AGORA International Journal of Juridical Sciences, http://univagora.ro/jour/index.php/aijjs
ISSN 1843-570X, E-ISSN 2067-7677
Vol. 19, No. 2 (2025), pp. 174-190

BLOCKCHAIN AND DATA PRIVACY IN NIGERIA: RECONCILING INNOVATION WITH THE NIGERIA DATA PROTECTION ACT 2023

R. F. MAHMOUD, E. YUSUF, M. OLOHUNGBEBE

Rilwan Mahmoud[1], Eeman Yusuf[2], Mamudat Olohungbebe[3]
[1] [2] [3] University of Ilorin, Nigeria
[1] https://orcid.org/0000-0002-1162-149X, E-mail: mahmoudesq@yahoo.com
[2] https://orcid.org/0009-0007-9466-9352, E-mail: yusufeeman2003@gmail.com
[3] https://orcid.org/0009-0004-4785-8933, E-mail: olohungbebe.mi@unilorin.edu.ng

Abstract*: The rapid adoption of digital technologies has amplified concerns over privacy and data protection, particularly in developing regions such as Africa. Nigeria's Data Protection Act (NDPA) 2023 provides a comprehensive framework for safeguarding personal data by stipulating lawful bases for processing, ensuring security, and establishing rights of data subjects. Meanwhile, blockchain technology has emerged as a prominent privacy-enhancing technology (PET), valued for its decentralization, immutability, and cryptographic security. However, blockchain's transparency and permanent storage of records raise tensions with confidentiality principles and rights such as erasure, central to both the NDPA and the EU General Data Protection Regulation (GDPR). This paper critically examines blockchain's compatibility with Nigeria's NDPA, assessing how features such as pseudonymization, decentralization, and replication align—or conflict—with statutory principles including lawfulness, fairness, data minimization, storage limitation, and accuracy. The study highlights blockchain's potential to reinforce data integrity and security while underscoring legal and practical challenges in reconciling its technical features with privacy rights.*

Keywords: *Data Protection, Blockchain, Privacy Regulation*

Introduction

The threat to the right to privacy is a universal one that transcends borders and regions, and as such, it will be erroneous to assume that some regions are immune to the effects of infringement of the right to privacy. Even in regions like Africa, where there is a misconception that the right to privacy is irrelevant, it must be noted that Africa, just like the rest of the world, encounters security and privacy challenges even if they differ in magnitude (Makulilo, 2024). Therefore, it is crucial to explore innovative solutions that prioritize privacy while harnessing the benefits of these technologies. The primary data protection regulation that governs every organization, person, or technology in Nigeria is the Nigeria Data Protection Act 2023 (NDPA). The Act provides the lawful basis for which personal data may be processed, states essential security measures and safeguards for the protection of personal data. The Act also defines the roles and obligations of data controllers and processors in ensuring adequate protection and privacy of data. Additionally, it establishes rights of data subjects which must be respected and upheld, amongst other provisions tailored towards the protection and privacy of personal data (Section 2, NDPA 2023). The growing reliance on the Internet in day-to-day activities has necessitated the development of privacy-enhancing technologies (PETs) such as blockchain-based technology to ensure the integrity and confidentiality of personal data (Melzi et al., 2024). Privacy-enhancing technologies refer to technologies that help implement fundamental principles of data protection and privacy. However, PETs are not completely foolproof, nor can they completely and effectively address all data privacy risks and threats. Blockchain helps to ensure data integrity; however, data confidentiality continues to be a primary concern (Henry et al., 2018). One of the features of blockchain technology is pseudonymization — a means by which personal identifiers of data are removed and replaced with random characters or artificial identifiers (pseudonyms), thus making the owner of the data unidentifiable. Meanwhile, as a result of the transparency of data and records, it becomes easy to trace transactions to a particular pseudonym and thereafter unmask the identity behind the pseudonym (Froomkin, 1999). This article examines the extent of blockchain's compliance with confidentiality and privacy rules as stipulated by data privacy regulations such as the Nigeria Data Protection Act (Section 2, NDPA 2023) and the EU General Data Protection Regulations (GDPR, 2016/679).

