THE IMPLICATIONS OF EMERGING TECHNOLOGIES ON INTELLECTUAL PROPERTY RIGHTS IN NIGERIA: BLOCKCHAIN AND BIOMETRICS IN PERSPECTIVE

Temitope O. Oloko *

Abstract

The emergence of blockchain and biometrics has had profound implications for intellectual and privacy rights. These technologies can potentially revolutionize various sectors, including healthcare, supply chain management, finance, and e-government. Even though they have their benefits, there are significant concerns regarding security and privacy issues related to data protection, consent, identity theft, and surveillance. These emerging technologies can potentially disrupt traditional notions of privacy and intellectual property, as they rely on the collection and sharing of vast amounts of personal data, raising questions about ownership, control, and consent. Hence this paper examines how the integration of blockchain technology could play a pivotal role in protecting intellectual property rights by enabling secure and transparent transactions, while also addressing the challenges associated with privacy concerns in biometric data collection and usage. Adopting a doctrinal method of legal research, the study evaluates the potential of blockchain to enhance privacy and safeguard personal data against unauthorised access and breaches, aligning with global standards such as the European Union General Data Protection Regulation. Additionally, the paper explores the dynamics of biometrics as a means to bolster security and identity verification in various sectors, while also identifying its inherent risks related to privacy rights. The implications of these technologies are analyzed in light of Nigeria's legal framework, ethical considerations, and the need for policy development to regulate technology integration while preserving intellectual and privacy rights. The paper concludes that there is a need to establish robust protections and standards to mitigate the risks associated with the adoption of these technologies in Nigeria.

Keywords: Intellectual property rights, privacy, blockchain, biometrics

1. Introduction

Blockchain and biometrics are two emerging innovations that are transforming the way data is used and the safeguard mechanism that improves digital identity management. Blockchain's decentralised and immutable nature has sparked widespread interest in its ability to secure and

* Temitope O. Oloko Faculty of Law Lagos State University Ojo.

 https://doi.org/10.59568/KIULJ-2024-6-2-01

administer intellectual property rights (IPRs).[1] Blockchain technology is still emerging although it has been in existence since 2008.[2] Blockchain technology is a combination of technologies which have been merged in a "new and creative way to give us an amazing new platform to build solutions".[3]According to Chapman, Blockchain presents a fundamental change in the way information is stored and shared, it "is a distributed ledger that records transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks".[4] He further expounded on mechanisms by stating that blockchain technology secures data by grouping transactions into "blocks" and linking them chronologically. Each block is cryptographically sealed, making alterations practically impossible to change every subsequent block and guaranteeing the permanence of the recorded data.[5] The key concept to comprehend in blockchain is decentralisation 'which is a departure from traditional centralised systems like banks or government registries.'

Blockchain revolutionises intellectual property management by providing a secure, transparent, and immutable record of creation and ownership. This technology minimises fraud, simplifies transactions, and strengthens IP protection. Blockchain is a digital ledger where every entry is set in stone. The unalterable nature of blockchain ensures the integrity of recorded transactions. Once a transaction is validated and added to the chain, it cannot be modified or erased, creating a permanent and tamper-proof history. This feature is particularly valuable for IPRs because it ensures that records of creation, ownership, and changes to intellectual property are tamper-proof and indisputable. For example, when an artist registers a new work on a blockchain, that record becomes unalterable proof of authorship, providing a secure and transparent way to establish the originality and ownership of the work. By distributing control and eliminating single points of failure, this system enhances security and mitigates the risks of manipulation or fraud. This decentralised approach, when applied to intellectual property, has the potential to establish a robust and trustworthy platform for the recording, verification, and transfer of ownership and licensing rights. This feature is particularly valuable for IPRs because it ensures that records of creation,

[1] G Gürkaynak and others 'Intellectual Property Law and Practice in the Blockchain Realm' (2018) 34 *Computer Law & Security Review* 847-862.
[2] S Nakamoto 'Bitcoin: A Peer-to-peer Electronic Cash System' (2008) https://bitcoin.org/bitcoin.pdf. (Accessed 14 May 2024).
[3] S Rathore *Concepts of Blockchain e-book* (2022) 24.
[4] A Chapman *Blockchain the Autodidact's Toolkit. A* (2023) 3.
[5] Chapman (n 4).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

ownership, and changes to intellectual property are tamper-proof and indisputable. For example, when an artist registers a new work on a blockchain, that record becomes unalterable proof of authorship, providing a secure and transparent way to establish the originality and ownership of the work. Blockchain provides a transparent and secure way to record transactions which is great for intellectual property. Its unchangeable nature means intellectual property records are safe and fraud is impossible as there is an immutable history of production and ownership. Unfortunately, this also means it is harder to fix mistakes in the record which is why blockchain needs to be modified in this area.[6]

With blockchain, each transaction or update related to an IP asset is recorded in a secure and immutable manner. Once a record is added to the blockchain, it cannot be altered or deleted, ensuring the integrity and authenticity of the information. This immutability is a powerful feature, as it prevents unauthorised modifications and reduces the risk of fraud, guaranteeing that the history of production and ownership is accurate and trustworthy. In traditional databases, mistakes can be corrected relatively easily by updating or deleting entries. On the blockchain, the immutability that protects against fraud also means that any error, whether it is a clerical mistake or a more significant issue, is permanently recorded. This characteristic can complicate the process of rectifying inaccuracies or updating information. For instance, if an IP record contains incorrect data, the only way to address it is by adding a new transaction that acknowledges and corrects the mistake, rather than modifying the original entry. This can lead to a more complex and cumbersome process for managing records, particularly in industries where accuracy and up-to-date information are critical.

Biometrics, on the other hand, is a fast-evolving area that uses distinctive bodily traits to improve security and personal identity.[7] Webster's Dictionary defines biometrics as the measurement and analysis of unique physical or behavioural characteristics (such as fingerprint or voice patterns), especially as a means of verifying personal identity.[8] According to Petrovska-Delacrétaz, biometric applications offer four distinct approaches to individual recognition: verifying claimed

[6]M Swan 'Blockchain: blueprint for a new economy' (2015) http://cds.cern.ch/record/2000805. (Accessed 15 May 2024).
[7] Maria del Coro *et al* 'Managing intellectual property rights in innovation: the key to reaching the market' *WIPO Magazine* March 2021, https://www.wipo.int/wipo_magazine/en/2021/01/article_0009.html (Accessed 29 May 2024).
[8] 'Biometrics Definition & Meaning' *Merriam-Webster Dictionary* https://www.merriam-webster.com/dictionary/biometrics (Accessed 29 May 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

identities, ensuring non-enrollment, matching against a defined database (closed-set), or identifying within a potentially vast pool while rejecting imposters (open-set).[9]

In the rapidly evolving digital landscape, the intersection between IP and biometrics has become a crucial area of exploration and concern. Biometric data, inherently unique to each individual, is increasingly used to protect IP itself. The intersection of IP and biometrics is a complex and evolving field, driven by advancements in artificial intelligence (AI) and the increasing use of biometric data for identification and authentication. For instance, biometric authentication can secure access to sensitive databases containing patented inventions or copyrighted works, preventing unauthorised access and infringement.[10] The sensitivity of biometric information necessitates robust data protection frameworks and consent protocols. Striking a balance between leveraging biometrics for enhanced IP security and safeguarding individual rights remains an ongoing challenge, requiring careful consideration by policymakers, innovators, and the public alike. These advancements have profound implications for the protection and management of IP, as biometric data can be considered a form of personal information that may be subject to various IP-related laws and regulations.[11] In addition, the use of biometrics in authentication and identification processes has the potential to enhance the security and integrity of IP-protected systems, providing a more reliable and tamper-resistant method of access control.[12]

In Nigeria, the collection, storage, and processing of biometric data also raises significant privacy concerns, as this information can be highly sensitive and personal. Regulatory bodies, such as the National Information Technology Development Agency (NITDA), have sought to address these challenges by establishing guidelines[13] and safeguards for the use of biometric data, striking a balance between the benefits of biometric technologies and the need to protect individual privacy.

