, which is the process of grouping similar data pieces into clusters that will have yet to be

---

[68] T Mitchell et al 'Machine Learning' (1990) 4 *Annual Review of Computer Science* 417–33.
[69] Oliver Theobald *Machine Learning for Absolute Beginners: A Plain English Introduction* 2 ed (2017).
[70] Qiong Liu & Ying Wu 'Supervised Learning' (2012*) Encyclopedia of the Sciences of Learning 3243–3245*.
[71] Ibid.
[72]Siddhesh Shinde 'What is Supervised Learning in Machine Learning? A Comprehensive Guide' available at https://emeritus.org/blog/ai-and-ml-supervised-learning/ accessed on 10 January 2024.
[73] Samreen Naeem et al. 'An Unsupervised Machine Learning Algorithms: Comprehensive Review' (2023) 13 *IJCDS Journal* 911–21.

defined prior.[74] So, the machine learning model will find any similar patterns, similarities or differences within the uncategorised data structure by itself. If any natural groups or data structure exists, the model will pick it up.[75]

3.3.2.4.Reinforcement Learning

Reinforcement learning derives its inspiration from how people learn from experiences.[76] In this type of learning, the model, referred to as the agent, learns how to make decisions based on its surroundings; moreover, it receives feedback in the form of awards and penalties, and it learns to maximise cumulative rewards.[77] For example, search engines like Google make use of reinforcement learning.

3.3.3. Deep learning

The use of artificial neural networks to perform tasks by learning from large amounts of data is called deep learning (DL), and it is a subfield of ML. In contrast to traditional machine learning that necessitates programming and feature engineering, DL algorithms use multiple layered neural networks or deep neural networks to learn hierarchical representations of data automatically.[78]

Modelled after the composition and operation of the human brain, artificial neural networks are the building blocks of deep learning. There are layers of interconnected neurons, maybe referred to as nodes, which make up the system, and the system consists of the input layer, where numerical values, text, and image data are sent in their raw form; the hidden layers use weighted connections to process all the data that is fed to the system and the output layers then gives the result.[79] In deep learning, there are various neural networks. However, only three will be briefly expanded on, namely, Convolutional Neural Network (CNN), Recurrent Neural Network (RNN) and Generative Adversarial Neural Network (GAN). Convolutional Neural Networks, frequently used in image recognition tasks [80], are proficient at finding patterns and figures in images, making them employable for facial recognition, object identification and medical image analysis functions.[80] One of their real-life applications is in the medical field for MRI and X-ray image analysis to help with disease

[74] Ibid.
[75] Ibid.
[76] Richard S Sutton & Andrew G Barto *Reinforcement Learning: An Introduction* 2 ed 2014.
[77] Ibid.
[78] Jianqing Fan et al 'A Selective Overview of Deep Learning' (2021) 36 *Statistical Science: A Review Journal of The Institute Of Mathematical Statistics* 264–90.
[79] Ibid.
[80] Ibid.

diagnosis.[81]

RNN is mainly made for sequential data like time series or natural language, And it works efficiently on tasks like sentiment analysis, language translation and speech recognition.[82] Google's language translation uses RNNs to deliver accurate translations between different languages.[83] GAN is another type of neural network that can create new data samples.[84] Using GANs, artificial intelligence can produce new data, such as text, realistic-looking images, or deepfake videos, where faces can be convincingly manipulated to create realistic but fabricated content.[85]

3.3.4. Natural Language Processing (NLP)

Natural language processing is another field of AI that focuses on enabling computers to understand, interpret and generate human language in a meaningful and contextually relevant manner. Its goal is to ensure that computers communicate in a way that mimics natural speech and covers various tasks, such as speech recognition, sentiment analysis, machine translation, language generation, and understanding.[86] Language understanding is NLP's core competency, and it does so through deriving meaning from speech or written language. NLP achieves this by employing a variety of strategies, including part of speech tagging, which picks out the grammatical components of each word tokenisation, which serves to divide the text into individual words or phrases and sentiment analysis, where NLP identifies the emotional tone of a text as positive, negative, or neutral.[87]

A notable example of an NLP use case is Google Translate. It uses NLP algorithms to translate text between languages while maintaining the original meaning.[88] To be able to do so, the system examines the syntax and semantics of sentences, considering idiomatic expressions and linguistics subtleties. NLP is used in virtual assistants such as Google Assistants, Amazon's Alexa, and Apple's Siri.[89] So, using NLP, these systems can comprehend user inquiries, provide natural responses, and respond to spoken language requests.

---

[81] Arkapravo Chattopadhyay & Mausumi Maitra 'MRI-Based Brain Tumour Image Detection Using CNN Based Deep Learning Method' (2022) 2 (4) *Neuroscience Informatics* 100060.
[82] Fan et al op cite note 78.
[83] Françoise Beaufays 'The Neural Networks Behind Google Voice Transcription' available at https://blog.research.google/2015/08/the-neural-networks-behind-google-voice.html accessed on 17 March 2024.
[84] Pegah Salehi et al 'Generative Adversarial Networks (GANS): An Overview of Theoretical Model, Evaluation Metrics, And Recent Developments' 2020 at 3.
[85] Ibid.
[86] Irum Hafeez Sodhar & Abdul Hafeez Buller 'Natural Language Processing: Applications, Techniques and Challenges' (2020) 18 *Advances in Computer Science* 1–25.
[87] Ibid.
[88] Andre Ye 'Breaking Down The Innovative Deep Learning Behind Google Translate' Analytics Vidhya available at *https://medium.com/analytics-vidhya/breaking-down-the-innovative-deep-learning-behind-google-translate-355889e104f1* accessed on 17 March 2024.
[89] Irov Vaul 'How Natural Language Processing Powers Virtual Assistants' Skill Success Blog available at https://blog.skillsuccess.com/how-natural-language-processing-powers-virtual-assistants/ accessed on 17 March 2024.

3.3.5. Computer Vision

Computer vision focuses on enabling machines to interpret and understand visual information from the world, which is a subfield of AI.[90] It functions by having digital photos or videos fed to its algorithms, which then analyse the media data and extract useful information to help with decision-making and action.[91]

A core computer vision component is image recognition, where algorithms are trained to recognise and categorise objects in images. CNNs are frequently used for this purpose because they can imitate the hierarchical structure of the human visual system.[92] One practical example of computer vision's use case is that autonomous vehicles detect objects in real-time, like other cars, pedestrians, and roadblocks, assisting the vehicle with navigating safely.[93] Another essential component of computer vision is image segmentation, which functions by splitting an image into discrete areas or segments according to predetermined criteria using algorithms.[94]

An example of image segmentation in computer vision is found in the medical field, where it can recognise and distinguish organ anomalies, assisting with diagnosis and treatment planning.[95] Computer vision is also used in object tracking, where programs track objects' motion across frames.[96] This is mainly used in surveillance systems that monitor and spot suspicious activity. Lastly, facial recognition is one the most popular components of computer vision and functions by using facial features to identify and authenticate people so they can gain access to a device.

3.4. Conclusion

Conclusively, it is paramount to understand these two technologies before diving into the solutions they can weave in chapter four. Above is a breakdown of AI and blockchain so that there can be surface-level comprehension of how they function. In the chapter, it was mentioned that blockchain technology has layers which help it function successfully. At the top is the hardware layer, which harbours all the physical components that enable the network to run, such as computers. This is

---

[90] IBM 'What is Computer Vision' available at *https://www.ibm.com/topics/computer-vision* accessed on 23 July 2024.
[91] Ibid.
[92] Ibid.
[93] Plainsight Editorial 'Autonomous Vehicles Are Driving Computer Vision into The Future' Plainsight available at https://plainsight.ai/blog/autonomous-vehicles-computer-vision/ accessed on 17 March 2024.
[94] IBM op cite note 90.
[95] Ramakrishna Kolikipogu et al 'Introduction to Computer Vision Aided Data Analytics in Healthcare Industry 4.0' in P. Karthikeyan et al *Healthcare Industry 4.0: Computer Vision-Aided Data Analytics* 1 ed (2023) 1–18.
[96] Fatih Porikli & Alper Yilmaz 'Object Detection and Tracking' (2012) 409 *Studies in Computational Intelligence* 4-41.

followed by the data layer, which stores all the information shared across the network and then the network layer, which enables data exchange through communication and transactions. Following that is the consensus layer, responsible for agreements allowing miners to add blocks to the chain, and then the application layer. This frontend interface enables users to interact with the blockchain.

It is important to note that blockchain technology has two types, namely, private and public. The public blockchain is open to any node that wants to connect and is entirely decentralised, as no one has sole control over it. Still, the private blockchain is controlled by a single entity, which determines how it is run. Blockchain has various consensus methods to validate transactions and add blocks to the blockchain. However, only two were deliberated in this chapter: PoW and PoS. As noted above, PoW functions by requiring miners to solve complex mathematical problems to be able to add a block to a chain. So, miners compete, and the first one to get it right is rewarded in crypto. Although it is applauded for its high-level security specs, this method consumes much energy, which might be a catalyst for carbon footprints.

In contrast to PoW, PoS requires miners to lock up their stake as collateral to be selected to add a block to the chain. This means the more the stake on locks up, the more chances they have of getting chosen to add blocks to the chain. To achieve the high level of security it is applauded for, blockchain uses cryptography to secure its network. Cryptography ensures that no one interferes with the network by converting all the data in transit into ciphertext, which needs a corresponding key. Blockchain has 3 phases, and the first one is the crypto-asset phase, which introduced cryptocurrencies like Bitcoin and P2P payment systems. The second one is smart contracts, which were programmed to self-execute the fulfilment of each condition. The last one is the dApps, which is responsible for all the front-end applications that users interact with whenever they want to use the blockchain network.

After blockchain, this chapter also dives into AI, expanding some of its essential features. AI is a system encompassing various things like software, hardware, computers, algorithms, etc, to execute tasks just like humans. AI has multiple types, but only two are mentioned in this chapter. ANI is known as weak AI, and its functionality is limited to tasks it was trained to execute and nothing else. Then there is the AGI, which is said to be not yet in existence by scholars but is said to be a type of AI that aims to outperform human beings at everyday tasks. Under AI, there are various fields, and in this chapter, a few are focused on, including machine learning, natural language processing, and computer vision. The chapter broke down machine learning, indicating three types of machine learning: supervised, unsupervised, and reinforcement learning.

Moreover, under machine teaching, one would find a subfield called deep learning, which employs

artificial neural networks to execute tasks. Besides machine learning, computer vision and NLP are also used. Computer vision mainly focuses on enabling machines to comprehend visual data, and NLP enables machines to comprehend human languages.

Chapter 4: Blockchain and AI-based Mechanisms to Enforce Copyright

4.1. Introduction

The previous chapter provided an overview of blockchain technology and AI. It presented a rounded discourse of the two technologies, unpacking their nature and functionality, providing an understanding needed to follow the arguments to be unwrapped in this chapter on how blockchain and AI can facilitate copyright enforcement. Notably, these technologies facilitate private enforcement measures. The Copyright Act does not explicitly provide for them, so the rights holder may employ them at their own will and expense.