1. Primary Regulatory Frameworks on Data Protection in Nigeria

1.1. The Nigeria Data Protection Act (NDPA) 2023

The Nigeria Data Protection Act (NDPA) 2023 is the current and primary regulatory framework that governs the protection and privacy of data in Nigeria. The Act does not only apply where processing of data occurs in Nigeria, but it shall also apply where the data controller or data processor is domiciled in, resident in, or operating in Nigeria and where the data controller or data processor is not domiciled, resident, or operating in Nigeria but is processing data of a Nigerian data subject (Section 2, NDPA 2023; Article 1(4), NDPA GAID 2025). The Nigeria Data Protection Act, General Application and Implementation Directive (GAID) 2025 provides further explanation on the status of a data subject. The Directive states that the NDPA shall apply to any data subject within the territory of Nigeria, a data subject whose data has been transferred to or is in transit through Nigeria, and a Nigerian citizen not residing within the country (Article 4(4), NDPA GAID 2025). This position represents an advancement over the previous data protection law, the Nigeria Data Protection Regulation (NDPR) 2019, which provided that the regulation shall apply to Nigerians residents and non-residents. The Nigeria Data Protection Regulation (NDPR) 2019 and its Implementation Framework in 2020 were the first attempt at a comprehensive data protection and privacy law in Nigeria. In 2023, the Nigeria Data Protection Act (NDPA) was enacted, and it effectively repealed every provision of the NDPR that contradicted the Act, whilst making some additions to the provisions of the Regulation. However, upon the issuance of the Nigeria Data Protection Act, General Application, and Implementation Directive (GAID) 2025, the Nigeria Data Protection (NDPR) 2019, and by extension its Implementation Framework, ceased to be a data protection instrument in Nigeria (Article 4(2), NDPA GAID 2025). Therefore, the Nigeria Data Protection Act (NDPA) 2023 is the only primary legal instrument in Nigeria that regulates the protection and privacy of personal data. The Act was promulgated with the objective of promoting data processing practices that safeguard the security of personal data and the privacy of data subjects. Some other objectives include ensuring fair, lawful, and accountable processing of personal data, protecting the rights of data subjects as well as providing means of recourse and remedies in the event of the breach of the data subject's rights, amongst other objectives. In line with these objectives, the Act provides for lawful bases and data processing principles in that every data controller or processor must adhere to while processing data (Section 1, NDPA 2023). The Act also establishes the need to put in place adequate measures to ensure the security and confidentiality of data whilst outlining a number of security measures that can serve as guidelines (Sections 30–31, NDPA 2023). Moreover, the Act provides and protects the rights of data subjects whilst outlining compulsory guidelines for cross-border transfer of data, processing of sensitive data, and children's data, making it a comprehensive and encompassing data protection regulation (Section 49, NDPA 2023).

2. Secondary Regulatory Frameworks on Data Protection in Nigeria

2.1. The Cybercrimes Act 2015

The Cybercrimes (Prohibition, Prevention, etc.) Act is a statutory legislation enacted with the objective of prohibiting, preventing, detecting, and punishing cybercrimes. One of its other objectives includes the promotion of cybersecurity, protection of computer systems and networks, electronic communications, and privacy rights. This is evidenced in its penalization of offences that consist of elements of data privacy breaches, such as identity theft, impersonation, and breach of confidence by service providers (Section 1(c), Cybercrimes Act 2015; Sections 22(1–3), Cybercrimes Act 2015; Section 29, Cybercrimes Act 2015).

The Central Bank of Nigeria (CBN) Consumer Protection Regulations (2019)

The CBN Consumer Protection Regulations provide standards required of banks and other institutions offering financial services on the fair treatment of customers, business conduct, disclosure and transparency, protection of consumer rights, and accountability of the institutions. The purpose of this enactment is to enhance consumer confidence in the financial service sector and promote financial stability and growth (Introduction, CBN Consumer Protection Regulations, 2019; CBN Circular, 2019).

2.2. The Freedom of Information Act 2011

The Freedom of Information Act was enacted with the purpose of ensuring that public documents and records are protected, available, and freely accessible by the public. The Act was enacted in response to the growing demand for easy accessibility to public records and documents and accountability in Nigerian public institutions, and as such is not regarded as a data protection and privacy legal framework.

2.3. The National Health Act 2014

The National Health Act was enacted to create a framework to regulate, develop, and manage the national health system and set standards for rendering health services within the federation. Relevant provisions in the Act include the concept of informed consent, which obliges the healthcare provider to provide relevant and appropriate information to the client, in the language he understands and taking into consideration his level of literacy. The provisions of the Act also include the obligation on the healthcare provider to ensure confidentiality and protect against unauthorized access to patient records (Preamble, National Health Act 2014; Sections 23, 26, & 27, National Health Act 2014).

A blockchain is a permanent digital record (or ledger) that creates and stores transactions that are time-stamped and grouped in blocks linked to each other, as you would find in a chain. Each transaction entered into the blockchain database is authenticated by the consensus of every computer across the network collaborating in this verification process (Yaga et al., 2018; Dong et al., 2023). In other words, it is a chain of blocks that stores and enables the transmission of information. Each block contains a set of information and specific metadata of the block, known as the block header. The blocks are linked and protected through cryptography, validated, and maintained by a distributed network of peers, eliminating the need for a centralized intermediary. The metadata associated with each block includes its unique hash function and the hash function of the preceding block, establishing a sequential, secure and tamper-resistant arrangement of blocks. This process also ensures the authenticity and tamper-resistance of the information contained in the block. Thus, blockchain may be regarded as an endlessly growing chain of blocks that are interconnected and protected by cryptography (Cirone, 2021).