[9] D Petrovska-Delacrétaz *et al Guide to Biometric Reference Systems and Performance Evaluation* (Springer-Verlag London Ltd 2009).
[10]The Michelson Institute for Intellectual Property 'Biometrics as intellectual property in an AI-Driven world' https://michelsonip.com/biometrics-as-intellectual-property-in-an-ai-driven-world/ (Accessed 29 May 2024).
[11] K Modi & L Devaraj 'Advancements in Biometric Technology with Artificial Intelligence' (2022) *Cornell University* https://doi.org/10.48550/arxiv.2212.13187. (Accessed 29 May 2024).
[12] T Board 'Biometric Recognition: Challenges and Opportunities' (2010) https://www.amazon.com/Biometric-Recognition-Challenges-Opportunities-Cybersecurity/dp/0309142075. (Accessed 29 May 2024).
[13] Nigeria Data Protection Regulation 2019.

 https://doi.org/10.59568/KIULJ-2024-6-2-01

To address these challenges, there is a growing recognition that blockchain systems may need to be modified to better accommodate the specific needs of intellectual property management. One potential solution is the development of protocols that allow for the inclusion of corrective transactions or annotations that can clarify or supersede previous records. These protocols would enable the blockchain to maintain its integrity and immutability while providing a mechanism for addressing errors or changes in the status of IP assets. Another approach could involve the creation of specialised smart contracts that can automate certain aspects of IP management, such as licensing and royalty payments, while also including provisions for dispute resolution or error correction. While blockchain technology offers significant advantages for managing intellectual property, its unchangeable nature also presents challenges that need to be addressed. By exploring modifications to blockchain protocols and smart contract designs, it may be possible to create a system that combines the benefits of transparency, security, and immutability with the flexibility needed to correct mistakes and adapt to changing circumstances.

Against this background, this explores the implications, benefits and challenges of blockchain and biometrics for intellectual property and privacy rights. The rest of this paper is divided into six sections following the introduction. The second section of this paper discusses the meaning and nature of blockchain technology while the third section dwells on the application of biometrics. The fourth section identifies and highlights the interfaces between blockchain and biometrics. The fifth section examines the legal and ethical considerations frameworks to navigate these technologies and use them responsibly and in line with current laws and regulations. The sixth section proffers recommendations for addressing the privacy issues that relate to blockchain technology and biometrics while the final section concludes the paper.

2. Blockchain Technology: An Overview

Nigeria is one of the biggest cryptocurrency markets in the world.[14] The advent of blockchain gradually crept on us from the 1970s when the theories of communication and computation were discussed as a means to provide the tools to solve cryptographic long-standing problems.[15] Diffie and Hellman noted that the development of computer-controlled communication networks has the

[14] N Ogbonna & N Booty 'Binance: Nigeria orders cryptocurrency firm to pay $10bn' https://www.bbc.co.uk/news/world-africa-68451238 (Accessed 15 June 2024).
[15] W. Diffie & ME Hellman 'New Directions in Cryptography' (1976) IT-22 *IEEE TRANSACTIONS ON INFORMATION THEORY* https://ee.stanford.edu/~hellman/publications/24.pdf. (Accessed 15 June 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

potential for 'effortless and inexpensive contact between people or computers on opposite sides of the world,' and that this system could replace traditional communication systems, but must be made secure. [16] This concept introduced the idea of digital ledger technology (DLT). To foster trust among mutually distrusting groups, Chaum[17] proposes a distributed computer system that leverages physically secure "vaults," established cryptographic techniques, and the novel concept of threshold secret sharing to guarantee secure group management, private transactions, and individual privacy. Chaum's vault system lays out a foundational framework for blockchain governance by defining four key participant roles: Watchers (passive observers of the ledger), Doers (transaction executors and state providers), Executives (block validators), and Czars (policy setters and executive appointers). He refers to these positions as "bodies," and he leaves open the possibility of them being implemented as algorithms, hinting at the potential for automated governance in such systems.[18] In those two-research eavesdropping was a major concern because the information had to go through a third party.

This concept was further advanced in the 1990s by Haber and Stornetta,[19] which proposed time mathematically sound and computationally to create a solution to time stamping data, by using a method that allows the client to verify the accuracy of the document's time-stamp. Dwork and Naor,[20] explored the computational approach to reduce the prevalence of unsolicited mail and ensure fair use of shared resources by imposing a cost on the sender, thereby discouraging abuse.

In 1997, Back introduced "hashcash," a proof-of-work system designed to mitigate denial-of-service (DoS) attacks, the mechanism was set up to prevent email spam which influenced the many modern systems, and the idea of creating a digital currency such as cryptocurrencies like Bitcoin, which use similar proof-of-work concepts to secure transactions. Still in the 1990s Wei,[21]

[16] Diffe (n 15).
[17] DL Chaum, 'Computer systems established, maintained, and trusted by mutually suspicious groups' Electronics Research Laboratory, University of California, Berkeley, UCB/ERL M79/10 1979 computer-systems-by-mutually-suspicious-groups.pdf (nakamotoinstitute.org) (Accessed 15 June 2024).
[18] Chaum (n 17)
[19] S Haber & WStornetta How to Timestamp a Digital Document' (1991) 3 *Journal of Cryptology* 99-111 https://link.springer.com/article/10.1007/BF00196791. (Accessed 15 June 2024).
[20] Dwork & Moni, 'Pricing via processing or combatting junk mail' in Brickell (ed) *Advances in Cryptology: Proceedings of Crypto* 92 (1993) 139-147.
[21] W Dai 'B-Money: An Anonymous and Decentralized Monetary System' https://nakamotoinstitute.org/library/b-money/ (Accessed 15 June 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

introduced a protocol that empowers untraceable, pseudonymous entities to engage in efficient and more secure collaboration, by establishing a secure medium for exchanging value and enforcing agreements while acknowledging the potential for further optimisation, the author believes this work represents a significant step towards realising the practical potential of crypto-anarchy. The millennium has brought with it significant advancement in technology in all areas, of particular note is the scholarly research of Nakamoto[22] which is the foundational document for Bitcoin and blockchain technology. It proposed a system for electronic transactions without relying on trust, "peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power." Nakamoto's innovation combined the principles of decentralised networks using proof-of-work to timestamp transactions, cryptographic security, solving the double-spending problem and peer-to-peer networking to create a secure and transparent system for digital transactions.

Pulling all the works of the scholars together Sherman *et al*, [23] gave a comprehensive understanding of blockchain systems by analyzing the interplay between four key actors, watchers, doers, executives, and czars and the access, control, and consensus policies governing their functions. The research also provided a structured lens for examining critical system elements and facilitates comparative analysis across different blockchain implementations, given their capacity to address long-standing demands for tamper-proof record-keeping across diverse domains like finance, property, and supply chain management, coupled with robust cryptographic underpinnings and significant ongoing investment, blockchain technologies hold immense transformative potential. This technology helps track assets, both physical (such as cars and land) and non-physical (such as intellectual property) as well as record transactions. As noted by Chapman[24] and other scholars

[22] S Nakamoto 'Bitcoin: A peer-to-peer electronic cash system' (2008) https://nakamotoinstitute.org/library/bitcoin/ https://bitcoin.org/bitcoin.pdf (Accessed 15 June 2024).
[23] AT Sherman and others 'On the Origins and Variations of Blockchain Technologies Cyber Defense Lab' (2018) 1810.06130 (arxiv.org) (Accessed 15 June 2024).
[24] A Chapman *Blockchain the Autodidact's Toolkit*. A (2023) 3.

 https://doi.org/10.59568/KIULJ-2024-6-2-01

[25] understanding how blockchain technology, works to ensure the privacy and security of the data generated we need to look at its key features.[26]

2.1 Core Features of Blockchain Technology

a. Decentralisation

Blockchain technology distinguishes itself through its inherent decentralised peer-to-peer network eliminating the vulnerability of a single point of control. Unlike traditional, centrally managed databases, blockchain distributes a complete copy of the ledger across a network of nodes. These nodes operate under a consensus mechanism, ensuring data synchronisation and integrity. This distributed architecture bolsters security by mitigating the risk of single-point failures and making data tampering exceedingly difficult. Moreover, decentralisation fosters resilience against censorship and undue influence from any single entity, thereby promoting data autonomy and democratic governance.[27]

b. Immutability

Another feature of blockchain technology is immutability. This feature prevents alteration or deletion of the data recorded through cryptographic algorithms and a consensus model, requiring network-wide agreement on the validity of transactions. Each block references the previous one through a hash function, forming an unbreakable chain. Modifying data in an earlier block would require recalculating all subsequent hashes and achieving consensus from the majority of nodes, a task rendered practically impossible by the sheer scale of a robust blockchain network. Blockchain systems are inherently secure, largely due to the cryptographic algorithms they rely on. [28]

c. Transparency

[25] Z Zheng and Others, 'An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends' (2017) *IEEE international congress on big data (BigData congress)* 557-564. Amey and others 'Blockchain & cryptocurrency' (2024) *Indian Scientific Journal Of Research In Engineering And Management* <doi: 10.55041/ijsrem30332>; M Pilkington 'Blockchain technology: principles and applications' (2016) *Edward Elgar Publishing eBooks* https://doi.org/10.4337/9781784717766.00019. (Accessed 16 June 2024).
[26]M Pilkington 'Blockchain technology: principles and applications' in *Edward Elgar Publishing eBooks* (2016) https://doi.org/10.4337/9781784717766.00019. (Accessed 16 June 2024).
[27] Zheng (n 25).
[28] Chapman (n 24).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