Literature suggests that AI and blockchain tech, such as machine learning, smart contracts, and deep learning, possess the potential to tie up some of the loose ends within the digital copyright enforcement space, enabling an effective and smooth system of enforcing copyright, tackling issues such as circumvention, algorithm bias, non-compliance and lack of accessibility. This chapter will propose various ways machine learning, deep learning, and blockchain can be used to enforce copyright in the digital space. These suggested mechanisms will be in response to some of the enforcement problems that have been raised in Chapter Two. The chapter will first present the problem and then outline how the technology may mitigate the problem.

4.2. Circumvention

4.2.1. AI Detection System of Brute Force Attacks

First, a breakdown of a brute force attack and how it is used to circumvent access control methods of copyright protection, such as passwords, is tabled. This hacking method targets passwords and encryption keys and attempts to crack them by systematically and exhaustively trying all possible combinations until the correct one is found.[1] Hackers use brute force to circumvent TPMs used to enforce copyright protection. Simple brute force attempts are meant to guess one's credentials. Dictionary attacks are used for password cracking, and they run possible passwords against a username until they get the correct one.[2] Hybrid brute force attacks combine simple brute force and dictionary brute force. It is used to figure out passwords containing a combination of words and other characters.[3]

To counter this attack, a system based on machine learning can be developed first to detect and then

[1] Natalija Vugdelija et al 'Review of Brute Force Attack and Protection Techniques' *ICT Innovations Conference* (2021) 1-10.
[2] Ibid at 3.
[3] Ibid.

stop brute force attacks at the login stage by leveraging their ability to analyse patterns and anomalies. The algorithms will detect anomalies by identifying the deviations from the established patterns and patterns established by training algorithms on extensive data sets that contain information about normal and abnormal login behaviour, including frequency, timing, and the location of login attempts.[4] The model can learn to recognise unusual password-guessing patterns, like trying combinations of common passwords.[5] So, if a user attempts to log in from a different location and there is an unusual number of login attempts in a short period, the algorithms will detect this as suspicious behaviour.

DL would enhance the features of analysing abnormal behaviour since it has neural networks with multiple layers. These layers are effective in detecting sophisticated brute-force attacks. Once the anomaly is picked up, the algorithms will trigger automated responses such as locking the account after many attempts, implementing additional authentication measures like multifactor authentication or notifying the content owner.[6] Moreover, because of ML's ability to learn independently of programming from new data, it will continuously update itself and improve its accuracy in detecting brute force attacks. Vectra AI leverages machine learning to detect and stop bruteforce attacks.[7]

AI will bolster copyright enforcement in the digital space by utilising ML and DL. By developing this system to detect and stop activities like brute force attacks, copyright holders can protect their works from infringement, and it can be integrated into websites where copyright holders store their content.

4.2.1. Blockchain-Based Malware and Phishing Detection

Second, encryption in access control converts plain, readable data into a secure and unreadable format using cryptographic algorithms. This process ensures that the person with the correct key (authorised user) can decrypt the text into readable and understandable information.[8] Data is encrypted using either asymmetric or symmetric, as explained in chapter three under cryptography. Organisations may implement encryption protocols to encrypt data to control access on different infrastructure layers, such as data at rest on storage devices and in transit. As a result, only authorised persons can access

---

[4] Maryam Najafabadi et al 'Machine Learning for Detecting Brute Force Attacks at The Network Level' (2014) *IEEE International Conference on Bioinformatics and Bioengineering* 379–85.
[5] Ibid.
[6] Stephen Wanjau et al.'SSH-Brute Force Attack Detection Model Based on Deep Learning' (2021) 10 *International Journal of Computer Applications Technology And Research* 42–50.
[7] Vectra AI 'How Vectra AI Detects Threats' available at *https://www.vectra.ai/detections* accessed on 2 August 2024.
[8] Temitope Olufohunsi 'Data Encryption' available at *https://www.researchgate.net/publication/337889039_DATA_ENCRYPTION_Olufohunsi_T* accessed on 10 March 2024.

data because they would be carrying a corresponding key. For example, a website that contains research papers usually has paywalls. Access to these research papers requires a decryption key, which can only be obtained when one pays for the subscription.

However, to circumvent encryption, hackers employ various methods. A standard method involves attacking systems and endpoints where the data is decrypted for authentic or legitimate use. This is achieved by deploying malware, like keyloggers or man-in-the-middle attacks, which can capture encryption keys or intercept decrypted data in transit or being processed. Additionally, social engineering methods like phishing are also used by hackers to con users into revealing their credentials, allowing attackers to gain access to encrypted data.

To overcome this problem, the blockchain can detect malware by securely storing signatures or fingerprints of the known malware within the blockchain, and these signatures can be cryptographic hashes generated from the unique features of malware files.[9] This is done because blockchain is well known for its record-keeping abilities. Therefore, this means that when a new file is introduced to the system, its hash will be computed and compared against the stored hashes, and if there are any matches, the system will indicate the presence of malware. Additionally, blockchain can facilitate a decentralised and trustless intelligence signature-sharing system. In this system, parties to it can contribute to a shared blockchain-based repository where malware signatures are shared, making it competent and efficient in terms of detecting malware. Smart contracts could also enhance efficiency with the detection and countermeasures by automating all the security processes. In this regard, a smart contract can be programmed to monitor all network activity and file changes. Once there is any suspicious behaviour, the smart contract will trigger alerts or countermeasures against the malware that would have been detected.

To detect phishing, blockchain's smart contracts come into play to automate the filtering of malicious data. By leveraging the framework of smart contracts, the copyright holder would employ algorithms to identify all the data with phishing content using a homographic URL detector, filter it and then withhold it in the blockchain.[10] PoW is used in this method to choose the block miners, and the block's contents are made visible to all the users once the block is mined, making the users aware of phishing. So once the filtering is complete, the documents that have not been added to the blockchain are deemed to be safe. Chainalysis is an example of a platform that uses blockchain to analyse and track

[9] S Sheela et al 'Decentralized Malware Attacks Detection Using Blockchain' (2023) 53 *ITM Web of Conferences* 03002 1-10.

[10] Dunjie Zhang & Jinyin Chen 'Blockchain Phishing Scam Detection Via Multi-Channel Graph Classification' (2021) 1490 *Blockchain and Trustworthy Systems* 241-256.

cryptocurrency transactions, uncover scams, hacks, fraud, and illicit activities involving digital assets.[11]

As a result, malware and phishing have been used to obtain login details, giving access to copyright-protected work illegally. However, with a blockchain-based malware and phishing detection system, copyright holders can reduce the occurrence of infringements against their works.

4.2.3. Deep Learning Adaptive Watermarking Algorithm

Like other enforcement measures, watermarking is also vulnerable to circumvention and creatives, primarily those who create media content, find themselves in situations where they use the work after removing the embedded watermarks to make it look like it is their work. To remove digital watermarks, one may use a signal processing method to analyse the characteristics of the watermark. These include the frequency or the spatial distribution. After the analysis, they will use algorithms to alter or remove the watermark without degrading the quality of the content. Another approach to circumvent watermarks includes exploiting the software's vulnerabilities that process the watermarked content. One can identify weaknesses in the systems and then disable or manipulate the watermarking mechanism in their favour.

Deep Learning algorithms can bolster digital watermarking through adaptive algorithms. Since traditional watermarking methods employ fixed patterns, which can become predictable and susceptible to attacks over time, DL algorithms can continuously learn and adapt to all emerging circumvention methods.[12] A neural network-based watermarking system can dynamically adjust its embedding and detection methods to respond to ever-evolving threats, posing a challenge to people intending to manipulate or decipher watermarked content.

Additionally, CNN can enhance the perceptual transparency of the watermarks. The goal is to embed the watermark in a way that keeps the quality and aesthetics of the content intact.[13] So deep learning models can learn intricate patterns in the data, allowing more smart and context-aware watermarking methods, ensuring the data remains appealing to the human eye while still withstanding circumvention. Reinforcement learning techniques are applicable to optimise the trade-off between the watermark's invisibility and robustness. This helps the system learn to adjust parameters dynamically based on feedback from its surroundings, adopting a strategy that allows it to find the optimal balance between making the watermark challenging to remove and ensuring less content

[11] Chainalysis 'Know what happens on blockchains' available at *https://www.chainalysis.com/company/* accessed on 16 March 2023.

[12] Manish Rai et al. 'An Optimized Deep Fusion Convolutional Neural Network-Based Digital Color Image Watermarking Scheme for Copyright Protection' (2023) 42 (7) *Circuits, Systems, And Signal Processing* 4019-4050.

[13] Ibid.

distortion.[14]

This system can handle anomaly detection and identify unusual patterns or behaviours that may indicate an attack on the content. With its models trained on diverse data sets, including authentic and manipulated content, the system learns to identify the subtle deviations that may signal tempering, allowing for early detection of potential circumvention attempts. Some companies already use the above technique; companies like StegAI and Google Deep Mind's SythID use deep learning-based watermarks.[15]

Therefore, this system would be much more useful for multimedia content creators. With traditional watermarking prone to circumvention, deep learning reinforces these algorithms to ensure they are formidable and hard to tamper with.

4.2.2. ML VPN Detection and Blocking System.

As discussed in Chapter Two, one of the most significant tools online copyright infringers use is a VPN because of its ability to hide the user's identity. However, machine learning enables copyright owners to detect whether a person engaging with their content is using a VPN and blocks them from further engaging with the copyright owner's content.[16] The system works by identifying the usage of VPNs and analysing the patterns and characteristics of user data traffic against the patterns and characteristics learned from datasets.[17] In the flow process of the system, it analyses the network packets to extract features that can help identify VPN traffic, which may include the packet size, payload content, and headers.

It will further gather information to understand the behaviour of various traffic, capturing the timing, number of packets and direction. Once it has collected the information, it will begin extracting features from the data that may differentiate VPN traffic data from regular traffic data.[18] Once the system detects VPN traffic, it will initiate the blocking function and restrict the network parameters associated with the VPN traffic to ensure the user has no access. Another exciting thing about this system is its ability to adapt and learn to keep up with VPN developments and function effectively. An example of this system includes the one developed by CrowdSec, which has become an effective cybersecurity tool that individuals employ against cyberattacks.[19] Because some people use VPNs

---

[14] Ibid.
[15] Deepmind 'SythID' available at *https://deepmind.google/technologies/synthid/* accessed on 3 August 3, 2024.
[16] Shane Miller et al. 'Detection of Virtual Private Network Traffic Using Machine Learning' (2020) 9 *International Journal of Wireless Networks and Broadband Technologies* 60–80.
[17] Ibid.
[18] Ibid.
[19] Crowdsec 'AI-Powered Proxy and VPN Detection', available at *https://www.crowdsec.net/blog/ai-powered-proxy-and-vpn-detection* accessed on 18 March 2024.

against complying with the laws, copyright owners can employ the system above to ensure the safety of their content.