The underlying principle that guides the operation of blockchain technology is that once a transaction has been recorded by a network of distributed peers, it cannot be altered by anyone. When a transaction is made on the blockchain, it is authorized cryptographically through the verification of the digital signature of the person that initiated the transaction, which is based on asymmetric encryption, that is, a pair of public and private key unique to the person. A public-private key comprises two uniquely linked keys: a private key held securely by the owner and used to sign and verify transactions initiated, and the public key, which is openly accessible to identify the pseudonymous owner and authenticate transactions received by the nodes. The authorized transactions are validated and authenticated by the decentralized network of nodes that verify that the users have correctly cryptographically signed the transactions. Thereafter, a block that contains a record of the validated transaction is added to the chain of blocks and the newly created block is time-stamped and published on the blockchain network. The process of authentication and validation by the decentralized network is carried out through a consensus mechanism, which may be reached through various methods such as Proof-of-Work (Zheng et al., 2017), Proof-of-Stake (Yaga et al., 2018) or Proof-of-Authority (Yaga et al., 2018). In conjunction with its decentralized and consensus-based approach to validation and verification of transactions, blockchain technology also employs Merkle trees to ensure the integrity and tamper-resistance of the records of transactions. A Merkle tree is a cryptographic mechanism named after Ralph Merkle, utilized in blockchain technology to store records of blockchain data securely and efficiently (Merkle, 1988; Sáez, 2022). It is a tree-like data structure where each blockchain transaction is hashed in pairs and repeatedly recorded together until there is only one transaction hash left that has a record of all pairs that have been hashed together, known as the Merkle root or root hash. Similar to an actual tree, a Merkle tree consists of leaf nodes at the lowest level of the structure that represent the cryptographic hash of a single record or transaction, known as a child node (Bosamia, 2018). When two child nodes are paired together, they form a parent node that stores the combined hashes of the paired child nodes (Ayyalasomayajula & Ramkumar, 2023). The parent nodes are also paired repeatedly to form other parent nodes until only the Merkle root or root hash is left. An attempt to change any transactions affects the root hash signaling tampering of data. Thus, the Merkle tree plays an important role in verifying and ensuring the integrity of records of transactions on the blockchain (Peng et al., 2021; Chhabra et al., 2024). However, once data is committed to the Merkle tree, removing it without disrupting the structure becomes nearly impossible, conflicting with privacy principles such as the right to be forgotten.

3. Types of Blockchain

3.1. Public Blockchain

This is the earliest and the most common type of blockchain. It is a type of blockchain where anyone can participate in the network, and the records of the blockchain are made open for public verification. To participate in a public blockchain as a node or validator or as a user, no special permission or qualification is required, thus regarded as a permissionless blockchain. Similarly, in a public or permissionless blockchain, there is no central or single authority in charge of the persons that participate in the network. Every node in the network participates in the necessary computation to validate the block and a copy of this record is stored by every node with the end goal being the prevention of a single point of failure or arbitrary takeover of the network. Therefore, a public blockchain may be regarded as a decentralized blockchain that is open to anyone to participate, view and publish (Solat et al., 2021; Strehle, 2020). Public or permissionless blockchains promote transparency and openness, potentially conflicting with principles of data confidentiality. Nonetheless, public blockchains have become a popular choice in the financial sector, where transparency of actions and records are essential. However, in corporate establishments that require scalability, system responsiveness and ease of update, the implementation of public blockchain may not be adequate. For example, the most widely used public blockchain, Bitcoin, can handle only about 7–15 transactions per second and takes at least 10 minutes to confirm a block of transactions.

3.2. Private Blockchain

Private blockchain refers to a kind of blockchain where there are restrictions as to who can access and interact with the blockchain. To participate as a node in validating a transaction or as a user submitting a transaction, there is a need for permission and authorization. In a private blockchain, the blockchain systems are usually governed by an authority that grants access to interact with the blockchain to certain persons (Perera & Weinand, 2020). Just like in a typical blockchain, consensus must be reached before a transaction is validated in a private blockchain. Due to the restriction on the participating nodes, consensus requires less computational power or expensive resources; it is the identity of a node that is required to participate in the network and the authority given to the node may be revoked if it acts contrary to the authority granted. Moreover, it is only nodes that have been granted the authority to interact with the blockchain that can participate in the process of reaching a consensus. This is coupled with the authority to publish the records as well as the authority to view them. This implies that only nodes that have been authorized can record or publish a copy of the transactions and the published record can only be viewed by these selected nodes. However, in some other instances, a private blockchain may restrict access to use and interact with the blockchain, but not have restrictions as to who can view the record. Private blockchains are often employed in organizations and establishments, especially those that prioritize efficiency, accountability and privacy. Additionally, private blockchains may be employed in sectors that deal with sensitive data and as such, require the privacy of data in conjunction with the "immutability" of data offered by blockchain. Some arguments against private blockchain is that it is a form of centralization, as only a selected few are involved in the participation and validation process. Some other arguments state that since a private blockchain may require some kind of authority in order to operate, it is in contradiction with the reason for the evolution of blockchain, which is the elimination of third-party interference or authority. A noteworthy feature of private blockchain is the lack of openness of the transactional records, which may hinder the transparency of the actions of the nodes. Nonetheless, private blockchains offer more privacy than public blockchains due to the confidentiality and authorized access that they offer.