Blockchain technology is characterized by its inherent transparency. Given that all transactions are documented on the blockchain, and each node maintains a copy of the ledger, the system exhibits a high level of transparency. This real-time audibility fosters trust and accountability among participants, eliminating the need for traditional intermediaries like banks that typically operate within opaque systems. This represents a fundamental shift from conventional financial models, where transaction data remains privy to involved parties and their institutions.[29]

d. Scalability

As blockchain adoption expands, developers face the ongoing challenge of scalability – enhancing network capacity to handle growing transaction volumes and data loads. The balance between decentralization, security, and scalability, often referred to as the "Blockchain Trilemma," poses a persistent challenge for blockchain architects striving for optimal performance without sacrificing core principles. Lightning Network are being developed which divides the network into smaller, interconnected segments, and layer-two protocols to enable off-chain transactions that can later be reconciled on the main blockchain.[30]

e. Facilitation of cross-border transactions

One of blockchain's most transformative applications lies in its capacity to streamline cross-border transactions by enabling parties in different jurisdictions to transact without intermediaries. This can significantly reduce the cost and complexity of international transactions, promoting global economic inclusiveness and simplifying processes that traditionally involved banks, regulators, and payment processors by eliminating intermediaries and enabling direct peer-to-peer transactions across geographical boundaries. These foundational features underpin blockchain's disruptive potential across a wide array of industries. Beyond its cryptocurrency origins, blockchain technology is poised to revolutionize sectors like finance, supply chain management, intellectual property rights, and more. This is a developing area and its ability to grow is enormous its impact is expected to broaden, potentially reshaping the very fabric of our economic and social infrastructure.[31]

[29] Chapman (n 24).
[30] Chapman (n 24).
[31] GE 'Blockchain's Practical and Legal Implications for Global Trade and Global Trade Law' in MBurri (ed) *Big Data and Global Trade Law* (2021) 128-159; Chapman (n 24).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

2.2. Potential Benefits of Blockchain for Intellectual Property

Intellectual Property (IP) is a crucial branch of law that safeguards the creations of the human mind, often considered some of the most beautiful manifestations of human imagination.[32] It encompasses the legal rights granted to individuals and entities over their inventions, innovations, creative works, and other intangible assets recognised as property. These rights cover a broad spectrum, including inventions, literary and artistic works, designs, symbols, names, and images used in commerce as well as scientific discoveries and industrial designs to trademarks, service marks, and commercial names. Intellectual Property Rights (IPR) are the rights granted to creators and inventors to protect their work from unauthorised and unfair use by others. [33] [34] These rights are inherently preventive, allowing the owner to exclude others from using this subject matter without their authorisation. For example, a patent grants the inventor the right to preclude others from making, using, or selling the invention without permission.[35] Similarly, copyright protects literary and artistic works, giving creators the exclusive right to reproduce, distribute, and perform their works.[36]

The concept of intellectual property also imposes certain duties and responsibilities. While it grants the owner exclusive rights, it also requires them to respect the rights of others and to use their IP in a manner that does not infringe on the rights of others. This balance of rights and duties is essential for fostering innovation and creativity while ensuring fair competition and the free flow of ideas.[37] Intellectual property law encompasses the legal framework that governs these rights. It addresses the protection of creative efforts, inventions, and the commercial reputation or goodwill associated with a business.[38] This area of law is vast and complex, covering everything from copyright, patents, and trademarks to the protection of trade secrets and the rights of performers and broadcasters. It seeks to strike a balance between the interests of creators and the public, ensuring that creators are rewarded for their contributions while also promoting the dissemination

[32] WR Cornish *Intellectual Property* (1995) 3.
[33] Art 2, para viii, World Intellectual Property Organization (WIPO) Convention 1967.
[34] CN Saha & S Bhattacharya 'Intellectual property rights: An overview and implications in the pharmaceutical industry' (2011) 2 *J Adv Pharm Technol Res*. 88-93. doi:10.4103/2231-4040.82952 (Accessed 26 June 2024).
[35] Patent and Designs Act P2 LFN 2004. Sec 6(1).
[36] Copyright Act 2022 secs 9-13.
[37] RK Bera 'The Global Importance of Patents' (2009) 96 *Current Science Journal* https://www.jstor.org/stable/24104555 (Accessed 26 June 2024).
[38] Saha (n 34).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

of knowledge and cultural expression.[39] Blockchain technology has immense potential for intellectual property (IP), especially concerning improving ownership attribution and copyright protection[40]. Traditionally, management techniques for IP have often been frustrated by issues such as piracy, unauthorised use, and difficulty in proving ownership rights. Blockchain's inherent features enable it to surmount these challenges.

2.2.1 Copyright Protection and Ownership Attribution

Copyright, like most legal concepts, has no precise definition. It is a benefit that arises at no cost to the creator.[41] Copyright is a domain of intellectual property that protects the results of imaginative efforts, including but not limited to original text, artwork, computer programs, photographs, recordings, broadcasts, musical scores and films.[42] It is an entitlement given against the copying of defined types of cultural, informational and entertainment productions. It is a legal system that protects the creative outputs of authors by granting them exclusive powers to control the use of their creations for a / time, subject to certain limitations, exceptions and statutory licensing arrangements allowing use and exploitation without the author's consent.[43] Blockchain's immutable and transparent nature ensures that once a copyright is registered on the blockchain, it cannot be tampered with. This provides the user with a credible and provenance record. For instance, regarding copyright infringement issues, blockchains may act as indelible ledgers indicating when the work was created, who owned it at what time and any changes thereof. This can make proving ownership and addressing allegations of copyright infringement much easier. There are various ways in which blockchain can be used in copyright, they include immutable records of ownership, automated royalty payments, transparent copyright transfer, anti-piracy measures, decentralized content management and digital rights management (DRM). The paper will discuss the three most relevant uses to Nigeria currently.

---

[39] Article 19, 'Balancing the Right to Freedom of Expression and Intellectual Property Protection in the Digital Age' December 2012 https://www.article19.org/data/files/medialibrary/3716/13-04-25-share-BACKGROUND-PAPER.pdf (Accessed 26 June 2024).
[40] T Krajewski 'Blockchain and Intellectual property' (2019) *Social Science Research Network* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3316992 (Accessed 26 June 2024).
[41] Copyright Act 2022 sec 4; WR Cornish and D Llewelyn *Intellectual Property: Patents, Copyright, Trademarks and Allied Rights* (2003) 8.
[42] WIPO 'Understanding Copyright and Related Rights' (2016) 3 https://www.wipo.int/edocs/pubdocs/en/wipo_pub_909_2016.pdf. (Accessed 26 June 2024).
[43] WIPO (n 42).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

a. Streamlining Royalty Payments and Licensing

The possibility of royalty payments via smart contracts is among the things that blockchain technology might contribute towards expediting licensing. Conventional royalty distribution is frequently beset by delays and inefficiencies.[44] Smart contracts on blockchain technology can automate the payment process so that artists get paid early enough without making errors with the time or amount due to them. For instance, with the deployment of blockchain technology, the Copyright Society of Nigeria (COSON) may improve its royalty distribution system. Through the implementation of an immutable and open ledger system, COSON can ensure the receipt of compensation for the works of creators and artists. Smart contracts are capable of cutting down the need for middlemen and administrative costs by distributing royalties automatically, under specified parameters.[45]

b. Anti-Piracy Measures

One of the problems bedevilling copyright in Nigeria is piracy. The advancement in technology has also brought about the ease of copying protected works and can also play a pivotal role in fortifying IP. Blockchain technology offers a robust solution to combat IP piracy. Its decentralized and immutable nature provides a secure platform for creators to share their work while protecting their IP. Its decentralized and immutable nature provides a secure platform for creators to share their work while protecting their intellectual property. The transparent ledger ensures clear ownership records, eliminating disputes. Smart contract usage enforcement rules help in reducing unauthorized use, ensuring fair and secure management of digital and intellectual property rights.[46] Additionally, cryptographic techniques ensure data integrity and detect tampering, making it extremely difficult to tamper with or alter digital content. Consequently, the use of blockchain features enables creators to securely share their content through various means such as forensic watermarking and content monitoring ensuring that unauthorized copies can be detected and addressed thereby preventing misuse of copyrighted work. The Act makes provision to make regulations specifying the conditions necessary to give effect to prescribe any design, label, mark,