4.3. Lengthy and Costly Legal Proceedings

4.3.1. Blockchain Arbitration Platform

This dispute resolution platform based on blockchain technology settles disputes between two or more people. It can be called an on-chain arbitration platform, while classical arbitration is an off-chain platform.[20] There are two different approaches to on-chain arbitration, namely expert pools and crowdsourcing; on the one hand, in expert pools, jurors form "expert pools" and offer services anonymously, with parties unaware of the pool members. On the other hand, in crowdsourcing, algorithms randomly select jurors via crowdsourcing.[21] Both approaches ensure anonymity and voluntary evidence collection; unlike classical arbitration, the parties cannot be compelled to provide evidence, and decisions are typically enforced through an escrow mechanism.[22] The role of blockchain in settling disputes aims to streamline arbitration as individuals are guaranteed immediate enforcement of the arbitral award, less costly proceedings and easy access to the settling disputes.[23] The process of initiating a blockchain arbitration kicks off with both parties in a dispute agreeing to conduct the arbitration proceedings on the blockchain or if there was a pre-existing contract between the parties that requested the proceedings be held on the blockchain.[24] Selecting the arbitrators in the system depends on an algorithm that randomly selects the jurors, ensuring anonymity, and also on the platform's approach.

4.3.1.1.Expert Pools

The expert-pooling approach entails semi-anonymous decision-making, with jurors forming specialised pools that gain reputations through evaluations by parties served. This reputation system ensures jurors establish their expertise before being appointed for future disputes.[25] Parties can choose from these pools, impacting juror quality and competence while keeping jurors anonymous. Transparent reputation scores, kept on a blockchain, aid in determining juror professionalism and building trust. Individual jurors, however, cannot be picked to maintain pseudonymity, and

[20] Christoph Salger 'Decentralized Dispute Resolution: Using Blockchain Technology and Smart Contracts in Arbitration' (2024) 24 (1) *Pepperdine Dispute Resolution Law Journal* 65-90.
[21] Ibid at 73.
[22] Ibid at 74.
[23] Ibid at 66.
[24] Luis Bergolla et al 'Kleros: A Socio-Legal Case Study of Decentralized Justice & Blockchain Arbitration' (2022) 37(1) *Ohio State Journal on Dispute Resolution* 4-49.
[25] Ibid at 74.

before signing contracts, parties can designate these notary pools as the controlling authority.[26]

4.3.1.2.Crowdsourcing

Crowdsourcing expands on the expert-pooling approach by delegating tasks to many people (the crowd) who select assignments based on their skills and are compensated for their time, knowledge, or resources.[27] This is known as "crowd arbitration," which uses game-theoretic methods to establish a consensus result. Jurors, or "crowd jurors," stake crypto tokens as security; more significant stakes enhance the possibility of selection and the risk of loss due to wrong votes.[28] Jurors are assigned to cases at random and vote anonymously using the "Schelling Point Principle," which encourages them to agree with the prevailing judgement. Correct votes earn more tokens, whilst erroneous votes result in token losses.

4.3.1.3.Kleros

The most notable on-chain arbitration platform is Kleros. By using crowdsourcing with blockchain and game-theoretic methods, the platform allows jurors to analyse consumer disputes.[29] Anyone, regardless of legal background, can register to serve as a juror, and cases filed to Kleros are assigned to a randomly selected jury using smart contracts. Jurors can self-select for specialised courts, ensuring expertise.[30] According to the Schelling Point Principle, financial prizes are only granted if a juror's vote agrees with that of the majority; furthermore, to prevent collusion, voting is anonymous and confidential, and the results are released after the vote.[31] Blockchain guarantees evidence integrity and fair jury selection, whilst smart contracts automatically enforce rewards and juror remuneration. Kleros provides for appeals, and each one increases the jury size and trial expense.

Kleros presents itself as a "justice-as-a-service" platform that handles various legal issues, such as minor claims, e-commerce, banking, and intellectual property.[32] In 2022, a Mexican court enforced Kleros' blockchain-based award.[33] The platform emphasises efficiency and transparency through collective intelligence, blockchain technology, and integration options for consumer complaints on third-party marketplaces like Amazon. Kleros has resolved 1,644 cases and paid jurors $1,316,000 in

---

[26] Ibid
[27] Ibid at 75.
[28] Ibid.
[29]Ibid at 78.
[30] Bergolla op cite note at 24.
[31] Ibid at 65.
[32] Salgar at 79.
[33] Maxime Chevalier 'Arbitration Tech Toolbox: Is a Mexican Court Decision the First Stone to Bridging the Blockchain Arbitral Order with National Legal Orders?' Kluwer Arbitration Blog available at *https://arbitrationblog.kluwerarbitration.com/2022/03/04/arbitration-tech-toolbox-is-a-mexican-court-decision-the-first-stone-to-bridging-the-blockchain-arbitral-order-with-national-legal-orders/* accessed on 26 July 2024.

prizes. 733 active jurors have staked $5,949,500 in Kleros' cryptocurrency, PNK.[34]

Despite the benefits of blockchain arbitration, it comes with its shortfalls. For example, pseudonymity in blockchain arbitration can jeopardise confidentiality, which is crucial when disputes involve sensitive data, such as trade secrets. Parties often prefer arbitration to keep such matters private. Still, there are concerns about juror confidentiality under pseudonymous models, as jurors may not keep sensitive information secret after case resolution, making it challenging to guarantee confidentiality. Additionally, while traditional judicial proceedings allow jurors to follow the law without jeopardising their finances, focusing entirely on the case's merits, on-chain jurors are motivated by economic self-interest, resulting in choices based on expected votes rather than legal correctness. In the end, the financial incentive for jurors to conform to popular opinions further destabilises the system, making it prone to errors and lack of trust

Blockchain arbitration decision-making challenges are exacerbated by a lack of jurisdictional and legal clarity, which results in inconsistent and localised judgements with no set rules or precedents. Due to the lack of broad criteria, juror decisions are arbitrary and, driven by human biases rather than legal consistency. Jurors may vote for subjective grounds, such as personal dislikes or perceived fairness, with no apparent connection to legal concepts. This condition weakens the consistency and predictability required by legal systems, leaving consumers needing clarification about how to form contracts or predict outcomes. Furthermore, the illusion of uniformity in specialised courts, such as those recommended by Kleros, ignores the differences in legal norms among regions, potentially leading to contradicting verdicts.

4.4. AI Online Infringing Content Detection and blocking System

Machine Learning can play a crucial role in the policing of copyright-infringing content on the internet. A system can be developed to detect and block any content that seems to violate the interested party’s copyright to stop the third party from further infringing again. The system can monitor internet activity by employing a web crawling system, where algorithms are deployed to systematically navigate web pages to collect information and identify potential infringing content.[35] The web crawling system powered by machine learning can recognise patterns associated with infringement, copyright to be specific.[36] By analysing text and media content, the system can learn to distinguish between legitimate and infringing material and to enhance the accuracy and precision of the distinction the algorithms in the system make, supervised learning techniques will have to be

[34] Salgar at 79.
[35] Jilcha & Kwak op cite note 85 CH2.
[36] Ibid.

employed to train models on labelled datasets carrying examples of both infringing and non-infringing content.[37]

For this system to be fully operational at its best, various machine learning models, such as natural language processing (NLP) for textual analysis, have to be involved. NLP can analyse the text to detect any infringing written text associated with the copyright-protected material.[38] It is an adaptive approach that enables the algorithms to evolve along with the new copyright infringing trends and techniques, rendering it efficient, so once the system detects the infringing content, it is blocked or removed.[39] The blocking and removing process is more seamless when the system is paired with ISPs. For example, Mobileum offers an antipiracy service that deploys its ML-based system, which will crawl the internet and search for infringing content distribution sources.[40] Once it does, it will block, disrupt or remove the infringing content, stopping it from further infringing the copyright owner's rights.

4.5. Benefits And Challenges Of Using AI And Blockchain To Enforce Copyright

4.5.1. Benefits

4.5.1.1. Immutability

Blockchain supports immutability, implying that editing or deleting the data recorded in the blockchain is impossible. Traditional record-keeping methods rely on centralised databases or paper-based records, which can be subject to fraud, inaccuracies, and manipulation. In contrast, blockchain technology is a tamper-proof ledger that generates an immutable data record, preventing data from tampering within the network.[41]

4.5.1.2. Transparency

Since blockchain is decentralised, anyone from the public can join the network and verify data, making it transparent. [42] Traditional databases are centralised, and users can only access the information in the database with authorisation from a single entity, usually the administrator. Moreover, the users only have access to the data the administrator chooses. As a result, that cannot

---

[37] Ibid at 2890.
[38] Sindhura Kannappan 'Sentiment Analysis Using Natural Language Processing and Machine Learning' (2023) 38 (2) *Journal of Data Acquisition and Processing* 522-526.
[39] Jilcha & Kwak at 2885.
[40] Carlos Marques 'Content Piracy: What You Don't Know Can Hurt You', available at *https://blog.mobileum.com/content-piracy-what-you-dont-know-can-hurt-you* accessed on 19 March 2024.
[41] Yuanjun Ding et al 'The Digital Copyright Management System Based on Blockchain' *2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology* 63–8.
[42] Annabel Tresise et al. 'What Blockchain Can and Can't Do for Copyright' (2018) 28 *Australian Intellectual Property Journal* 144.

be classified as transparent behaviour. So, one of blockchain's benefits is allowing every member of the blockchain to see what is going on in the network and also allowing them to verify the data entries.

4.5.1.3.Traceability

Blockchain can create an audit trail that documents the movement of information from when it is recorded in the network. Whenever new information has been verified, every block linked to the information is timestamped and recorded in the block. As a result, it is easy to follow up and trace data due to how it is recorded.

4.5.1.4.Increased efficiency

AI can handle enormous amounts of data rapidly and reliably, making it efficient in carrying out tasks. It can examine enormous datasets and identify patterns that might be obscure to people. Accordingly, it can be trained to identify patterns in data, such as particular phrases, file kinds, and metadata, for example, connected to copyright infringement where the system is supposed to detect infringing content. Additionally, it can assist in finding things more quickly and accurately than manual searches by processing enormous volumes of data.[43]

4.5.1.5.Improved accuracy

With a high degree of accuracy, AI can be trained to identify patterns in data, lowering the possibility of false positives and negatives and reducing the requirement for manual inspection.[44] False negatives happen when an algorithm fails to detect content, whereas false positives occur when an algorithm wrongly flags content as being infringing when it is not.[45] In context, copyright enforcement agencies can use machine learning and human knowledge to lessen these mistakes and ensure that no genuine content is mistakenly identified as infringing.

4.5.2. Challenges

4.5.2.1.Regulatory Concerns

Implementing copyright enforcement systems based on AI will require adherence to South African laws relevant to digital technologies, such as the POPI Act, Cybercrimes Act, and Copyright Act.

---

[43] European Union Intellectual Property Office 'Study on The Impact of Artificial Intelligence on The Infringement and Enforcement of Copyright and Designs' available at *https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs_FullR_en.pdf* accessed on 20 January 2024.

[44] Jilcha & Kwak at 2889.

[45] Robert Bold et al. 'Reducing False Negatives in Ransomware Detection: A Critical Evaluation of Machine Learning Algorithms' (2022) 12 *Applied Sciences* 12941; Aakanksha Saha et al 'Secrets in Source Code: Reducing False Positives Using Machine Learning' *2020 International Conference on Communication Systems & Networks (Comsnets)* 168–75.