3.3. Consortium Blockchain

A consortium blockchain may be defined as the union of public and private blockchains. In a consortium blockchain, participation and consensus processes are limited to a distributed network of organizations. This is carried out by distributed peers in various organizations and not peers within an organization, like in the case of private blockchains (Chen et al., 2024; Dib et al., 2018). A notable feature of consortium blockchain is the ability of validators to alter previous blocks once there is an agreement between validators (Oladeji et al., 2025). Although in comparison to public and private blockchains, consortium blockchain offers more scalability and efficiency. Nonetheless, consortium blockchain still remains well in use, especially by organizations that have co-partners and is an attempt at a balance between private and public blockchain (Yao et al., 2021).

4. Features of Blockchain

Blockchain technology has certain attributes that are intrinsic to its operation. This part of this work shall examine these features and the extent to which these features can ensure the protection and privacy of data stored on the blockchain. These features include:

4.1. The use of cryptography

Cryptography can be defined as a process of concealing data or information, known as encryption, in order to ensure the integrity and confidentiality of such data in a manner that unauthorized persons will not be able to understand the meaning. Blockchain technology utilizes cryptographic measures such as hash functions, digital signatures, Merkle trees, and asymmetric encryption to ensure the security and integrity of data on the blockchain (Abdelrahman, 2022; Tiwari & Asawa, 2012). A hash function is a cryptographic mechanism whereby an original message, which is an input, is converted to a fixed-length output, known as the hash value, which is different from the original message. A good property of a hash function is that the hash value must be so random that it will be hard to decipher the original message or input (Mahmoud et al., 2020). In blockchain, the hash function uses the hash value of the preceding block to calculate the hash value of the new block; as such, the verification and validation of blocks can be done by comparing the hash values of the blocks. The Merkle tree is a cryptographic mechanism that uses the hash values of blocks to efficiently store and secure transaction records on a blockchain in a tree-like data structure (Bosamia, 2018; Ayyalasomayajula & Ramkumar, 2023). Asymmetric encryption, also known as public-private key, is a form of cryptography in which a user has access to a unique public key, which is public and used to verify transactions, and a unique private key, which is kept secret and used to authenticate transactions. Asymmetric encryption is relied upon by a user to create and authenticate a digital signature in order to release data to another party who verifies the hash value of the data received. Essentially, these cryptographic mechanisms are at the core of the operations of blockchain technology, which helps to ensure the security and integrity of data stored on the blockchain.

4.2. Decentralization

Blockchain technology emerged in order to remove the need for intermediaries or third parties, such as a central authority in the facilitation of transactions amongst parties. Instead of relying on a central authority, decision-making power is distributed across all network participants using consensus protocols. This implies that a new block can only be added to the existing chain of blocks after a consensus has been reached within the distributed network. The distributed nature of blockchain makes it harder for a singular bad actor to attempt to influence the consensus so as to take over the network. Thus, blockchain technology operates as a distributed structure where data is stored, shared and accessed in order to achieve decentralization. A decentralized technical structure reduces the risk of a single point attack or failure, data loss, data manipulation and other forms of data breach. Decentralization in blockchain technology is also reflected in the governance model (Mahmoud et al., 2019). Blockchains are governed through Decentralized Autonomous Organizations (DAOs), which comprise various entities that make decisions by voting through governance tokens. For a blockchain to be truly decentralized, the supply of governance tokens must not be concentrated in the hands of a few but must be distributed proportionally across all members of the DAO (Akram & Bross, 2018).

4.3. Transparency

The idea of blockchain is an open one, where transactions on the blockchain are made open and visible to everyone in the network. In the case of public blockchains, where anyone can join the network, the transactions carried out on the network are transparent, accessible and public. This helps to enhance the verifiability of transactions, as anyone can verify any transaction that took place on the blockchain and trace such a transaction to the public addresses that carried out the transaction. In the case of private blockchains, where there is a restriction on persons who can join and have access to the network, the transparency of transactions is limited to the persons who are in the network and have access to it (Zhang et al., 2019).

4.4. Pseudonymity

Pseudonymity is a state of being recognized by an identifier other than the real or actual name of the person. The users in a blockchain are not identified by their actual or original name; rather, they are identified by their unique public keys, which act as pseudonyms. Therefore, users on a blockchain can interact and carry out transactions without revealing their real identities. However, this is not to state that the real identity and activities of a user of a blockchain cannot be revealed. Although blockchain offers pseudonymity to users by way of public addresses, transactions may be linked to the public addresses since the transactions on the blockchain, which include the public address of the user who initiated the transaction, are made open and public. Thus, pseudonymity does not equal or grant full anonymity (Jain, 2022; Rahardja et al., 2021).