[44]A Damodaran 'Royalty payments on intellectual property: A preliminary analysis of the principal policy issues facing India' (2017) *Social Science Research Network* https://doi.org/10.2139/ssrn.3100144 (Accessed 28 June 2024).
[45] H Taherdoost 'Smart contracts in blockchain technology: A critical review' (2023) 14 *Information* 117 https://doi.org/10.3390/info14020117 (Accessed 28 June 2024).
[46] D Dadhich 'Preventing Digital and Intellectual Property Piracy: A Global Perspective' Preventing Digital and Intellectual Property Piracy: A Global Perspective | by Dhanraj Dadhich | Medium (Accessed 29 June 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

impression or any other anti-piracy device for use on, in, or in connection with any work in which copyright subsists.[47] In section 50[48] "technological protection measure" means a technology, device, product or component incorporated into the work which is designed to effectively prevent or inhibit the infringement of any copyright or related right" The Act considers a technological protection measure effective if, during its regular operation, it controls access to a protected work or prevents/restricts unauthorized actions concerning the work, unless those actions are permitted by law. However, this provision does not apply to measures that, in their normal operation, solely control access for non-infringing purposes.[49]

c. Digital Rights Management (DRM)

The primary goal of DRM is to give content creators maximum control over their digital works by setting specific terms and conditions for access and use, however, it also brings challenges related to falsification, alteration, or removal of rights management information. The integration of blockchain technology into digital rights management (DRM) systems has introduced new ways to protect and manage intellectual property which involves software and hardware that define, protect, and manage rules for accessing and using digital content.[50] DRM aims to give rights holders extensive control over digital content through self-enforcing terms and conditions. It supports the distribution of electronic books, digital movies, music, games, software, and other digital objects.[51] This control is typically enforced through license agreements that translate into technical restrictions within the DRM architecture. DRM involves software and hardware that define, protect, and manage rules for accessing and using digital content. These systems are popular in the media industry for enforcing copyright and neighbouring rights and blockchain, DRM systems can provide secure and efficient management of digital rights, enabling piracy detection and prevention while ensuring fair compensation for creators.[52]

[47] Copyright Act 2022 sec 49.
[48] Copyright Act 2022 sec 50(3).
[49] Copyright Act 2022 sec 50(3)(c).
[50] M Finck & V Moscon 'Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management' (2019) 2.0. *IIC 50* 77–108 (2019) https://link.springer.com/article/10.1007/s40319-018-00776-8#citeas (Accessed 30 June 2024).
[51] S Ramani and others 'Blockchain for digital rights management' in SK Hafizul Islam and others (eds) *Hybrid computational intelligence for pattern analysis, blockchain technology for emerging applications* (2022) 177-205.
[52] A Savelyev 'Copyright in the blockchain era: Promises and challenges' (2018) 34 *Computer Law & Security Review* 550-561.

 https://doi.org/10.59568/KIULJ-2024-6-2-01

3. Biometrics: Applications and Concerns

Biometrics generally refers to technologies that measure and analyze unique human physical or behavioural characteristics.[53] Its operation is more easily understandable because its use has been in existence for centuries. This technology has two major applications one of which is when people are being watched while the other one pertains to access control.[54] In the context of surveillance, biometrics is used to monitor individuals in real-time or retrospectively by analyzing video footage the system can employ facial recognition technology to identify and track individuals in public spaces, such as airports, train stations, and sports arenas.[55] These systems can compare the captured facial images with a database of known individuals to identify persons of interest, such as wanted criminals or missing persons.[56] Biometric surveillance has become an essential tool for law enforcement and security agencies, as it offers a non-intrusive way to monitor large crowds and identify potential threats. Additionally, biometric data can be used to analyze patterns of behaviour, helping to predict and prevent criminal activities. For instance, gait recognition, which analyzes an individual's walking pattern, can be used to identify suspects or detect unusual behaviour. The word "biometrics" has its roots in the Greek language; it is derived from the words bio meaning life and metric meaning to measure[57]. Biometric technologies have been employed extensively within the identification space due to their ability to accurately identify individuals based on their individualistic physiological or behavioural traits which are unique to them alone. The Nigeria Data Protection Act, of 2023 defines biometric data to mean personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition and deoxyribonucleic acid (DNA) analysis.[58]

---

[53] JA Unar and others 'A review of biometric technology along with trends and prospects' (2014) 47 *Pattern recognition* 2673-2688.
[54] A Jain 'An introduction to biometric recognition' (2004) 14 *IEEE Transactions on Circuits and Systems for Video Technology* 4–20 https://doi.org/10.1109/tcsvt.2003.818349. (Accessed 30 June 2024).
[55] AA Gikay 'Regulating use by law enforcement authorities of live facial recognition technology in public spaces: An incremental approach' (2023) 82 *The Cambridge Law Journal* 414-449.l doi:10.1017/S0008197323000454 (Accessed 30 June 2024).
[56] Gikay (n 55).
[57] C Fontesl 'AI-powered public surveillance systems: why we (might) need them and how we want them' (2022) 71 *Technology in Society* https://doi.org/10.1016/j.techsoc.2022.102137. (Accessed 4 July 2024).
[58]Nigeria Data Protection Act, 2023 s. 65 https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf (Accessed 4 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

3.1. Prominent Types of Biometric Technologies

Biometric identifiers are divided into two main types: physiological and behavioural characteristics.

a. Physiological Biometrics

These types of biometrics rely on the physical characteristics of a specific individual. Various types of physiological biometrics are in use in Nigeria, however, the most common ones are fingerprint technology which captures the unique patterns of ridges and valleys on each finger. Since fingerprints are unique and do not change, this method is often used for controlling access and identifying individuals.[59] Also facial recognition system identifies people by analyzing their facial features. It creates a digital map of a person's face by measuring the space between their eyes, nose, mouth, and jawline.[60] This map is then matched with stored information to help identify or verify the person.[61] Retina Scanning uses the unique pattern of blood vessels in the retina, which is found at the back of the eye. The retinal pattern is a dependable way to identify someone because, like the iris, it is unique and does not change over time. Iris Recognition Analyzes the intricate patterns in the coloured ring surrounding the pupil, offering high accuracy.[62] DNA matching is not commonly used for regular security checks because it is complex and expensive. However, it uses the unique genetic code in each person's DNA and is extremely useful in forensic science and legal cases. Just like a fingerprint or iris pattern, your voice has distinct qualities that can be used for authentication.

b. Behavioral Biometrics

Signature is regarded as one of the behavioural biometrics. While often considered a simple act, signing your name is a complex behavioural biometric that can be used for authentication. Signature analysis recognises each person's signature uniquely. To check signature verification, factors like pressure, speed, and the sequence of strokes are used to analyse the signature data.

[59]H Biswas and others 'Smart city development: Theft handling of public vehicles using image analysis and cloud network' in *Elsevier eBooks* (2021) 155–169 https://doi.org/10.1016/b978-0-12-822844-9.00013-x. (Accessed 4 July 2024).
[60] R J Baron 'Mechanisms of human facial recognition' (1981) 15 International *Journal of Man-machine Studies*, 137–178 https://doi.org/10.1016/s0020-7373(81)80001-6 (Accessed 4 July 2024).
[61] Mohammad Saber Niazy, Nijad Ahmad, Zahra Habibi, Badam Niazi *Australian Journal of Engineering and Innovative Technology*, 2023.
[62] JB Mazumdar 'Retina based biometric authentication system: A review' (2018) 9 *International Journal of Advanced Research in Computer Science* 711–718 https://doi.org/10.26483/ijarcs.v9i1.5322. (Accessed 4 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

Online signature verification of signature data is done in real time using digital devices like tablets or touchscreens. The technological advancement, signature verification systems are becoming more sophisticated and accurate. Researchers are exploring new techniques, such as using artificial intelligence and machine learning algorithms, to improve forgery detection and enhance the reliability of this biometric method for the protection of IP. Voice recognition technology also known as speaker recognition identifies people by analyzing their voice patterns through voiceprint authentication by looking at like pitch, tone, and speaking style.[63] Another unique profile for identification is the movement or gait of an individual such as stride length and walking speed.[64]

By removing the need for more complicated security methods such as passwords or physical tokens, these biometric solutions enhance security and make things easier.[65] The use of biometric technology fulfils the need for efficient, scalable identity management systems and improves security in both worldwide and Nigerian situations. The application of biometric technology in banking and elections, particularly in Nigeria, highlights the importance of enhancing security and transparency.