Concerning AI, the current Copyright Act lacks the statutory exception to access and use various copyright-protected works for AI training purposes, which are crucial for compiling datasets used to train algorithms[50] to carry out tasks such as content detection and filtering flawlessly, including videos, audio, images and text. AI's functionality depends on data (parameters), and the range of its ability depends on the amount of data used to train it.[46] Such poses a challenge for developers because if the relevant material required to compile suitable datasets is copyright protected, they cannot use it without the copyright holder's authorisation, or they will risk getting sued for infringement.[47] Even if they were to try and obtain a license, it would be strenuous and time-consuming to try and retrieve information and contact every individual owning the copyright to the works they want to use.[48] Ultimately, developers end up settling for the works available on open source platforms to compile training datasets or abscond the initiative entirely as they might develop a model that will not meet the demands of the problem presented before them and, more importantly, develop a model that is biased due to insufficient data.

Section 12 of the South African Copyright Act is limited and needs to adequately accommodate the needs of developers who use copyright-protected material for training AI algorithms. The Act allows for specific uses of copyrighted works, such as private study, research, criticism, and reporting current events.[49] This provision does not extend to the diverse and dynamic applications required for developing AI technologies, particularly in ML, where large datasets are essential. For instance, training an AI model might necessitate ingesting thousands of copyright-protected images, texts, or other media forms to enhance the algorithm's ability to recognise patterns and make accurate predictions. However, this process falls outside the permitted uses outlined in the Act, constituting an infringement under current legal frameworks. The CAB is a substantial and welcome start towards resolving the rigidity of s 12 of the South African Copyright Act, explicitly using copyright-protected content for AI training. Despite its potential benefits, the CAB is not yet in effect and awaits the president's signature before becoming law.

Moreover, the technical processes involved in training AI algorithms often require the temporary copying of material, including copyright-protected content.[50] Although these activities are typically for non-commercial purposes and are transient, they still qualify as reproduction under copyright law.

---

[46] Alisson Oliveira & Hugo Tadeu 'Artificial Intelligence: Learning and Limitations' (2020) 17 *WSEAS Transactions on Advances in Engineering Education* 80–6.
[47] Steven Euijong Whang et al *Data Collection and Quality Challenges in Deep Learning: A Data-Centric AI Perspective* (2020) 13 (12) *PVLDB* 3429-3432.
[48] The '*Policy Brief on Clarifying Copyright to Enable AI Research in Africa'* (published 1 May 2024) at 4.
[49] s12 of the Copyright Act.
[50] The '*Policy Brief on Clarifying Copyright to Enable AI Research in Africa*' at 4.

For example, if a developer copies a single copyright-protected image temporarily to train an AI model, this act is seen as reproduction; even though it is not for commercial exploitation and does not commercially affect the original work, the rationale for compensating copyright holders for the use of a single item becomes questionable.[51] This lack of clarity and flexibility in the Act contributes to some challenges faced with integrating AI in enforcing copyright.

4.5.2.2.Privacy concerns

A public, immutable database storing information on a blockchain may give rise to privacy concerns. Since it is a decentralised ledger system, data cannot be readily erased from or deleted from the blockchain; moreover, it is public, meaning anyone who becomes a member of the blockchain has access to it. This means that even if personal data is posted to the blockchain for lawful reasons, it may still be open to unauthorised access or use,[52] and this may result in reputational harm.

Significant privacy problems may result from the employment of AI to find copyright violations through the monitoring and surveillance of user activities. Large volumes of user data, including their online behaviour, interests, and interactions with copyright-protected works, are collected and analysed as part of this type of monitoring. To identify potential instances of copyright infringement, the AI systems used for monitoring and surveillance are often built to evaluate patterns and trends in user data. Data from other sources, including social networking platforms, file-sharing websites, and online marketplaces, may need to be analysed. However, the employment of these AI systems can give rise to worries regarding user privacy.[53]

Users could feel uneasy if they learn that their online behaviour is being tracked and studied without permission, for instance. This can cause people to lose faith in online platforms, making them less likely to utilise them. Additionally, tracking and examining user data may lead to gathering personal information, including a user's location, browsing history, and hobbies, which would be in contravention of s5 of the POPIA.[54] Users may suffer harm from data breaches and exploitation of this information, such as identity theft or cyberbullying.

4.5.2.3.Ethical considerations

Employing AI to enforce copyright raises moral questions about fairness, transparency, and prejudice.

---

[51] Ibid.

[52] Nicolene Schoeman-Louw 'Privacy, Cybercrime and Blockchain' available *at https://www.lexisnexis.co.za/lexis-digest/legal/privacy,-cybercrime-and-blockchain* accessed 13 May 2023.

[53] Andrew Onesimu et al 'Security and Privacy Challenges of Deep Learning: A Comprehensive Survey' in K. Martin Sagayam et al *Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks* (2020) 42–64.

[54] According to s 5, "The data subject has a right to the lawful processing of their personal data. In accordance with sections 18 and 22, they also have the right to notification if their personal information is being collected, or if it has been accessed or obtained by an unauthorized person."

Ensuring these algorithms are trained ethically and responsibly is crucial to avoid bias, as the occurrence of algorithmic bias in AI systems can take various forms. Using skewed training data and inaccurate or unjust results may result in racial and gender biases.[55] For instance, the AI system may mistakenly classify users from other places or races as engaging in copyright infringement if the training data only contains examples of copyright infringement by users from specific locations or of specific races.

Bias may occur in the development of the AI algorithms. It can also produce unfair and erroneous results if the algorithms are created with presumptions or biases. For instance, incorrectly labelling people as infringers may occur if an AI algorithm predicts that users from regions or races are more likely to engage in copyright infringement. Algorithmic prejudice can have serious repercussions, potentially perpetuating discrimination against groups of individuals, resulting in the unfair and erroneous enforcement of copyright rules.[56] For instance, if an AI system favours users from specific regions or races, this may encourage discriminatory attitudes and practices toward others.

4.5.2.4.Costs

While copyright enforcement systems based on blockchain and machine learning have the potential to lower costs compared to traditional enforcement methods, they also require an initial investment in infrastructure and technology, which may present a barrier for some copyright owners. First, creating and implementing blockchain-based and machine-learning algorithms for copyright enforcement is a complex process that takes time and resources. Hiring knowledgeable developers and researchers and buying the required hardware and software can be expensive.[57] These expenses might be too much for small enterprises and independent content producers, limiting their ability to safeguard IP.

Secondly, developing and administrating a sizable amount of data is necessary for blockchain-based copyright enforcement. Multiple parties must be able to access and store this data on a distributed ledger, which necessitates extensive processing and storage resources. This results in expensive infrastructure costs, which can place a heavy load on the copyright owners. Lastly, massive datasets

[55] European Union 'Bias in Algorithms – Artificial Intelligence and Discrimination' *Publications Office of the European Union* (2022) 3-101.
[56] Zuiderveen Borgesius 'Discrimination, Artificial Intelligence, And Algorithmic Decision-Making' (2018) *Directorate General of Democracy* at 22.
[57] Coincoverage 'Openai's Chatgpt Reportedly Costs $100,000 A Day To Run – Ciocoverage Driven For Technology Leaders' available at *https://www.ciocoverage.com/openais-chatgpt-reportedly-costs-100000-a-day-to-run/* accessed on 20 May 2024.

are needed to train machine learning algorithms for copyright enforcement.[58] These can be expensive to acquire, especially when copyrighted works are tracked across numerous platforms and legal systems.

4.6. Conclusion

To conclude this chapter, it is essential to note the extraordinary capabilities that blockchain and AI offer when enforcing copyright in the digital space. Under the deliberation, it was stressed in the chapter that the methods are private enforcement mechanisms that individuals who want to strengthen their protection against the infringement of their works take. Further, the chapter addressed the inadequacies highlighted in chapter two, even though it was not exhaustive. Amongst the solutions, it pointed out how ML, DL and blockchain can solve the circumvention problem that copyright owners face. In short, to respond to brute force attacks, copyright owners may use ML and DL to detect and stop the attack. What enables AI to do this is the ability of algorithms to analyse and learn. As a result, they are trained to analyse normal login behaviour and anomaly login behaviour. Of course, the dataset on which the algorithms will be trained will include other important information, such as time and frequency. Therefore, whenever a dictionary brute force, general brute force, hybrid brute force or any sophisticated type of brute force is attempted, the AI-based system will detect this activity and trigger an automated response of locking the account or any other alternative security measures.

Moving further, to strengthen the encryption of content, blockchain technology offers a malware and phishing detection system that protects individuals from giving up their login details, eventually giving hackers access to their content. All the malware's signatures are taken and stored in the blockchain in this system. Moreover, a decentralised sharing system where updates on new malware signatures are shared to keep the system updated. Therefore, in its functionality, the detection system will compare every data that comes through it with the malware signatures. Once it detects similarities, it will signal the data as malware and further automated action will be taken.

Through adaptive algorithms, AI algorithms can be used to watermark content. Such algorithms, DL, to be specific, are preferred because of their learning nature, allowing them to learn patterns in the data and paving the way for smarter and context-aware watermarking methods. Moreover, paired with machine learning, the system can detect unusual patterns that may indicate an attack on the content.

---

[58] Damir Yalalov 'AI Model Training Costs Are Expected to Rise from $100 Million to $500 Million by 2030', *Metaverse Post*, available *at https://mpost.io/ai-model-training-costs-are-expected-to-rise-from-100-million-to-500-million-by-2030/* accessed on 20 May 2024.

In the chapter, a mechanism against non-compliance was understood to be based on a machine-learning VPN detection and blocking system. Bad actors use VPNs to evade and avoid complying with the legal requirements. As a result, a VPN detection and blocking system will ensure that anyone who wants to access the copyright owner's content is not using a VPN and complying with the legal requirements to access the content. If not, the system will block the person from accessing the content. CrowdSec's system is an example of a system discussed above. It analyses a person's traffic to determine whether they are using a VPN or not, followed by blocking access should it identify the use of one. Apart from the outlined mechanisms, it was also crucial for the chapter to outline the benefits and challenges of using systems based on the two technologies. Enforcing copyright using blockchain and AI is mainly inspired by its benefits. Features like transparency and immutability, enhanced security, and increased efficiency, to mention a few, qualify AI and blockchain for bolstering copyright enforcement in South Africa. However, the two technologies also come with their challenges that copyright owners who intend to employ them should be aware of, such as regulatory compliance, privacy concerns, and ethical considerations, to name a few. Such should be considered because ignorance of the challenges may lead to legal complications.

Chapter 5: Recommendations and Conclusion

5.1. Introduction

In the digital era, where information is exchanged across borders and IP rights face infringement challenges, copyright protection in the digital space has surfaced as an essential matter. Like other countries, South Africa struggles with safeguarding creators' rights in an environment characterised by technological advancements and evolving platforms. By recognising the imperative for innovative solutions to address the struggle, this dissertation explored the integration of AI and blockchain technology as instruments rights holders may use to enforce copyright within the South African context. Integrating AI and blockchain presents an effective avenue for enhancing copyright enforcement mechanisms. AI algorithms can detect instances of copyright infringement efficiently across vast and various digital landscapes and create formidable watermarks. This provides content creators with effective means to monitor and safeguard their copyrights. In the same breath, blockchain technology offers a decentralised, immutable ledger system and smart contracts, which can used to establish a digital arbitration system or a phishing and malware detection system.