4.5. Immutability

Immutability is one of the well-known features of blockchain. It connotes that once a block is added to the chain of pre-existing blocks by a consensus reached by the distributed network of nodes, the transactions on the block cannot be changed or altered (Tripathi et al., 2023; Taufick, 2020). As a result of the use of cryptography, once a new block is added to the chain of existing blocks, it is time-stamped and a hash value is generated for it. An attempt to tamper with a block in the blockchain will lead to a change in the hash value of the block and even where such an actor further attempts to disguise by altering the hash values of all other previous blocks, it will be inconsistent with the genesis block (the first block to be created), thus making any alteration in a blockchain easily detectable. The purpose of immutability is to ensure that data and transactions stored on the blockchain cannot be altered or falsified, thus achieving data integrity and trust. However, this does not prevent the addition of new blocks that contain updates to the existing blocks. On the other hand, there are views that blockchains are not completely immutable, as changes to the blockchain may occur due to occurrences such as a 51% attack or a hard fork, although a very complicated process, but not an impossible one. A 51% attack is when an attacker gains over 50% of the control of the network and as such, can make decisions on the operations of the blockchain, including rewriting the blockchain. This will require over 50% computation power or over 50% of the total stake in a POW and POS system, respectively. Another means through which a blockchain can undergo changes is through forking, where changes are made to a blockchain protocol, which results in a split in the blockchain. These changes may be a slight upgrade in the blockchain in which the former and new protocol will be compatible and the end result is a single blockchain; this is known as a soft fork. However, where the changes are such that the previous and new protocols are no longer compatible and the split results in two different blockchains, it is known as a hard fork (Nakomoto, 2008; Mehar et al., 2017). Taking the possibilities of a 51% attack and the process of forking into consideration, blockchain technology cannot be said to be completely immutable. However, the complexity behind amending the records of a blockchain poses a challenge to privacy principles such as the right of erasure.

5. The Applicability and Sufficiency of the NDPA to Blockchain-Based Platforms in Nigeria

The NDPA regulates the collection, processing, and storage of personal data in Nigeria by Data Controllers. Consequently, the stakeholders and custodians of blockchain platforms are obligated to abide by the rules and principles as defined by the Act (Nigerian Data Protection Act, 2023). Since the operation of blockchain platforms involves the collection and transfer of data, this section examines the extent and sufficiency of the NDPA to blockchain-based platforms. The primary principles defined by the act are as follows:

5.1. Lawful Basis, Fairness and Transparency

The NDPA states that data can only be processed where there is a lawful basis and in accordance with the principle of fairness and transparency (Nigerian Data Protection Act, 2023). The principle of fairness means that data is processed in a way that is free from prejudice and exploitation and it is generally consistent with civil liberties in a democratic society (Nigerian Data Protection Act, 2023). The lawful basis for processing personal data includes consent, contractual necessity and other legal bases laid out in the Act (Nigerian Data Protection Act, 2023). Transparency in processing personal data may mean that data controllers are fully, clearly and explicitly open with data subjects with regard to the data being collected from the data subjects and the purpose for which the data is being collected. This principle subsists even where consent or contractual obligation is not the lawful basis for which personal data is being processed. One of the key features of most blockchains is decentralization, where the power to carry out any action on the blockchain is not subject to a centralized authority but vested in a vast majority of people. Therefore, blockchain technology strongly practices democracy in its operations and accordingly aligns with the principle of fairness in data processing (Finck, 2019). Also, blockchain technology strongly complies with the principle of transparency in data processing (Mougayar, 2016). In reality, blockchain technology suffers from an overwhelming amount of transparency, especially in public blockchains, where every action carried out by a user is publicly available. Although blockchain does not present a technological limitation to the adherence with the transparency principle, inadequate governance of the blockchain network could result in a lack of communication among participants in the network who play active roles in validating and broadcasting transactions, leading to non-compliance with the principle of transparency.

The lawful basis for the processing of personal data refers to the instances in which such processing of personal data may be allowed and considered legally acceptable (Nigerian Data Protection Act, 2023). This implies that processing of personal data in any other instance not stated in the Act shall be considered unacceptable and unlawful. The essence of having a lawful basis for processing personal data is to ensure that personal data is processed in a manner that upholds and respects the rights, freedoms, and interests of data subjects. Therefore, if no lawful basis for processing personal data is identified, the use and appropriateness of such blockchain technology may be reconsidered.