3.2. The Use of Biometrics in Authentication and Identification

Identification and authentication procedures heavily rely on biometric technologies. To authenticate a person's claimed identity, their biometric data is compared to a stored template. On the other hand, identification involves matching the provided biometric data against multiple stored templates to determine a person's identity. Biometrics offer greater security than traditional methods like passwords and PINs, which can be easily forgotten, stolen, or guessed. Since biometric features are unique to each person, they are difficult to copy or steal. For instance, access control systems and smartphones often use fingerprint and facial recognition technologies, providing secure and seamless user experiences.[66] Large-scale detection applications, including

[63]V Mann 'Development of voice recognition: Parallels with face recognition' (1979) 27 *Journal of Experimental Child Psychology* 153–165. https://doi.org/10.1016/0022-0965(79)90067-5 (Accessed 4 July 2024).
[64]RB Davis 'A gait analysis data collection and reduction technique' (1991) 10 *Human Movement Science* 575–587. https://doi.org/10.1016/0167-9457(91)90046-z (Accessed 4 July 2024).
[65] Manoj *et al* 'Biometrics: an introduction to new modes of security' (2015) *International Journal of Modern Trends in Engineering and Research.*
[66]A Ross and others 'Information fusion in biometrics' (2003) 24 *Pattern Recognition Letters* 2115–2125. https://doi.org/10.1016/s0167-8655(03)00079-5 (Accessed 8 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

border control, law enforcement, and national inspection systems, require the use of biometric technology. Authorities can improve security, speed up processes and better identify people by matching biometric data against a larger database.[67] Nigeria, for example, uses biometric technology for voter authentication and registration to ensure the integrity of electoral processes.

3.3. Privacy Risks Associated with Biometric Data

While biometric technology has many advantages, its use poses serious privacy risks. Since biometric data is sensitive, strict precautions must be taken to avoid misuse and unauthorised access. Data breaches, unauthorised access, and the possibility of surveillance and personalisation are the three main privacy threats.

3.4. Data Breaches and Unauthorised Access

Biometric data is incredibly private and it can have serious ramifications if it is stolen. Biometric traits are not replaceable in case of theft, unlike passwords. Identity theft, fraud, and other malicious activities may result from incidents causing biometric data to be intercepted. The security issues and suggestions for a secure biometric authentication system as detailed by Bhartiya et al have been effectively addressed in their study. To protect biometric data from breaches and undesirable access it is important to use multiple factors for authentication, secure storage, and encryption.

3.5. Potential for Surveillance and Profiling

These biometric technologies similarly open up concerns around profiling and surveillance. Whilst those biometric and facial recognition systems are being used, they are also watched and monitored in real-time meaning that the monitoring that goes on with such technologies could lead to the normalisation of surveillance or always-on surveillance, adding to the invasion.[68] Whiskerd et al focus on the importance of data protection rules and universal human rights while discussing the criteria that biometrics need to fulfil to maintain privacy. They go on to posit that even though biometric systems have the potential to improve safety, they must be designed with privacy as a

[67]NK Ratha *et al* 'Enhancing security and privacy in biometrics-based authentication systems' (2001) 40 *IBM Systems Journal* 614–634 https://doi.org/10.1147/sj.403.0614 (Accessed 8 July 2024).
[68] S Wachter 'Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR' (2018) 34 *Computer Law & Security Review* 436 https://doi.org/10.1016/j.clsr.2018.02.002. (Accessed 8 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

priority and comply with laws like the General Data Protection Regulation (GDPR). In the case of biometric technology, two ethical dilemmas are involved; the first is that of consent. Individuals must have the opportunity to opt out of having their biometric data collected or used. An individual's consent should be informed by understanding the risks and implications involved with biometric data use, and individuals must be transparently informed about how their data is being treated. The second issue is that of bodily integrity. In the collection of biometric data, companies should be non-intrusive and non-coercive in their methods. They must respect the privacy of individuals and their bodies.[69] While there are numerous security and practical benefits associated with biometrics, there are privacy risks and ethical dilemmas to consider. To use biometrics, it is important to secure biometric data with strong security protocols, compliance and individual rights.

4. Synergies between Blockchain and Biometrics

The integration of biometrics and blockchain technology is beneficial in many ways for enhancing the efficiency and security of digital identity management. Blockchain technology itself can help a decentralised ledger to be maintained by nodes which could be untrusted and to provide services that are reliable and irreversible. This is very important for biometric systems where protecting personal identifier information is a must. By improving the properties of security, transparency, scalability and decentralisation, the use of blockchain technology can make a significant improvement to biometric authentication. In addition, the immutability property of blockchain ensures that biometric data is kept secure and immutable once it is stored, representing a significant hurdle to data alteration. Blockchain technology has significant potential to enhance the audibility and accountability of data storage[70]. This is because it can ensure the unadulterated preservation of biometric patterns, a necessary feature for security and legal interests. There also exists the opportunity for blockchain technology to foster the development of important decentralised applications, which are autonomous from a central authority and increase the security and trustworthiness of biometric authentication systems.

[69]M Faundez-Zanuy 'Privacy issues on biometric systems' (2005) 20 *IEEE Aerospace and Electronic Systems Magazine* 13–15 https://doi.org/10.1109/maes.2005.1397143. (Accessed 8 July 2024).
[70] S Saberi 'Blockchain technology and its relationships to sustainable supply chain management' (2018) 5 *International Journal of Production Research* 2117–2135 https://doi.org/10.1080/00207543.2018.1533261. (Accessed 8 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

4.1. Enhanced Security for Biometric Data Storage and Transfer

The advantage of incorporating blockchain technology into biometric identification lies in its ability to ensure the security of storing and transmitting data. For the traditional centralised database, it is easy to have security loopholes in the storage or during the data transmission stage, especially for sensitive biometric data. These security vulnerabilities can allow biometric data to be misused or accessed without authorisation. Blockchain achieves secure storage and efficient transmission of biometric data by the distributed mode of data storage among redundant nodes while utilising its decentralised architecture, thus placing more obstacles in the way of malicious attackers who wish to exploit the data and down the system[71]. Furthermore, the cryptographic features of blockchain are used to encrypt and protect biometric data from generation to transmission, seeking to prevent unauthorised access and guaranteeing the integrity and confidentiality of biometric data.

4.2. Improved Transparency and Accountability in Biometric Systems

Blockchain technology in biometric systems increases transparency and accountability. A blockchain is a timestamped, irreversible transaction record that makes it transparent and verifiable audit trails.[72] Transparency is very beneficial in identity management, where verifying the authenticity and validity of biometric data is crucial. Blockchain allows businesses to keep biometric transactions permanently so that changes or access to the data are documented and can be viewed. Transparency not only aids regulatory compliance but also boosts our confidence in biometric technology.

4.3. Amplified Risks and Challenges

Blockchain and biometrics have potential advantages but there are some challenges that they may pose. Blockchain networks could pose a problem, especially for real-time applications that require speed. Biometric verifications may not be possible in current blockchain frameworks, making it difficult to use them in practical scenarios where immediate authentication is necessary.

[71] MA Khan *et al* 'IoT security: Review, blockchain solutions, and open challenges' (2018) 82 *Future Generation Computer Systems* 395–411 https://doi.org/10.1016/j.future.2017.11.022. (Accessed 15 July 2024).
[72] P Centobelli 'Blockchain technology for bridging trust, traceability and transparency in the circular supply chain' (2022) 59 *Information & Management* https://doi.org/10.1016/j.im.2021.103508. (Accessed 15 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

4.4. Exacerbated Privacy Concerns Due to Data Permanence on the Blockchain

The permanence of data on the blockchain poses significant privacy challenges for the fusion of biometrics and blockchain. The inability to alter or remove biometric data that has been stored raises questions about data privacy and the right to be forgotten.[73] Blockchain data storage is permanent, so it could be cumbersome to vet unauthorised access and protect people's privacy in the event of a breach or misuse. To minimise privacy risks, it is essential to strategically store biometric data on the blockchain, including methods like hashing or encryption.[74]

4.5. The Need for Robust Legal and Ethical Frameworks

Robust legal and ethical frameworks are also required for the integration of biometrics and blockchain to handle new difficulties. In blockchain systems, accountability distribution is still difficult, especially when biometrics are included. Concerns like carrying out appropriate Data Protection Impact Assessments must be handled to guarantee adherence to privacy regulations such as the Nigerian Data Protection Act 2018 (NDPA) and Nigeria Data Protection Regulation (NDPR), even if introducing a Public Key Infrastructure (PKI) to biometrics through blockchain is advantageous, it must be implemented carefully to prevent the creation of new weak spots or vulnerabilities.[75] Legal frameworks must change to meet the particular difficulties brought about by this fusion of technologies, guaranteeing that people's rights and privacy are sufficiently safeguarded while encouraging innovation and uptake. Biometrics and blockchain require robust legal and ethical frameworks to tackle new challenges. Biometrics and blockchain are a challenge for accountability.[76] Furthermore, even if a Public Key Infrastructure (PKI) for biometrics is a good approach, it must be implemented with caution to avoid creating new issues or other weaknesses. The legal frameworks must be modified to address the specific challenges posed by