As this dissertation delves into the potential applications of AI and blockchain in copyright enforcement, it will conclude by providing actionable recommendations for relevant parties within the South African copyright ecosystem. By examining the challenges, opportunities, and ethical considerations involved in adopting these technologies, this study aims to provide insights that will inform the development of robust, practical strategies for safeguarding copyright in the digital age.

5.2.Recommendations

5.2.1. Regulation of AI and Blockchain

The regulation of AI and blockchain is not merely a bureaucratic exercise; it is a strategic imperative that enables these transformative technologies to enforce copyright effectively in a rapidly evolving digital landscape. By establishing clear legal frameworks, governments can create an environment where AI systems operate safely and predictably, while blockchain's immutable ledger enhances transparency and trust in copyright enforcement. South Africa needs to align such regulatory initiatives with its Vision 2030 for technology integration.[1] A robust and forward-thinking regulatory approach would secure legal recourse, clarify liability in cases of technology malfunction,

[1] South Africa National Development Plan 2030 available at https://www.gov.za/sites/default/files/gcis_document/201409/ndp-2030-our-future-make-it-workr.pdf accessed on 24 February 2024

and spur innovation by providing a stable, predictable market environment.

This section also undertakes a comparative analysis of regulatory approaches across the EU, UK, Malta and UAE. As indicated in chapter one these jurisdictions were chosen because the EU establishes a model for a strict risk-based governance, while the UK encourages AI innovation-friendly regulation that is sectoral, Malta leads in blockchain legislation, and the UAE promotes a business-friendly model, and their frameworks provide vital lessons into South Africa's regulatory development. By drawing lessons from each of the chosen jurisdictions South Africa will facilitate a progressive implementation of the two technologies in copyright enforcement.

5.2.1.1.The EU AI Regulatory Approach

The European Union's approach is anchored in a comprehensive, risk-based framework embodied in the EU AI Act adopted on 21 May 2024.[2] This legislative initiative categorises AI systems according to risk levels, imposing stringent requirements such as transparency, accountability, and human oversight on high-risk applications.[3] The prescriptive nature of the AI Act is designed to ensure that AI systems used in critical areas, meet robust safety and ethical standards. Although this approach may impose significant compliance burdens, it provides a high degree of consumer protection and trust, which is particularly vital when AI systems make decisions with legal ramifications.[4]

5.2.1.2.The UK AI Regulatory Approach

In contrast, the UK has opted for a more flexible, principles-based approach to AI regulation as outlined in the AI (Regulation) Bill introduced to the House of Lords on the 22nd of November 2023.[5] Rather than imposing a prescriptive statutory framework, the UK government emphasises an agile regulatory environment that leverages existing sectoral regulators and encourages self-regulation and innovation within the industry.[6] This approach seeks to reduce bureaucratic hurdles, enabling rapid technological development and adoption allowing different sectors to create measures tailored to the needs and risks they pose.[7] The UK's model, often referenced in its AI Sector Deal context, promotes a balanced regime that safeguards ethical standards while fostering an environment where

---

[2] The AI Act (Regulation (EU) 2024/1689. The full analysis of this instrument is beyond the scope of the dissertation. For analysis, see Marco Almada and Nicolas Petit 'The EU AI Act: Between the Rock of Product Safety and The Hard Place of Fundamental Rights' (2025) 62 *CLMR* 85-120; Sandra Wachter 'Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond' (2024) *Yale Journal of Law and Technology* 26(3) 671–718.
[3] Almada and Petit at 91.
[4] Ibid.
[5] AI (Regulation) Bill [HL].
[6] The *White Paper on A pro-innovation approach to AI regulation: Government response to consultations* (February 2024).
[7] Ibid.

AI can evolve without being stifled by overly rigid rules.[8]

5.2.1.3.Key Differences and Similarities

The EU's risk-based approach ensures that high-impact applications are rigorously controlled, which can build public trust in AI systems used for sensitive tasks such as copyright enforcement.[9] In contrast, the UK's flexible, principles-based approach is designed to adapt quickly to technological changes and reduce compliance overhead, accelerating innovation.[10] While the EU's detailed and prescriptive framework may impose higher compliance costs on developers, it also provides clear guidelines that minimise legal recourse and liability ambiguity. By relying on sector-specific regulation and existing oversight mechanisms, the UK model offers a lighter regulatory touch that can be more attractive to startups and innovators.[11] Both models stress the importance of transparency, but the EU explicitly mandates mechanisms for accountability such as mandatory reporting and risk assessments for high-risk AI systems.[12] At the same time, the UK encourages industry best practices and self-regulatory measures to achieve similar ends.

5.2.1.4.Key Takeaways for South Africa

South Africa recently published its National AI Policy Framework on the 14th of August 2024, which aims to harness the transformative potential of artificial intelligence while addressing critical ethical, legal, and socio-economic challenges.[13] The policy focuses on developing an approach that balances innovation with safeguarding individual rights. It highlights key areas such as bias, privacy protection, and the need for clear definitions and accountability mechanisms in AI-driven processes.[14] In its consultative phase, the policy called for public and private sector collaboration, increased investments in digital skills, and establishing regulatory frameworks that can adapt to the rapid pace of technological change. Recently, Dumisani Sondlo the acting director of Information Society Evaluation and Impact Assessment, Department of Communications and Digital Technologies (DCDT) announced that South Africa's National AI Policy Framework will undergo official evaluation in April 2025.[15]

---

[8] The UK Industrial Strategy Artificial Intelligence Sector Deal available at https://assets.publishing.service.gov.uk/media/5ae0f342e5274a0d85c1c6d5/180425_BEIS_AI_Sector_Deal__4_.pdf accessed on 24 February 2025.
[9] Oghenetejiri Odogun 'Evaluating the Developing Field of AI Governance by Comparing the EU's Precautionary Approach versus the UK's Permissive Approach' (2024) 3.
[10] Ibid at 6.
[11] Ibid at 10.
[12] The AI Act.
[13] South Africa National AI Policy Framework (published 14 August 2024) 10.
[14] Ibid.
[15] Christopher Tredger 'ITWebAI2025: SA's National AI Policy framework under construction but promises much' *ITWeb* available at https://www.itweb.co.za/article/itwebai2025-sas-national-ai-policy-framework-under-construction-but-promises-much/JBwEr7n3oXeM6Db2 accessed on 9 March 2025.

From the above approaches, as suggested by Hlomani, South Africa may adopt a contextual, holistic approach that harnesses the strengths of both risk-based and principles-based approaches while taking into consideration the country's socioeconomic background.[16] In such an approach AI systems deployed where errors can have significant legal and financial consequences, a risk-based regulatory framework like the EU's can ensure that high-risk applications are subject to rigorous standards of transparency and accountability. To avoid stifling technological development, South Africa may integrate principles of flexibility and self-regulation, as seen in the UK approach.[17] This may involve using existing regulatory bodies to oversee AI applications while allowing for iterative improvements and industry-led innovation.[18]

A clear delineation of liability in cases of malfunction or misuse is essential, this would be relevant in copyright infringement cases involving AI as a tool of enforcement by providing clear guidelines on determining liability. So, South Africa's framework should establish definitive guidelines for accountability, drawing from the EU's prescriptive measures while ensuring that these rules do not hinder innovation. South Africa can develop a tailored regulatory framework that is contextual by comparing the EU and UK approaches. This framework should be designed to protect individual rights and encourage the development of advanced copyright enforcement tools that leverage AI.

5.2.1.5.Malta Blockchain Approach

Malta and UAE have emerged as two leading jurisdictions with innovative regulatory approaches to blockchain and crypto assets. In Malta, the cornerstone of its blockchain framework is embodied in the Malta Digital Innovation Authority Act (MDIA Act) that was enacted on the 4th of July 2018. This legislation was designed with dual objectives: to provide legal certainty for blockchain technology and to foster a vibrant digital innovation ecosystem.[19] The MDIA Act establishes the Malta Digital Innovation Authority (MDIA) to certify technology arrangements, including distributed ledger technology (DLT) platforms and smart contracts, and to ensure that innovative digital services meet rigorous consumer protection and market integrity standards.[20] By setting clear guidelines and a certification regime, Malta aims to attract domestic and international blockchain ventures while mitigating risks such as fraud and system failures.

---

[16] Hanani Hlomani 'Why South Africa needs a more holistic and contextual approach to AI regulation' *Daily Maverick* available at https://www.dailymaverick.co.za/article/2023-05-23-why-south-africa-needs-a-more-holistic-and-contextual-approach-to-ai-regulation/ accessed on 8 March 2025.
[17] Huw Roberts, Marta Ziosi and Cailean Osborne et al 'A Comparative Framework for AI regulatory Policy' The International Centre of Expertise on Artificial Intelligence in Montreal (2023) 33.
[18] Valeria Gallo and Suchitra Nair 'The UK's framework for AI regulation' *Deloitte* available at https://www.deloitte.com/uk/en/Industries/financial-services/blogs/the-uks-framework-for-ai-regulation.html accessed on 8 March 2025.
[19] Article 3 of the Malta Digital Innovation Authority Act.
[20] Article 5.

5.2.1.6.UAE Blockchain Approach

In contrast, the UAE has developed a multi-faceted regulatory framework that leverages a combination of national authorities and specialised free zones to create a balanced, innovation-friendly environment. The UAE's approach involves key regulatory bodies such as the Securities and Commodities Authority (SCA), the Virtual Assets Regulatory Authority (VARA), and the financial regulators in free zones like the Dubai International Financial Centre (DFSA) and the Abu Dhabi Global Market (ADGM).[21] This integrated framework aims to provide a unified regulatory environment that not only imposes robust licensing requirements on Virtual Asset Service Providers (VASPs) but also encourages the adoption of blockchain technology across government and private sectors. For instance, the UAE's Emirates Blockchain Strategy 2021 seeks to migrate 50% of government transactions to blockchain platforms, thereby underscoring the nation's commitment to digital transformation.[22]

Malta's MDIA Act and the UAE's regulatory framework share essential commonalities. They emphasise consumer protection and market integrity while fostering innovation yet diverge in their methods. Malta opts for a certification-based model that provides detailed regulatory clarity for blockchain service providers. In contrast, the UAE employs a multi-layered regulatory approach that combines sector-specific licensing with a strong focus on compliance and the facilitation of digital asset innovation across various jurisdictions. This diversity of models illustrates how robust regulation can be tailored to local priorities and technological goals such as developing reliable blockchain based enforcement tools.

5.2.1.7.Key Takeaways for South Africa

For South Africa, the lessons from Malta and the UAE are highly instructive. First, South Africa can benefit from adopting a transparent, certification-driven framework like Malta's MDIA Act to provide legal certainty and establish standardised criteria for technology arrangements. Such an approach would facilitate creating and deploying secure and reliable blockchain solutions that would be used to enforce copyright. Second, the UAE's collaborative and multi-authority framework underscores the importance of integrating rigorous licensing requirements while simultaneously promoting innovation. By engaging multiple stakeholders including regulators, industry experts, and technology developers South Africa can create a flexible regulatory environment that not only mitigates risks but also accelerates the adoption of blockchain technologies in copyright enforcement.

[21] The Emirates Blockchain Policy (published April 2018).
[22] Ibid.

By synthesising the prescriptive clarity of Malta's regulatory model with the dynamic, multi-agency approach of the UAE, South Africa could craft a regulatory framework that would ensure trustworthy and reliable blockchain-based copyright enforcement tools that are also capable of evolving.