5.2. Purpose-Specification and Limitation

The Act also establishes the requirement of transparency by data controllers on handling personal data. It states that personal data must be collected for specified, explicit, and legitimate purposes, and there shall be no further processing of personal data in a way incompatible with the purpose for which it was collected (Nigerian Data Protection Act, 2023). This implies that a data controller must expressly declare legitimate intentions of the specific purposes for which the data is being collected and processed and must not go further to process such personal data in a manner that will be incompatible with the specific purpose for which it was originally collected. Most times, processing of personal data (public keys and transactional details that contain personal data) is not just limited to the original transaction. This conflicts with the principle of purpose specification, especially where the users are not informed of the further processing of personal data that has taken place. The principle of purpose specification is not completely incompatible with blockchain as users may be informed of the purposes for which the personal data is being processed (Finck, 2019). However, the principle of purpose limitation may be harder to comply with in the case of blockchains, where data may need to be continuously processed. In privacy-preserving blockchains where the data stored on the blockchain has either been anonymized or hashed and the personal data is stored offline in erasable ledgers, the principle of purpose limitation is significantly easier to comply with (Mougayar, 2016). This is due to the fact that the continuous processing that will occur on the blockchain does not include the processing of personal data.

5.3. Data Minimization

The Act provides that the processing of personal data must be adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed (Nigerian Data Protection Act, 2023). Adequacy means that the processing of personal data must be appropriate as to quality, quantity, and relevancy. This further implies that the processing of personal data must be materially useful in the fulfilment of the legitimate purpose for which the data was collected. The principle of data minimization provides that it is the least data necessary in fulfilment of the legitimate purpose for which the data was collected that should be collected or processed. Blockchain technology can be said to fulfil the principles of adequacy and relevance as the personal data collected are appropriate and materially useful in order to process personal data (Finck, 2019). On the other hand, the principle of data minimization may conflict with blockchain technology. As a decentralized structure, once a transaction is executed and a new block is added to the chain, a copy of the executed transaction is sent to all nodes in the network. This leads to a mass replication of personal data depending on how many nodes are in a particular blockchain network. This may conflict with the provisions of the Act, which states that only the least data necessary should be processed. The interpretation of the word “least” in this context may be used in terms of the quantity of data to be processed and as such, replication of personal data across many nodes may appear contrary to the provision. However, it should be noted that decentralization is a core aspect of blockchain technology, which is used to ensure the security and transparency of the network. Most users have regarded Bitcoin, a public blockchain with over 20,000 nodes, as the most secure blockchain ever as it has never been hacked and this has been largely attributed to the vast level of decentralization in the blockchain (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016). Therefore, the replication of transactions across all nodes should not conflict with the principle of data minimization because such an amount of data processing is required to fulfil one of the specific and legitimate purposes for which personal data is collected and processed: security.

5.4. Storage Limitation

The principle of storage limitation provides that personal data shall not be retained for longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed (Nigerian Data Protection Act, 2023). This implies that where the purpose for which personal data was collected or processed has been achieved, the data should be erased or deleted. This principle is in direct conflict with blockchain’s most favoured feature: immutability. Immutability on blockchain is to the effect that data stored on blockchain can never be erased or deleted. While this helps to ensure the transparency of transactions on the blockchain, it poses a risk to personal data, which has been identified in the earlier parts of this work to be included in the transaction on a blockchain. The principle of storage limitation only conflicts with immutable or append-only blockchains. For blockchains that store personal data in offline databases, such personal data can easily be deleted, thus adhering to the principle of storage limitation (Finck, 2019).

5.5. Accuracy

The Act states that the processing of personal data must be accurate, complete, not misleading, and, where necessary, kept up to date, having regard to the purposes for which the personal data is collected or is further processed (Nigerian Data Protection Act, 2023). The effect of this principle is that the state of personal data must be constantly updated in order to ensure personal data about to be processed is error-free and accurate. As previously stated, blockchains are immutable in nature as such, they cannot be altered or changed. Although the immutability of blockchains is in direct conflict with the principle of storage limitation and the right to erasure, it does not completely conflict with the principle of accuracy. More blocks can be added to the blockchain to show the updated status of the personal data. Also, when new blocks are formed once a transaction has been executed, the new block is timestamped. The timestamps on the blocks help to distinguish between a previous block of information and a newer block of information. The immutability of the blocks ensures that the updates to the blocks are not erased or deleted, thereby ensuring the accuracy of the personal data stored in the new block.

5.6. Security

The Act mandates that the processing of personal data must be in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing, access, loss, destruction, damage, or any form of data breach (Nigerian Data Protection Act, 2023). With the use of cryptography and distributed structures, blockchain technology ensures the security of personal data and prevents unauthorized access to it. Cryptographic measures such as the use of hash functions, Merkle trees, and asymmetric encryption enable blockchain to detect if a block has been tampered with or if unauthorized access has been granted. The distributed nodes across the network are responsible for checking whether the person who is initiating a transaction possesses the private and public keys to the data, which confirms if such a person is the original owner. The security principle is not incompatible with blockchain, as its architecture is built to ensure security and authorized access (Yaga, Mell, Roby, & Scarfone, 2018).

6. Rights of Data Subjects on Blockchain Platforms under the Nigerian Data Protection Act

The Nigeria Data Protection Act outlines the rights of data subjects regarding the collection, processing, and security of their personal data. These rights include the right to withdraw consent to process personal data, restrict data processing and portability, lodge a complaint with the commission, contest and terminate personal data processing, and to choose not to be subject to automated decision-making (Nigerian Data Protection Act, 2023).