[73] S Gardner 'Blockchain's forever memory confounds EU 'right to be forgotten' (2022) *Bloomberg Law*. https://news.bloomberglaw.com/privacy-and-data-security/businesses-adopting-blockchain-question-eus-strict-privacy-law. (Accessed 15 July 2024).
[74] S Yanushkevich 'Inverse biometrics: privacy, risks, and trust' in *Springer eBooks* (2021) 1–4 https://doi.org/10.1007/978-3-642-27739-9_1505-1 (Accessed 15 July 2024).
[75] JD McCabe 'Security and privacy architecture' in *Elsevier eBooks* (2007) 359–383 https://doi.org/10.1016/b978-012370480-1/50010-4 (Accessed 15 July 2024).
[76] C Tankard 'What the GDPR means for businesses' (2016) *Network Security* 5 https://doi.org/10.1016/s1353-4858(16)30056-3 (Accessed 15 July 2024)

 https://doi.org/10.59568/KIULJ-2024-6-2-01

the integration of technologies, guaranteeing the protection of privacy and people's rights while also promoting innovation and adoption.[77]

4.6. Technical Hurdles in Biometric Data Management

Technical limitations in terms of biometric data handling and storage are a barrier to its integration as well. The fault tolerance and decentralisation properties of blockchain are advantageous, but at the same time, stringent security measures should be deployed to avoid any unauthorised access and to ensure the integrity of the biometric data hosted among multiple nodes. In addition, efficient mechanisms should be developed to handle the storage overhead imposed by biometric data on blockchain networks to maintain its scalability and performance. The combination of blockchain technology with biometrics no doubt enhances the security and efficiency of biometric systems; however, there are new challenges as well that need to be addressed through further technological advancements in this area. It is expected that this combination will particularly revolutionise digital identity management processes, but wise steps should be taken to benefit from its advantages rather than introducing more vulnerabilities.

5. Legal and Ethical Considerations

The Nigeria Data Protection Act 2023 and Nigerian Data Protection Regulation 2019 are the legal frameworks governing data protection in Nigeria today.[78] The NDPR was Nigeria's first comprehensive regulation focused on data protection, it was issued by the National Information Technology Development Agency (NITDA) and came into effect on January 25, 2019.[79] The NDPR aims to protect the privacy rights of individuals by ensuring the proper handling and protection of personal data. The NDPA 2023 further strengthens data protection laws in Nigeria and provides a more robust legal framework, addressing some of the gaps in the NDPR. The NDPA establishes the NDPC as the primary regulatory body for data protection in Nigeria.[80] The Commission is responsible for enforcing the provisions of the Act and overseeing data protection

[77] NB Truong and others, 'GDPR-compliant personal data management: A blockchain-based solution' (2020) 15 *IEEE Transactions on Information Forensics and Security* 1746 https://doi.org/10.1109/tifs.2019.2948287 (Accessed 15 July 2024).
[78] O Babalola 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12 *International Data Privacy Law* 44-52.
[79] Nigeria Data Protection Regulation 2019 https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf (Accessed 2 July 2024).
[80] Nigeria Data Protection Act 2023 sec 4.

 https://doi.org/10.59568/KIULJ-2024-6-2-01

practices. It broadens the scope of data protection by covering both public and private sector entities, regardless of their size. It also extends protections to all types of personal data, including sensitive data.[81] These regulations lay out comprehensive criteria for the collection, storage, and handling of personal data, including biometric data. For instance, the NDPA defines sensitive personal data to include personal data relating to an individual's genetic and biometric data, to uniquely identify a natural person.[82] While these frameworks provide a robust foundation for data security, they fall short of addressing the complexities introduced by emerging technologies like biometrics and blockchain. The immutable nature of blockchain technology, when juxtaposed with the DPA's "right to be forgotten",[83] presents significant legal challenges. Moreover, legislative updates often lag behind the swift advancement of biometric technologies, creating gaps in regulation and protection. Additionally, as blockchain and biometric data can easily cross national borders, enforcement and compliance become more complicated, highlighting the limitations of current laws in dealing with inter-jurisdictional issues.

5.1. Ethical Considerations

Informed consent is a crucial ethical factor, requiring individuals to be fully aware of and agree to the use and storage of their biometric data. Data ownership is another major ethical issue, particularly in decentralised systems where determining ownership can be challenging. Blockchain's promise of self-sovereign identification offers a potential solution by giving individuals control over their data, but it also raises concerns about data portability—moving data between systems while maintaining security and privacy.[84] Algorithmic bias presents a significant ethical dilemma in biometric systems. Technologies like facial recognition have faced criticism for potential biases against specific demographic groups, leading to discrimination and unfair treatment.[85] Ensuring ethical deployment requires transparent algorithm development and the implementation of bias mitigation strategies.

[81] Nigeria Data Protection Act 2023 sec 30.
[82] Nigeria Data Protection Act 2023 sec 65.
[83] Nigeria Data Protection Act 2023 sec 34 (d).
[84] R Belen-Saglam *et al* 'A systematic literature review of the tension between the GDPR and public blockchain systems' (2023) 4 *Blockchain Research and Applications* https://doi.org/10.1016/j.bcra.2023.100129 (Accessed 2 July 2024).
[85] S Akter and others 'Algorithmic bias in data-driven innovation in the age of AI' (2021) *International Journal of Information Management 60* https://doi.org/10.1016/j.ijinfomgt.2021.102387 (Accessed 2 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

6. Implications of Biometrics and Blockchain on Intellectual Property

The emergence of blockchain and biometrics has significant implications for the management and protection of intellectual property (IP).[86] Both technologies offer new ways to secure, authenticate, and manage IP assets, but they also raise complex legal, ethical, and technical challenges. Blockchain technology, a decentralised and immutable ledger, can provide a transparent and secure record of IP transactions.[87] This feature is particularly valuable for establishing the provenance and ownership of creative works, patents, and trademarks. By recording the creation and transfer of IP assets on a blockchain, it becomes easier to verify ownership and prevent fraudulent claims.[88] This transparency can simplify the resolution of disputes over IP rights and ensure that creators receive due recognition and compensation. Moreover, blockchain's capability to execute smart contracts—self-executing agreements with terms written in code—can automate licensing processes and royalty payments. For instance, a musician can use a smart contract to automatically distribute royalties whenever their music is purchased or streamed.[89] This automation not only reduces administrative overhead but also minimises the risk of human error or intentional manipulation, ensuring that creators are fairly compensated for their work. However, the use of blockchain in IP management is not without challenges.[90] The irreversible nature of blockchain transactions means that errors or fraudulent entries cannot be easily corrected, posing risks if inaccurate information is recorded. Additionally, the pseudonymous nature of blockchain can complicate the identification of parties involved, making it difficult to enforce IP rights and hold infringers accountable.

This lack of a central authority also raises questions about jurisdiction and the applicability of existing IP laws, which are often designed for more centralised systems.[91] On the other hand, biometric technologies—such as fingerprint recognition, facial recognition, and iris scanning—offer a secure method of authentication based on unique biological traits. These technologies can

[86] S Fabian, 'Blockchain and Intellectual Property Rights' (2020) 25 *Intellectual Property & Tech* 147.
[87] Fabian (n 85).
[88] 'Blockchain Technology and Its Impact on Intellectual Property' https://abounaja.com/blogs/blockchain-technology-and-intellectual-property (Accessed 2 July 2024).
[89] EG Esu, 'Blockchain and Intellectual Property Rights: A Symbiotic Relationship' (2021) 12 Nigerian *Bar Journal* 1-18.
[90] J Andrew *et al* Blockchain for healthcare systems: Architecture, security challenges, trends and future directions' (2023) 215 *Journal of Network and Computer Applications*.
[91] Politou *et al* 'Blockchain Mutability: Challenges and Proposed Solutions' (2019) IEEE Transactions on Emerging Topics in Computing. PP. 1-1. 10.1109/TETC.2019.2949510. (Accessed 18 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

play a crucial role in protecting IP assets by ensuring that only authorised individuals can access sensitive information or digital content. For example, biometric authentication can secure access to a company's proprietary software or a digital library of copyrighted works, preventing unauthorised use and distribution.[92] Biometrics also have potential applications in digital rights management (DRM). By using biometric verification, content providers can ensure that only legitimate users access digital content, thereby preventing piracy and unauthorised sharing.[93] This can be particularly useful in industries like music, film, and publishing, where unauthorised distribution can lead to significant financial losses. Furthermore, biometric systems can create detailed audit trails, documenting who accessed specific IP assets and when which can be invaluable in investigating and addressing potential infringements. Despite these advantages, the use of biometric data in IP management raises significant privacy and ethical concerns.[94] Biometric data is inherently sensitive and cannot be easily changed if compromised, unlike passwords or physical keys.