5.2.2. Copyright Amendment Bill

The CAB is one of the positive steps taken by the government towards harmonising emerging technologies with copyright laws. The bill passed by the South African parliament is awaiting the president's signature before it goes into operation. It has amendments that effectively respond to the problem outlined in this dissertation. The CAB inserted a definition of technologically protected works, indicating that these are works protected using technological protection measures.[23] It further denotes that a technological protection measure is any method or tool that actively stops or limits copyright infringement and is considered a means of protection.[24] Moreover, a technological protection measure circumvention device or service was defined as a device or service mainly created or modified to help bypass technological measures put in place to protect something, such as digital content or systems.[25]

This provision clarifies that TPMs that protect works need protection but in a constructive way. By including an exception for reasonably bypassing the TPMs, the CAB aims to maintain the promotion of fair use, which is explained in detail below. Currently, no operating provision protects individuals circumventing TPMs for non-copyright infringing purposes. The Cybercrimes Act is strict, and it criminalises any circumvention despite the motive or intention of the act.[26] So, the CAB offers legal protection to individuals who circumvent TPMs protecting works for non-infringing purposes.[27] CAB responds to the inadequacy of accessibility concerns raised in Chapter 2.

It introduces fair use provisions sections 12A-12D, allowing developers to utilise copyright-protected works for non-commercial and technical purposes, including AI training.[28] Section 12C authorises anybody to produce temporary or incidental copies or adaptations of a work, including reformatting, if necessary for a technological procedure. This is permissible for two purposes: (a) allowing the work to be transmitted in a network between third parties via an intermediary or for

[23] s 1 of the Copyright Amendment Bill B13F-2017.
[24] Ibid.
[25] Ibid.
[26] s 7 Cybercrimes Act 19 of 2020.
[27] s 1 of the Copyright Amendment Bill.
[28] s 12.

any other lawful use, and (b) adapting the work for use on different technological devices, such as mobile devices if these acts have no commercial significance.[29]

Since training AI algorithms is a technical procedure that does not have commercial value and wo not affect the commercial exploitation of the original work, it would be protected under s12C. This amendment acknowledges the necessity for more flexible copyright laws in the context of modern technological advancements. By permitting the use of copyright-protected material in ways that do not interfere with the commercial exploitation of the original work, the CAB aims to foster an environment conducive to technological progress and innovation. However, despite its potential benefits, the CAB is not yet in operation and is awaiting the president's signature before becoming law. Until then, the narrow provision of the current Copyright Act remains in force.

5.2.3. Collaborations

Collaboration is paramount to successfully using AI and blockchain mechanisms for copyright enforcement. First and foremost, AI-powered algorithms can analyse vast amounts of digital content to detect copyright infringements efficiently. However, the accuracy and effectiveness of these algorithms heavily rely on access to high-quality data. Collaborative efforts between technology companies, content creators, and legal experts are essential to curating diverse and comprehensive datasets encompassing various types of copyrighted content and infringement patterns. Through collaboration, stakeholders can refine AI models, improving their ability to accurately identify and mitigate copyright violations across different platforms and media formats.

Additionally, blockchain technology offers a decentralised and immutable ledger system that can enhance transparency and traceability in copyright enforcement efforts. By recording copyright ownership information and licensing agreements on a blockchain, creators can establish verifiable proof of ownership and streamline the licensing process. However, realising the full potential of blockchain for copyright enforcement requires collaboration among industry players to develop interoperable standards and protocols. Collaborative initiatives can facilitate the integration of blockchain solutions into existing copyright management systems, enabling seamless interactions between different platforms and stakeholders while ensuring data integrity and security.

Furthermore, collaboration fosters knowledge sharing and capacity building, enabling stakeholders to stay abreast of emerging trends and best practices in AI and blockchain technology. Cross-sector partnerships between academia, industry, and government can facilitate research and development efforts to advance AI and blockchain solutions for copyright enforcement. By pooling resources

[29] s 12C.

and expertise, collaborators can accelerate innovation, address technical challenges, and overcome regulatory hurdles more effectively. Ultimately, collaborative endeavours pave the way for a robust ecosystem where AI and blockchain technologies work synergistically to protect the rights of content creators, foster creativity, and promote a fair and sustainable digital economy.

5.3.Conclusion

In conclusion, this dissertation has shed light on the inconsistencies within the South African copyright system, particularly in enforcing copyrights within the digital space. Through a detailed examination of various forms of copyright infringements and the available enforcement mechanisms, it has become evident that the existing approaches suffer from inadequacies such as lengthy legal proceedings, slow legislative updates, circumvention, accessibility concerns, non-compliance, and algorithmic bias. However, exploring emerging technologies like AI and blockchain offers a glimmer of hope in addressing these inadequacies. By harnessing the capabilities of AI and blockchain, copyright holders have the potential to bolster copyright enforcement significantly. Mechanisms such as AI Detection Systems, blockchain-based detection of malware and phishing, AI watermarking, machine learning-based VPN detection, blockchain arbitration, and AI-driven infringing content detection systems showcase promising avenues for improvement.

Yet, alongside these promising advancements, it is crucial to recognise both the benefits and challenges of their implementation. While transparency, security, increased efficiency, and improved accuracy are clear benefits, challenges such as regulatory compliance, privacy concerns, ethical considerations, and costs must be carefully navigated. Moving forward, copyright holders must engage in responsible and compliant utilisation of these technologies, ensuring alignment with the rules and regulations of South Africa. Moreover, ongoing research, collaboration, and adaptation will be essential in maximising the potential of AI and blockchain to strengthen copyright enforcement in the digital age. Through a concerted effort, South Africa can strive towards a more robust and effective copyright framework that fosters creativity and innovation while safeguarding copyright in the digital space.

Bibliography

Primary Sources

Statutes and Bills

South Africa

The Copyright Act 98 of 1978.

The Protection of Personal Information Act 4 of 2013.

The Electronic Communications and Transactions Act 25 of 2002

Cybercrimes Act 19 of 2020.

Copyright Amendment Bill B13F-2017.

Foreign

The Malta Digital Innovation Authority (MDIA) Act 591 of 2018

The AI Act (Regulation (EU) 2024/1689

Artificial Intelligence (Regulation) Bill [HL].

Cases

South Africa

CCP Record Co (Pty) Ltd v Avalon Record Centre 1989 (1) SA 445 (C)

Moneyweb (Pty) Ltd v Media 24 Ltd and Another 2016 (4) SA 591 (GJ).

Feldman No V Emi Music SA (Pty) *Ltd* [2009] 4 All SA 307 (SCA)

Galago Publishers (Pty) Ltd and Another V Erasmus [1989] 1 All SA 431 (A).

Blind SA v Ministry of Trade, Industry and Competition and Others (14996/21) [2021] ZAGPPHC 871; 2021 BIP 14 (GP)

Southern African Music Rights Organisation Ltd v Svenmill Fabrics (Pty) Ltd 1983 (1) SA 608 (C)

Foreign

A&M Records, Inc. v. Napster, Inc.,239 F.3d 1004 (9th Cir. 2001)

Secondary Sources

Books and Chapters

Dean, OH & Alison Dyer *Dean & Dyer: Introduction to Intellectual Property Law* 1 ed (2014) available *at https://search-ebscohost-com.ezproxy.uct.ac.za/login.aspx?direct=true&db=nlebk&AN=2175219&site=ehost-live* accessed on 20 July 2024.

Van Der Merwe *Information and Communications Technology Law* 2nd ed (2016) available *at https://search-ebscohost-com.ezproxy.uct.ac.za/login.aspx?direct=true&db=nlebk&AN=2139885&site=ehost-live* accessed on 20 July 2024.

Klopper *Law of Intellectual Property In South Africa* 2 ed (2016) available at *https://search-ebscohost-com.ezproxy.uct.ac.za/login.aspx?direct=true&db=nlebk&AN=2139897&site=ehost-live* accessed on 20 July 2024.

Theobald, Oliver *Machine Learning for Absolute Beginners: A Plain English Introduction* 2 ed (2017).

Sutton, Richard S & Andrew G Barto *Reinforcement Learning: An Introduction* 2 ed 2014.

Kolikipogu, Ramakrishna et al 'Introduction to Computer Vision Aided Data Analytics in Healthcare Industry 4.0' in P. Karthikeyan et al *Healthcare Industry 4.0: Computer Vision-Aided Data Analytics* 1 ed (2023) 1–18.

Journal Articles

Yampolskiy, Roman V 'AI Risk Skepticism' 2021

Adepoju, David; Bosun Tijani & Steven Karera 'Artificial Intelligence Skepticism in Career Domains' (2024) 15 *International Journal for Digital Society* 1880–8.

Anderson, Kent 'Can Blockchain Withstand Skepticism? An Inquiry' (2018) 38 *Information Services & Use* 1–6.

Gupta, Aishwarya 'Introduction to AI Chatbots' (2020) 9 (7) *International Journal of Engineering Research* 255-258.

Ene, Charlotte 'Smart Contracts - The New Form of The Legal Agreements' (2020) 14 *Proceedings of The International Conference on Business Excellence* 1206–10.

Gulyaeva, Natalia & Hogan Lovells 'Intellectual Property Law in The Digital Society: Challenges and Opportunities' available at

https://www.expertguides.com/articles/intellectual-property-law-in-the-digital-society-challenges-and-opportunities/arcpwtmm accessed on 26 March.

Blackburn 'Impacts of Digital Piracy on the U.S. Economy' (2019) *US Chamber of Commerce* 1-16.

Pam, Adamu Audu & John Ishaku Mantu 'Copyrights Infringement and Its Impacts on Developing Economies' 2018.

Snelling, Alexander P *Digital Piracy: How the media industry is being transformed* (Universidad Politecnica De Valencia, 2013).

Beiter, Klaus D 'Copyright Reform in South Africa: Two Joint Academic Opinions on the Copyright Amendment Bill [B13B-2017]' (2022) 25 *PELJ*.

Visser, Coenraad 'Technological Protection Measures: South Africa Goes Overboard. Overbroad' (2006) 7 *SAJIC* 54-63.

Mandal, Surajit 'Blockchain Technology and Its Effect on Environment: A Comparative Study Between Proof-Of-Work and Proof-of- Stake' (2023) 7 *International Journal of Rural Development, Environment and Health Research* 1–6.

Jensen, M 'The Protection of Copyright Works on The Internet - An Overview' (2005) 38 *CILSA* at 344.

Ibosiola, Damilola 'Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers' (2018) 12(1) *International AAAI Conference on Web and Social Media.*

Goel, Sanjai 'The Impact of Illegal Peer-to-Peer File Sharing on the Media Industry' (2010) 56 *Carlifornia Management Review* 6-33.

Ncube, Caroline B 'Copyright Enforcement: The Graduated Response Takes Centre Stage' (2012) 24 (2) *South African Mercantile Law Journal* 133-147.

Forere, Malebakeng A 'Keeping Up with The Developments in Technology: A Look into The Music Industry and The Copyright Laws in Southern Africa' (2019) 31 *IPLJ* 31-52.

Seng, Daniel 'Detecting and Prosecuting IP Infringement with AI can the AI Genie Repulse the Forty Counterfeit Thieves of Alibaba?' 2019 *Artificial Intelligence and Intellectual Property* 292–320.