Right to withdraw consent to process personal data

The NDPA provides a data subject with the right to withdraw their consent to the data controllers at any time to process personal data (Nigerian Data Protection Act, 2023). Additionally, consent given to the data controller to process personal data may not always be a sufficient basis for the processing of personal data, especially where the data controllers have not properly identified themselves on platforms like blockchain, where various actors can be involved in processing personal data.

6.1. Right to restrict data processing

A data subject has the right to restrict the processing of personal data by the data controller (Nigerian Data Protection Act, 2023). The right to restrict the processing of personal data is exercised where there is a pending resolution of a request, establishment of a legal claim, or objection to data processing by a data subject.

Right to lodge a complaint with the commission.

Under the NDPA, a data subject has the right to lodge a complaint with the Nigeria Data Protection Commission to seek redress of a violation of a right to privacy or a breach of personal data. The commission will acknowledge the receipt of the complaint within 7 days, after which the complaint shall be evaluated. Where an actual case of violation is discovered, an investigation will be launched, followed by a hearing to determine whether there has been a violation and the appropriate remedy for the data subject (Nigerian Data Protection Act, 2023).

6.2. Right to data portability

The right to data portability is the right of a data subject to request and receive personal data from a data controller in a machine-readable format and to have the personal data transferred from the data controller to another data controller, where possible. The right to data portability is qualified and can only be exercised where personal data is processed with a specific legal basis. The right will only be exercised where the legal basis for the processing of personal data is consent or for the performance of a contractual obligation. The right will not be applicable where personal data is processed with other legal bases such as public interest, legal obligation, vital interest, or legitimate interest (Nigerian Data Protection Act, 2023).

6.3. Right to contest and terminate personal data processing

A data subject has the right to object to the processing of personal data, in which the data controller must effectively discontinue the processing of personal data unless the data controller demonstrates a public interest or other legitimate grounds which override the fundamental rights and freedoms, and the interests of the data subject (Nigerian Data Protection Act, 2023). The consequence of this right is that unless a data controller can demonstrate grounds which override the rights of a data subject, the objection to data processing is a right guaranteed to a data subject which must be exercised.

6.4. Right to erasure of personal data

This is also known as the “Right to be forgotten.” A data subject may exercise the right to have their personal data erased, and the data controller must comply without undue delay (Nigerian Data Protection Act, 2023). A data subject may request the erasure of personal data where such personal data is no longer necessary to fulfill the purpose for which it was collected. Also, a data subject can only exercise the right of erasure where the legal basis for processing personal data is consent or legitimate interest.

6.5. Right to choose not to be subject to automated decision-making

The NDPA grants a data subject the right not to be subject to a decision based solely on automated processing of personal data, which may include profiling or any other action with similar legal consequences (Nigerian Data Protection Act, 2023). This right shall not be exercised where such automated decision has been authorized by a written law or consent of the data subject. The right will also not apply where the decision is necessary for entering into or for the performance of a contract between the data subject and a data controller. Similarly, the directive provides that data controllers who intend to deploy emerging technologies such as Artificial Intelligence, Internet of Things and Blockchain must take into consideration, amongst others, the right of a data subject not to be subject to automated decision making, whilst designing such technologies (Finck, 2019).

7. Implementational Challenges of Blockchain-Based Platforms

Despite the numerous benefits of blockchain technology in ensuring the transparency and privacy of transactions, it has certain limitations that may challenge its widespread adoption. These include:

- Scalability issues**:** Blockchain technology struggles with the scalability of large-scale transactions. Blockchain is designed to record all transactions carried out on it, and as transactions continue to increase, the blockchain becomes heavy, leading to a delay in transaction processing time. This could hinder its mainstream adoption, especially in organizations that process large-scale transactions and require fast processing (Dong, Abbas, & Kamruzzaman, 2023).
- Resource-intensive & Negative environmental impacts**:** Blockchain technology, particularly blockchains that employ the Proof-of-Work (POW) mechanism, requires a lot of computational power. POW blockchains create new blocks and publish blockchain records through mining, consuming a lot of electricity. This has been considered as one of blockchain’s most secure features, as the high cost of mining systems and the significant computational power required will deter malicious actors looking to take over the network. However, the substantial energy consumption during mining raises environmental concerns. Studies have revealed that blockchain mining has a negative impact on environmental sustainability (Stoll, Klaaßen, & Gallersdörfer, 2019).
- Complexity**:** Cryptography is one of the major components of blockchain technology, which is very unfamiliar to an average internet user. Users may encounter difficulty navigating complex cryptographic concepts like public-private key, smart contracts and managing a digital wallet, thereby enabling a wide knowledge gap which could hinder its widespread adoption (Narayanan et al., 2016).
- Security risks**:** Contrary to popular beliefs, blockchain technology is not completely free from cybersecurity attacks. While public blockchains allow for openness and transparency of transactions for the purpose of security, these may be exploited through cyberattacks like

Man-in-the-Middle (MITM) and Denial of Service (DoS) attacks. Blockchain technology is equally susceptible to malicious users (nodes) just like in centralized systems, especially in private or permissioned blockchains, which are less decentralized and transparent with transaction records (Zhang, Xue, & Liu, 2019).