The collection, storage, and use of such data must be handled with great care to protect individuals' privacy and prevent misuse. For example, the use of facial recognition technology for DRM purposes could lead to concerns about surveillance and the tracking of individuals' consumption habits.[95] This raises important questions about the balance between protecting IP rights and respecting users' privacy. Moreover, the combination of blockchain and biometrics can offer a robust solution for digital identity management in the context of IP. Blockchain can provide a secure and immutable record of digital identities, while biometrics can serve as a reliable method of verifying those identities. This synergy can enhance the security and trustworthiness of digital transactions involving IP assets.[96] For instance, in a scenario where a user wants to access copyrighted content, their biometric data can be verified against a blockchain-based identity

[92] N Boodoo-Jahangeer 'Trends in Biometric Technology' (2010) 16 *University of Mauritius Research Journal* 413-434.
[93] Boodoo-Jahangeer (n 92).
[94] Unpublished: Nakia Stokes Strategies to Reduce the Impact of Digital Piracy in the Media Industry Doctoral Dissertation Walden University https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=16875&context=dissertations (Assessed 18 July 2024).
[95] D Almeida *et al* 'The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks' (2022) 2 AI Ethics 377-387 doi: 10.1007/s43681-021-00077-w. (Accessed 18 July 2024).
[96] S Hamdy and Others 'Blockchain-based biometric identity management' (2023) 27 *Researchgate* 1-12.

 https://doi.org/10.59568/KIULJ-2024-6-2-01

record, ensuring that the user is who they claim to be and has the appropriate permissions. However, integrating these technologies also presents challenges.[97] The transparency of blockchain could conflict with the need for privacy in biometric data, as blockchain's open nature might expose sensitive information. Privacy-enhancing technologies, such as zero-knowledge proofs and homomorphic encryption, are being explored to address these concerns. These technologies aim to allow the verification of information without revealing the underlying data, thus protecting user privacy while maintaining the security and integrity of the blockchain.[98] In conclusion, the implications of blockchain and biometrics on intellectual property are profound and multifaceted.

These technologies offer significant benefits in terms of security, efficiency, and transparency, but they also introduce new challenges related to privacy, ethics, and legal frameworks. As these technologies continue to evolve, policymakers, technologists, and legal experts must collaborate in developing comprehensive guidelines and regulations. These efforts should aim to balance the protection of IP rights with the safeguarding of individual privacy and the promotion of innovation. The future of IP in the digital age will likely depend on how effectively these emerging technologies are integrated and regulated.

Delgado-Mohatar *et al*, are of the view that both blockchain technology and biometrics could potentially complement each other to foster innovation, enhance security measures, and optimize operational efficiency within an increasingly digital world which each other for improved intellectual property protection.[99] Blockchain technology could use both biometrics to create highly protected identities for creators. Through this approach, only legitimate owners can easily assert and defend their intellectual property rights thereby improving security levels.

[97] S Salem *et al* (2023). Blockchain-based biometric identity management. Cluster Computing. 27. 1-12. 10.1007/s10586-023-04180-x.

[98] S Shi and others 'Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey' (2020) 97 *Comput Secur*. doi: 10.1016/j.cose.2020.101966 (Accessed 18 July 2024); P Thantharate & A Thantharate 'ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain' (2023) 7 *Big Data and Cognitive Computing* 165 https://doi.org/10.3390/bdcc7040165. (Accessed 28 July 2024).

[99] O Delgado-Mohatar *et al* 'Blockchain and biometrics: A first look into opportunities and challenges' *Advances in intelligent systems and computing* 169–177 https://doi.org/10.1007/978-3-030-23813-1_21 (Accessed 28 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

7. Recommendations

The identity management field on the blockchain is undergoing a radical shift, with innovative startups and established firms in this sphere at the forefront of this development. Top blockchain development companies, such as SoluLab, are equipped to help guide subscribers through the intricacies involved in developing blockchain-based solutions. To truly maximise the potential of the technology, one should hire blockchain developers with many years of experience.

In addition, the close relation of biometrics to identity proofing in many domains means that they may play a significant role in future concepts related to identity management. One burgeoning area, early in its development, is the standardisation of identity throughout different blockchain systems: Decentralised Identity Documents.[100] The creation of standard units of identification, which is likely to accelerate as communities pursue the one strategy in earnest, will be determined by this. Another important but lesser-seen integration area where blockchain and biometric technology can evolve together is the implementation of secure, user-friendly, scalable identity management solutions. But as this technology continues to develop, we need to confront its challenges and harness its advantages for better national and international security infrastructures.

8. Conclusion

Ultimately, blockchain and biometric technologies can make a lasting impact on the field of intellectual property rights management as well as data protection. But doing so requires navigating the attendant legal and ethical challenges, surmounting technical barriers to interoperability, and enacting a collaborative governance framework across all stakeholders. Balancing innovation and fundamental rights will hopefully allow society to take advantage of new technologies in creating a safer, more efficient and inclusive digital world. This promise of blockchain and biometric innovation to have far-reaching implications across industries is still some way from realisation, though. In the interim period much more development work will be required alongside robust regulatory frameworks that enable the ethical sharing of these

[100] A Johnson-Ubah 'A beginner's guide to decentralized identifiers (DIDs)' (2023) *Medium* https://medium.com/veramo/a-beginners-guide-to-decentralized-identifiers-dids-5e842398e82c (Accessed 28 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

extraordinary new sources of data. This balanced approach is essential to embrace the benefits of technological advancements without neglecting their civil liberties and privacy.

However, the collection, storage, and processing of biometric data also raise significant privacy concerns, as this information can be highly sensitive and personal. Regulatory bodies, such as the NITDA have sought to address these challenges by establishing guidelines and safeguards for the use of blockchain[101] and biometric data, striking a balance between the benefits of biometric technologies and the need to protect individual privacy.[102]

References

A Ross and others 'Information fusion in biometrics' (2003) 24 *Pattern Recognition Letters* 2115–2125. https://doi.org/10.1016/s0167-8655(03)00079-5 (Accessed 8 July 2024).
A Chapman *Blockchain the Autodidact's Toolkit. A* (2023) 3.
A Damodaran 'Royalty payments on intellectual property: A preliminary analysis of the principal policy issues facing India' (2017) *Social Science Research Network* https://doi.org/10.2139/ssrn.3100144 (Accessed 28 June 2024).
A Jain 'An introduction to biometric recognition' (2004) 14 *IEEE Transactions on Circuits and Systems for Video Technology* 4–20 https://doi.org/10.1109/tcsvt.2003.818349. (Accessed 30 June 2024).
A Savelyev 'Copyright in the blockchain era: Promises and challenges' (2018) 34 *Computer Law & Security Review* 550-561.
AA Gikay 'Regulating use by law enforcement authorities of live facial recognition technology in public spaces: An incremental approach' (2023) 82 *The Cambridge Law Journal* 414-449.l doi:10.1017/S0008197323000454 (Accessed 30 June 2024).
AT Sherman and others 'On the Origins and Variations of Blockchain Technologies Cyber Defense Lab' (2018) 1810.06130 (arxiv.org) (Accessed 15 June 2024).
C Fontesl 'AI-powered public surveillance systems: why we (might) need them and how we want them' (2022) 71 *Technology in Society* https://doi.org/10.1016/j.techsoc.2022.102137. (Accessed 4 July 2024).
C Tankard 'What the GDPR means for businesses' (2016) *Network Security* 5 https://doi.org/10.1016/s1353-4858(16)30056-3 (Accessed 15 July 2024)
CN Saha & S Bhattacharya 'Intellectual property rights: An overview and implications in the pharmaceutical industry' (2011) 2 *J Adv Pharm Technol Res*. 88-93. doi:10.4103/2231-4040.82952 (Accessed 26 June 2024).
D Dadhich 'Preventing Digital and Intellectual Property Piracy: A Global Perspective' Preventing Digital and Intellectual Property Piracy: A Global Perspective | by Dhanraj Dadhich | Medium (Accessed 29 June 2024).