Liang, Mengna 'Copyright issues related to reproduction rights arising from streaming' (2020) 23(5-6) *Journal of World Intellect Property* 798-814.

Bond, Nicole M 'Linking and Framing on The Internet: Liability Under Trademark and Copyright Law Note' (1998) 11 *Depaul Business Law Journal* 185–228.

Winsherly, Tan 'TV Broadcast Piracy Through Illegal Live Streaming Applications:

Challenges and Legal Protection for Copyright Holders' 9 *Al-Adalah: Jurnal Hukum dan Politik Islam* 66-79.

Schonwetter, Tobias & Caroline Ncube 'New Hope for Africa? Copyright And Access to Knowledge in The Digital Age' (2011) 13 *Info* 64–74.

Iwahashi, Ryan 'How to Circumvent Technological Protection Measures Without Violating the DMCA: An Examination of Technological Protection Measures Under Current Legal Standards' (2011) 26 B*erkeley Technology Law Journal*.

Lillã, Maria 'Virtues and Perils of Algorithmic Enforcement and Content Regulation in The Eu - A Toolkit for A Balanced Algorithmic Copyright Enforcement' (2019) 11(1) *Journal of Law, Technology & The Internet*.

Gray, Joanne & Nicolas Suzor 'Playing with machines: Using machine learning to understand automated copyright enforcement at scale' (2020) 7 (1) *Big Data & Society* 1-13.

Klaaren, Jonathan 'What Does Justice Cost In South Africa? A Research Method Towards Affordable Legal Services' (2019) 35 *South African Journal on Human Rights* 1–14.

Jilcha, Lelisa Adeba & Jin Kwak 'Machine Learning-Based Advertisement Banner Identification Technique for Effective Piracy Website Detection Process' (2022) 71 *Computers, Materials & Continua* 2883–99.

Ho, Cheng-Yuan 'Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems' (2012) 50 *IEEE Communications Magazine - IEEE Commun.* Mag. 146–54.

Wang, Changjing 'A Review of Blockchain Layered Architecture and Technology Application Research' (2021) 26 *WUJNS* 415–28.

Sarmah, S 'Understanding Blockchain Technology' (2018) 8 *Scientific & Academic Publishing* 23–9.

Newell, Jared 'A Generalised Logical Layered Architecture for Blockchain Technology' 2021.

Chunhua, Liu 'The Overview of Blockchain Technology Foundation and Application Research' (2020) 2 *The Frontiers of Society, Science and Technology* 13-17.

Maboe, Realeboga An Overview of Blockchain Technology in The South African Financial Industry (published LLM thesis, Witswatersrand University, 2018) 34.

Quintais, Joao Pedro 'Blockchain and The Law: A Critical Evaluation' (2019) 2 *Stanford Journal of Blockchain Law & Policy* 28.

Laurie, Ben & Richard Clayton 'Proof-Of-Work" Proves Not to Work' available *https://www.semanticscholar.org/paper/%5CProof-of-Work%22-Proves-Not-to-*

Work-Laurie-Clayton/1680d5a7eb20a9e09a56017bf254d7a8969ef692 accessed on 26 July 2023.

Porat, Amitai 'Blockchain Consensus: An Analysis of Proof-Of-Work and Its Applications' 2017.

Gervais, Arthur 'On the Security and Performance of Proof of Work Blockchains' (2016) *ACM Digital Library* 3–16.

Zheng, Zibin 'Blockchain Challenges and Opportunities: A Survey' (2018) 14 (4) *Int. J. Web and Grid Services* 352-371.

Nguyen, Cong T 'Proof of Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities' (2019) 7 *IEEE Access* 85727–45.

Bains, Parma 'Blockchain Consensus Mechanisms: A Primer for Supervisors' (2022) *IMF: Fintech Notes*.

Aponte-Novoa, Fredy Andres 'The 51% Attack on Blockchains: A Mining Behavior Study' (2021) 9 *IEEE Access* 140549–64.

Fanti, Giulia 'Compounding of Wealth in Proof-Of-Stake Cryptocurrencies' (2019) *Financial Cryptography and Data Security* 42–61.

Sanda, Olanrewaju 'Long-Range Attack Detection on Permissionless Blockchains Using Deep Learning' (2023) 218 (1) *Expert Systems with Applications* 119606.

Mukhopadhyay, Ujan 'A Brief Survey of Cryptocurrency Systems' (2016) 14th *Annual Conference on Privacy, Security and Trust* 745–52.

Sergey, Ilya 'A Concurrent Perspective on Smart Contracts' (2017) *International Conference on Financial Cryptography and Data Security* 478-493.

Zheng, Zibin 'An Overview on Smart Contracts: Challenges, Advances and Platforms' (2020) 105 *Future Generation Computer Systems* 475–91.

Wu, Kaidong 'A First Look at Blockchain-Based Decentralized Applications' (2021) 51 *Software: Practice and Experience* 2033–50.

Wu, Kaidong 'An Empirical Study of Blockchain-Based Decentralized Applications' (2019) *In Proceedings of ACM Conference 17*.

Cai, Wei 'Decentralized Applications: The Blockchain-Empowered Software System' (2018) 6 *IEEE Access* 53019–33.

Yue, Kaifeng 'A Survey of Decentralizing Applications Via Blockchain: The 5G And Beyond Perspective' (2021) 23 *IEEE Communications Surveys & Tutorials* 2191–217.

Bhagattjee, Preeta 'Regulating Artificial Intelligence from A Data Protection

Perspective: Lessons from the EU' (2020) 20(11) *Without Prejudice* 9-10.

Martinez, Rex 'Artificial Intelligence: Distinguishing Between Types & Definitions' (2019) 19 *Nevada Law Journal.*

Goertzel, Ben 'Artificial General Intelligence: Concept, State of The Art, And Future Prospects' (2014) *Journal of Artificial General Intelligence*.

Mitchell, T 'Machine Learning' (1990) 4 *Annual Review of Computer Science* 417–33.

Liu, Qiong & Ying Wu 'Supervised Learning' (2012) Encyclopedia of the Sciences of *Learning*.

Naeem, Samreen 'An Unsupervised Machine Learning Algorithms: Comprehensive Review' (2023) *13 IJCDS Journal* 911–21.

Fan, Jianqing 'A Selective Overview of Deep Learning' (2021) 36 *Statistical Science: A Review Journal of The Institute of Mathematical Statistics* 264–90.

Chattopadhyay, Arkapravo & Mausumi Maitra 'MRI-Based Brain Tumour Image Detection Using CNN Based Deep Learning Method' (2022) 2 (4) *Neuroscience Informatics* 100060.

Salehi, Pegah 'Generative Adversarial Networks (GANS): An Overview of Theoretical Model, Evaluation Metrics, And Recent Developments' 2020.

Sodhar, Irum H & Abdul Hafeez Buller 'Natural Language Processing: Applications, Techniques and Challenges' (2020) 18 *Advances in Computer Science* 1–25.

Porikli, Fatih & Alper Yilmaz 'Object Detection and Tracking' (2012) 409 *Studies in Computational Intelligence* 4-41.

Vugdelija, Natalija 'Review of Brute Force Attack and Protection Techniques' *ICT Innovations Conference* (2021).

Najafabadi, Maryam 'Machine Learning for Detecting Brute Force Attacks at The Network Level' (2014) *IEEE International Conference on Bioinformatics and Bioengineering* 379–85.

Wanjau, Stephen 'SSH-Brute Force Attack Detection Model Based on Deep Learning' (2021) 10 *International Journal of Computer Applications Technology and Research* 42–50.

Olufohunsi, Temitope 'Data Encryption' available at *https://www.researchgate.net/publication/337889039_DATA_ENCRYPTION_Olufohunsi_T* accessed on 10 March 2024.

Sheela, S 'Decentralized Malware Attacks Detection Using Blockchain' (2023) 53 *ITM Web of Conferences* 03002.

Zhang, Dunjie & Jinyin Chen 'Blockchain Phishing Scam Detection Via

Multi-Channel Graph Classification' (2021) 1490 *Blockchain and Trustworthy Systems* 241-256.

Rai, Manish 'An Optimized Deep Fusion Convolutional Neural Network-Based Digital Color Image Watermarking Scheme for Copyright Protection' (2023) 42 (7) *Circuits, Systems, And Signal Processing* 4019-4050.

Miller, Shane 'Detection of Virtual Private Network Traffic Using Machine Learning' (2020) 9 *International Journal of Wireless Networks and Broadband Technologies* 60–80.

Salger, Christoph 'Decentralized Dispute Resolution: Using Blockchain Technology and Smart Contracts in Arbitration' (2024) 24 (1) *Pepperdine Dispute Resolution Law Journal* 65-90.

Bergolla, Luis 'Kleros: A Socio-Legal Case Study of Decentralized Justice & Blockchain Arbitration' (2022) 37(1) *Ohio State Journal on Dispute Resolution* 4-49.

Kannappan, Sindhura 'Sentiment Analysis Using Natural Language Processing and Machine Learning' (2023) 38 (2) *Journal of Data Acquisition and Processing* at 522.

Ding, Yuanjun 'The Digital Copyright Management System Based on Blockchain' 2019 *IEEE 2nd International Conference on Computer and Communication Engineering Technology* 63–8.

Tresise, Annabel et al. 'What Blockchain Can and Can't Do for Copyright' (2018) 28 *Australian Intellectual Property Journal* 144.

Bold, Robert 'Reducing False Negatives in Ransomware Detection: A Critical Evaluation of Machine Learning Algorithms' (2022) 12 *Applied Sciences* 12941.

Saha, Aakanksha 'Secrets in Source Code: Reducing False Positives Using Machine Learning' 2020 *International Conference on Communication Systems & Networks (Comsnets)* 168–75.

Oliveira, Alisson & Hugo Tadeu 'Artificial Intelligence: Learning and Limitations' (2020) 17 WSEAS *Transactions on Advances in Engineering Education* 80–6.

Whang, Steven E 'Data Collection and Quality Challenges in Deep Learning: A Data-Centric AI Perspective '(2020) 13 (12) *PVLDB* 3429-3432.

Onesimu, Andrew 'Security and Privacy Challenges of Deep Learning: A Comprehensive Survey' (2020) Deep *Learning Strategies for Security Enhancement*

in Wireless Sensor Networks 42–64.

European Union 'Bias in Algorithms – Artificial Intelligence and Discrimination' Publications Office of the European Union (2022) 3-101.

Borgesius, Zuiderveen 'Discrimination, Artificial Intelligence, And Algorithmic Decision-Making' (2018) *Directorate General of Democracy*s.

Oghenetejiri Odogun 'Evaluating the Developing Field of AI Governance by Comparing the EU's Precautionary Approach versus the UK's Permissive Approach' (2024) 3.

Marco Almada and Nicolas Petit 'The EU AI Act: Between the Rock of Product Safety and The Hard Place of Fundamental Rights' (2025) 62 CLMR 85-120;

Sandra Wachter 'Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond' (2024) Yale Journal of Law and Technology 26(3) 671–718.

Huw Roberts, Marta Ziosi and Cailean Osborne et al 'A Comparative Framework for AI regulatory Policy' The International Centre of Expertise on Artificial Intelligence in Montreal (2023) 33.

Internet Sources

Kessler, Garry C 'An Overview of Cryptography' available at *https://core.ac.uk/reader/217173980* accessed 20 November 2023.

Fasken 'Crypto Assets in South Africa are now legally recognised as Financial Products' available at *https://www.fasken.com/en/knowledge/2022/10/crypto-assets-in-south-africa-are-now-legally-recognised-as-financial-products* access on 14 August 2022.

Indiaai 'What Is Narrow Ai?', Indiaai, available *at https://indiaai.gov.in/article/what-is-narrow-ai accessed* on 16 March 2024.

Shinde, Siddhesh 'What is Supervised Learning in Machine Learning? A Comprehensive Guide' available at *https://emeritus.org/blog/ai-and-ml-supervised-learning/* accessed on 10 January 2024.

The 'National Blockchain Policy for Nigeria' (published 3 May 2023).

Report on The South African Open Copyright Review' at 1 available at *https://ip-unit.org/wp-content/uploads/2010/07/opencopyrightreport1.pdf* accessed on 20 July 2024.

The Verge 'Google's invisible AI watermark will help identify generative text and video' available at *https://www.theverge.com/2024/5/14/24155927/google-ai-*

synthid-watermark-text-video-io accessed on May 19 2024.

Custos 'Custos Use Case: Document Protection', Custos Media Technologies available at *https://www.custostech.com/blogchain/custos-use-case-document-protection/* accessed on 12 September 2022.

Vermeulen, Jan 'How SA's first online pirate was caught' available at *https://mybroadband.co.za/news/internet/103875-how-sas-first-online-pirate-was-caught.html* accessed on 13 September 2022.

Nicholson, Denise R 'The Copyright Amendment Bill: Its Genesis and Passage Through Parliament' InfoJustice.org available at *https://infojustice.org/archives/41167* accessed 14 September 2022.

Kasperskey 'Brute Force Attack: Definition and Examples', Kaspersky.Com available at *https://www.kaspersky.com/resource-center/definitions/brute-force-attack* accessed 10 July 2022.

VPN.com 'Can My Internet Provider See My VPN?' available at *https://www.vpn.com/faq/isp/* accessed 10 July 2022.

Riley, Duncan 'McKinsey offering aims to bridge the gap from AI prototypes to production' SiliconAngle 'available at *https://siliconangle.com/2024/06/18/enhanced-mckinsey-offering-aims-bridge-gap-ai-prototypes-production/* accessed on 22 July 2024.

Harwell, Drew 'A Face-Scanning Algorithm Increasingly Decides Whether You Deserve The Job' Washington Post available at *https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/* accessed on 14 August.

Jackson, Tom 'SA Startup Custos Uses Bitcoin to Disrupt Media Piracy', Disrupt Africa, available at *https://disrupt-africa.com/2015/07/08/sa-startup-custos-uses-bitcoin-to-disrupt-digital-piracy/* accessed on 14 August 2022.

Bird & Bird 'Private Blockchain Briefing Note' available at *https://www.twobirds.com/-/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf* accessed on 14 August 2022.

CNBC-TV18 'Private Blockchain and Their Use Cases' Cnbctv18.Com available at *https://www.cnbctv18.com/cryptocurrency/blockchain-private-and-their-use-cases-14166142.html* accessed on 14 August 2022.

Coingeek 'Private Vs. Public Vs. Permissioned Blockchain: A Comparative Guide' Coingeek.com available at *https://coingeek.com/bitcoin101/private-vs-public-vs-*

permissioned-blockchain-a-comparative-guide/ accessed 14 August 2022.

de Isidro, Roberto & Erik Anderson 'Proof of Work Vs. Proof of Stake Eu Final' Global X October 5, 2022, available *at https://globalxetfs.eu/content/files/proof-of-work-vs.-proof-of-stake-eu-final.pdf* accessed on 14 August 2022.

Bit Wave 'Explained: Proof of Work Vs. Proof of Stake Carbon Footprint' available at *https://www.bitwave.io/blog/explained-proof-of-work-vs-proof-of-stake-carbon-footprint* accessed 12 March 2024.

Finextra 'Blockchain and The Scalability Challenge: Solving the Blockchain Trilemma' available at *https://www.finextra.com/blogposting/24941/blockchain-and-the-scalability-challenge-solving-the-blockchain-trilemma* accessed on 12 March 2024.

Staff Writer 'New Laws Coming for Cryptocurrency In South Africa' available at *https://businesstech.co.za/news/banking/605900/new-laws-coming-for-cryptocurrency-in-south-africa/* accessed on 14 August 2022.

Team Luno 'Where to Spend Bitcoin In South Africa' available at *https://discover.luno.com/south-africa-pay-with-bitcoin/* accessed on 15 august 2022.

Axen, Douglas 'What Are NFT dApps? In-Depth Guide to Decentralized NFT Apps', Moralis Web3 | Enterprise-Grade Web3 Apis, available *at https://moralis.io/what-are-nft-dapps-in-depth-guide-to-decentralized-nft-apps* accessed on 15 March 2024.

Sunscrapers 'How Artificial Intelligence Is Changing the World?', Sunscrapers, available at *https://sunscrapers.com/blog/how-artificial-intelligence-is-changing-the-world-real-world-examples-of-ai-in-action/* accessed on 16 March 2024.

Marr, Bernard 'How Tesla Is Using Artificial Intelligence to Create the Autonomous Cars Of the Future', Bernard Marr, available at *https://bernardmarr.com/how-tesla-is-using-artificial-intelligence-to-create-the-autonomous-cars-of-the-future/* accessed on 20 May 2024.

Beaufays, Françoise 'The Neural Networks Behind Google Voice Transcription' available at *https://blog.research.google/2015/08/the-neural-networks-behind-google-voice.html* accessed on 17 March 2024.

Ye, Andre 'Breaking Down the Innovative Deep Learning Behind Google Translate' Analytics Vidhya available at *https://medium.com/analytics-vidhya/breaking-down-the-innovative-deep-learning-behind-google-translate-355889e104f1*

accessed on 17 March 2024.

Vaul, Irov 'How Natural Language Processing Powers Virtual Assistants' Skill Success Blog available at *https://blog.skillsuccess.com/how-natural-language-processing-powers-virtual-assistants/* accessed on 17 March 2024.

IBM 'What is Computer Vision' available at https://www.ibm.com/topics/computer-vision accessed on 23 July 2024.

Plainsight Editorial 'Autonomous Vehicles Are Driving Computer Vision into The Future' Plainsight available at https://plainsight.ai/blog/autonomous-vehicles-computer-vision/ accessed on 17 March 2024.

Crowdsec 'AI-Powered Proxy and VPN Detection', available at *https://www.crowdsec.net/blog/ai-powered-proxy-and-vpn-detection* accessed on 18 March 2024.

Chevalier, Maxime 'Arbitration Tech Toolbox: Is a Mexican Court Decision the First Stone to Bridging the Blockchain Arbitral Order with National Legal Orders?' Kluwer Arbitration Blog available at *https://arbitrationblog.kluwerarbitration.com/2022/03/04/arbitration-tech-toolbox-is-a-mexican-court-decision-the-first-stone-to-bridging-the-blockchain-arbitral-order-with-national-legal-orders/* accessed on 26 July 2024.

European Union Intellectual Property Office 'Study on The Impact of Artificial Intelligence on The Infringement and Enforcement of Copyright and Designs' available at *https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs_FullR_en.pdf* accessed on 20 January 2024.

Nicolene Schoeman-Louw 'Privacy, Cybercrime and Blockchain' available at *https://www.lexisnexis.co.za/lexis-digest/legal/privacy,-cybercrime-and-blockchain* accessed 13 May 2023.

Coincoverage 'Openai's Chatgpt Reportedly Costs $100,000 A Day to Run – Ciocoverage Driven for Technology Leaders' available at *https://www.ciocoverage.com/openais-chatgpt-reportedly-costs-100000-a-day-to-run/* accessed on 20 May 2024.

Yalalov, Damir 'AI Model Training Costs Are Expected to Rise from $100 Million to $500 Million by 2030', Metaverse Post, available at *https://mpost.io/ai-*

model-training-costs-are-expected-to-rise-from-100-million-to-500-million-by-2030/ accessed on 20 May 2024.

South African Government 'President Cyril Ramaphosa appoints Commission on Fourth Industrial Revolution' available at *https://www.gov.za/news/media-statements/president-cyril-ramaphosa-appoints-commission-fourth-industrial-revolution-09* accessed on 29 July 2024.

Vincent, Brandi '42 Countries Agree to International Principles for Artificial Intelligence' NextGovFCW available at *https://www.nextgov.com/artificial-intelligence/2019/05/42-countries-agree-international-principles-artificial-intelligence/157189/* accessed on 29 July 2024.

University of Johannesburg 'UJ, TUT and Department of Communications and Digital Technologies launch AI Institute of South Africa' available at *https://news.uj.ac.za/news/uj-tut-and-department-of-communications-and-digital-technologies-launch-ai-institute-of-south-africa-2/* accessed on 30 July 2024.

Department of Communications and Digital Technologies 'National AI Government Summit Discussion Document' available at *https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf* accessed on 27 July 2024.

Vectra AI 'How Vectra AI Detects Threats' available at https://www.vectra.ai/detections accessed on 2 August 2024.

Deepmind 'SythID' available at *https://deepmind.google/technologies/synthid/* accessed on 3 August 3, 2024.

Chainalysis 'Know what happens on blockchains' available at *https://www.chainalysis.com/company/* accessed on 16 March 2023.

The 'Policy Brief on Clarifying Copyright to Enable AI Research in Africa' (published 1 May 2024).

Marques, Carlos 'Content Piracy: What You Don't Know Can Hurt You', available at https://blog.mobileum.com/content-piracy-what-you-dont-know-can-hurt-you accessed on 19 March 2024.

The White Paper on On Artificial Intelligence - A European approach to excellence and trust (COM 65 final 19 February 2020).

The White Paper on A pro-innovation approach to AI regulation (815 29 March 2023).

The UK Industrial Strategy Artificial Intelligence Sector Deal available at https://assets.publishing.service.gov.uk/media/5ae0f342e5274a0d85c1c6d5/180425_

BEIS_AI_Sector_Deal__4_.pdf accessed on 24 February 2025.

The Emirates Blockchain Policy (published in April 2018).

Christopher Tredger 'ITWebAI2025: SA's National AI Policy framework under construction but promises much' ITWeb available at https://www.itweb.co.za/article/itwebai2025-sas-national-ai-policy-framework-under-construction-but-promises-much/JBwEr7n3oXeM6Db2 accessed on 9 March 2025.

Hanani Hlomani 'Why South Africa needs a more holistic and contextual approach to AI regulation' Daily Maverick available at https://www.dailymaverick.co.za/article/2023-05-23-why-south-africa-needs-a-more-holistic-and-contextual-approach-to-ai-regulation/ accessed on 8 March 2025.

Valeria Gallo and Suchitra Nair 'The UK's framework for AI regulation' Deloitte available at https://www.deloitte.com/uk/en/Industries/financial-services/blogs/the-uks-framework-for-ai-regulation.html accessed on 8 March 2025.

The South African National AI Policy Framework (published 14 August 2024)