[101] National Blockchain Policy for Nigeria 2023 https://nitda.gov.ng/wp-content/uploads/2023/05/National-Blockchain-Policy.pdf (Accessed 28 July 2024).
[102] N Whiskerd and others 'A Requirement Analysis for Privacy-Preserving Biometrics given Universal Human Rights and Data Protection Regulation' 1 September 2018, https://doi.org/10.23919/eusipco.2018.8553045 (Accessed 28 July 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

D Petrovska-Delacrétaz *et al Guide to Biometric Reference Systems and Performance Evaluation* (Springer-Verlag London Ltd 2009).
DL Chaum, 'Computer systems established, maintained, and trusted by mutually suspicious groups' Electronics Research Laboratory, University of California, Berkeley, UCB/ERL M79/10 1979 computer-systems-by-mutually-suspicious-groups.pdf (nakamotoinstitute.org) (Accessed 15 June 2024).
Dwork & Moni, 'Pricing via processing or combatting junk mail' in Brickell (ed) *Advances in Cryptology: Proceedings of Crypto* 92 (1993) 139-147.
G Gürkaynak and others 'Intellectual Property Law and Practice in the Blockchain Realm' (2018) 34 *Computer Law & Security Review* 847-862.
GE 'Blockchain's Practical and Legal Implications for Global Trade and Global Trade Law' in MBurri (ed) *Big Data and Global Trade Law* (2021) 128-159; Chapman (n 24).
H Biswas and others 'Smart city development: Theft handling of public vehicles using image analysis and cloud network' in *Elsevier eBooks* (2021) 155–169 https://doi.org/10.1016/b978-0-12-822844-9.00013-x. (Accessed 4 July 2024).
H Taherdoost 'Smart contracts in blockchain technology: A critical review' (2023) 14 *Information* 117 https://doi.org/10.3390/info14020117 (Accessed 28 June 2024).
JA Unar and others 'A review of biometric technology along with trends and prospects' (2014) 47 *Pattern recognition* 2673-2688.
JB Mazumdar 'Retina based biometric authentication system: A review' (2018) 9 *International Journal of Advanced Research in Computer Science* 711–718 https://doi.org/10.26483/ijarcs.v9i1.5322. (Accessed 4 July 2024).
JD McCabe 'Security and privacy architecture' in *Elsevier eBooks* (2007) 359–383 https://doi.org/10.1016/b978-012370480-1/50010-4 (Accessed 15 July 2024).
K Modi & L Devaraj 'Advancements in Biometric Technology with Artificial Intelligence' (2022) *Cornell University* https://doi.org/10.48550/arxiv.2212.13187. (Accessed 29 May 2024).
M Faundez-Zanuy 'Privacy issues on biometric systems' (2005) 20 *IEEE Aerospace and Electronic Systems Magazine* 13–15 https://doi.org/10.1109/maes.2005.1397143. (Accessed 8 July 2024).
M Finck & V Moscon 'Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management' (2019) 2.0. *IIC 50* 77–108 (2019) https://link.springer.com/article/10.1007/s40319-018-00776-8#citeas (Accessed 30 June 2024).
M Pilkington 'Blockchain technology: principles and applications' (2016) *Edward Elgar Publishing eBooks* https://doi.org/10.4337/9781784717766.00019. (Accessed 16 June 2024).
M Pilkington 'Blockchain technology: principles and applications' in *Edward Elgar Publishing eBooks* (2016) https://doi.org/10.4337/9781784717766.00019. (Accessed 16 June 2024).
MA Khan *et al* 'IoT security: Review, blockchain solutions, and open challenges' (2018) 82 *Future Generation Computer Systems* 395–411 https://doi.org/10.1016/j.future.2017.11.022. (Accessed 15 July 2024).
Maria del Coro *et al* 'Managing intellectual property rights in innovation: the key to reaching the market' *WIPO Magazine* March 2021, https://www.wipo.int/wipo_magazine/en/2021/01/article_0009.html (Accessed 29 May 2024).
Mohammad Saber Niazy, Nijad Ahmad, Zahra Habibi, Badam Niazi *Australian Journal of Engineering and Innovative Technology,* 2023.
N Ogbonna & N Booty 'Binance: Nigeria orders cryptocurrency firm to pay $10bn' https://www.bbc.co.uk/news/world-africa-68451238 (Accessed 15 June 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

NB Truong and others, 'GDPR-compliant personal data management: A blockchain-based solution' (2020) 15 *IEEE Transactions on Information Forensics and Security* 1746 https://doi.org/10.1109/tifs.2019.2948287 (Accessed 15 July 2024).
NK Ratha *et al* 'Enhancing security and privacy in biometrics-based authentication systems' (2001) 40 *IBM Systems Journal* 614–634 https://doi.org/10.1147/sj.403.0614 (Accessed 8 July 2024).
O Babalola 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12 *International Data Privacy Law* 44-52.
P Centobelli 'Blockchain technology for bridging trust, traceability and transparency in the circular supply chain' (2022) 59 *Information & Management* https://doi.org/10.1016/j.im.2021.103508. (Accessed 15 July 2024).
R J Baron 'Mechanisms of human facial recognition' (1981) 15 International *Journal of Man-machine Studies*, 137–178 https://doi.org/10.1016/s0020-7373(81)80001-6 (Accessed 4 July 2024).
RB Davis 'A gait analysis data collection and reduction technique' (1991) 10 *Human Movement Science* 575–587. https://doi.org/10.1016/0167-9457(91)90046-z (Accessed 4 July 2024).
RK Bera 'The Global Importance of Patents' (2009) 96 *Current Science Journal* https://www.jstor.org/stable/24104555 (Accessed 26 June 2024).
S Gardner 'Blockchain's forever memory confounds EU 'right to be forgotten' (2022) *Bloomberg Law*. https://news.bloomberglaw.com/privacy-and-data-security/businesses-adopting-blockchain-question-eus-strict-privacy-law. (Accessed 15 July 2024).
S Haber & WStornetta How to Timestamp a Digital Document' (1991) 3 *Journal of Cryptology* 99-111 https://link.springer.com/article/10.1007/BF00196791. (Accessed 15 June 2024).
S Nakamoto 'Bitcoin: A Peer-to-peer Electronic Cash System' (2008) https://bitcoin.org/bitcoin.pdf. (Accessed 14 May 2024).
S Nakamoto 'Bitcoin: A peer-to-peer electronic cash system' (2008) https://nakamotoinstitute.org/library/bitcoin/ https://bitcoin.org/bitcoin.pdf (Accessed 15 June 2024).
S Ramani and others 'Blockchain for digital rights management' in SK Hafizul Islam and others (eds) *Hybrid computational intelligence for pattern analysis, blockchain technology for emerging applications* (2022) 177-205.
S Saberi 'Blockchain technology and its relationships to sustainable supply chain management' (2018) 5 *International Journal of Production Research* 2117–2135 https://doi.org/10.1080/00207543.2018.1533261. (Accessed 8 July 2024).
S Wachter 'Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR' (2018) 34 *Computer Law & Security Review* 436 https://doi.org/10.1016/j.clsr.2018.02.002. (Accessed 8 July 2024).
S Yanushkevich 'Inverse biometrics: privacy, risks, and trust' in *Springer eBooks* (2021) 1–4 https://doi.org/10.1007/978-3-642-27739-9_1505-1 (Accessed 15 July 2024).
T Board 'Biometric Recognition: Challenges and Opportunities' (2010) https://www.amazon.com/Biometric-Recognition-Challenges-Opportunities-Cybersecurity/dp/0309142075. (Accessed 29 May 2024).
T Krajewski 'Blockchain and Intellectual property' (2019) *Social Science Research Network* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3316992 (Accessed 26 June 2024).

 https://doi.org/10.59568/KIULJ-2024-6-2-01

V Mann 'Development of voice recognition: Parallels with face recognition' (1979) 27 *Journal of Experimental Child Psychology* 153–165. https://doi.org/10.1016/0022-0965(79)90067-5 (Accessed 4 July 2024).
W Dai 'B-Money: An Anonymous and Decentralized Monetary System' https://nakamotoinstitute.org/library/b-money/ (Accessed 15 June 2024).
W. Diffie & ME Hellman 'New Directions in Cryptography' (1976) IT-22 *IEEE TRANSACTIONS ON INFORMATION THEORY* https://ee.stanford.edu/~hellman/publications/24.pdf. (Accessed 15 June 2024).
Z Zheng and Others, 'An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends' (2017) *IEEE international congress on big data (BigData congress)* 557-564.
Amey and others 'Blockchain & cryptocurrency' (2024) *Indian Scientific Journal Of Research In Engineering And Management* <doi: 10.55041/ijsrem30332>

 https://doi.org/10.59568/KIULJ-2024-6-2-01