- Regulatory concerns**:** The features of blockchain technology are distinct from existing traditional finance systems and, as such, have been stated to "challenge the boundaries of the legal orders in which they operate" (Cirone, 2021). Blockchain technology conflicts with existing regulations such as data protection laws, Know-Your-Customer (KYC) financial regulations, tax laws, and securities laws. Although attempts have been made to provide guidelines for the use of blockchain technology, there is yet to be a comprehensive legal framework. This poses complications for blockchain-based projects seeking widespread adoption.

Conclusions

The intersection of blockchain technology and Nigeria's Data Protection Act (NDPA) 2023 reveals both opportunities for innovation and challenges for compliance. Blockchain's immutability, decentralization, and cryptographic design provide strong safeguards for data security, integrity, and accountability, aligning with key NDPA objectives. Yet these same features generate tensions with data protection principles such as minimization, storage limitation, accuracy, and the right to erasure, raising difficult questions about how an immutable ledger can fully accommodate individual rights. To reconcile these tensions, Nigeria must adopt a balanced approach that neither stifles technological growth nor undermines privacy guarantees. This requires regulatory guidance from the Nigeria Data Protection Commission clarifying how NDPA provisions apply to blockchain use, as well as the development of technical solutions such as off-chain storage, encryption, and privacy-preserving cryptographic techniques. Permissioned or consortium blockchains may also offer more practical pathways for compliance in contexts involving sensitive personal data, while capacity building for regulators, legal practitioners, and developers is essential to ensure effective governance. In addition, aligning Nigeria's approach with international standards like the GDPR will strengthen cross-border compatibility and attract investment. Ultimately, the NDPA provides a strong framework for guiding blockchain adoption, but its effectiveness will depend on adaptive regulation, responsible technological design, and sustained commitment to protecting data subjects' rights in Nigeria's digital economy.

REFERENCES

Articles, Books, and Reports

1. Abdelrahman, M. (2022). Blockchain cryptography and security issues. *International Journal of Computer Science and Engineering Survey, 13.*
2. Akram, A., & Bross, P. (2018). Trust, privacy and transparency with blockchain technology and logistics. *Mediterranean Conference on Information Systems (MCIS).*
3. Ayyalasomayajula, P., & Ramkumar, M. (2023). Optimization of Merkle tree structures: A focus on subtree implementation. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC).*

4. Bosamia, M. (2018). Current trends and future implementation possibilities of the Merkle tree. *International Journal of Computer Sciences and Engineering.*
5. Chen, X., He, S., Sun, L., & Zheng, Y. (2024). A survey of consortium blockchain and its application. *Cryptography, 8(2).*
6. Chhabra, R., Saha, G., Kumar, G., & Kim, T. H. (2024). Navigating the maze: Exploring blockchain privacy and its information retrieval. *IEEE Access, 12,* 32089–32110.
7. Cirone, E. (2021). Blockchain and the General Data Protection Regulation: An irreconcilable regulatory approach? *Queen Mary Law Journal.*
8. Dib, O., Brousmiche, K., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. *International Journal on Advances in Telecommunications, 11.*
9. Dong, S., Abbas, K., & Kamruzzaman, J. (2023). Blockchain technology and application: An overview. *PeerJ Computer Science, 9,* e1563. https://doi.org/10.7717/peerj-cs.1563
10. Finck, M. (2019). *Blockchain regulation and governance in Europe.* Cambridge University Press.
11. Froomkin, M. A. (1999). The death of privacy. *Stanford Law Review, 52(5),* 1461–1543.
12. Henry, R., Herzberg, A., & Kate, A. (2018). Blockchain access privacy: Challenges and direction. *IEEE Security & Privacy, 16(4),* 38–45. https://doi.org/10.1109/MSP.2018.3111246
13. Jain, I. (2022). Blockchain technology and cryptography. *International Journal of Science and Research.*
14. Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In *Blockchain Technology* (pp. 349–371). Academic Press.
15. Kuznetsov, O., Rusnak, A., Yezhov, A., Kuznetsova, K., Kanonik, K., & Domin, O. (2024). Merkle trees in blockchain: A study of collision probability and security implications. *Internet of Things.*
16. Mahmoud, R. F, & Bellengere, A. H 'A social service? A case for accomplishing substituted service via WhatsApp in South Africa.' (2020) 137(3) The South African Law Journal 371, 374-375.
17. Mahmoud, R. F, Abdulazeez, H. O. & Wuraola, O. T. "An Assessment of the Legal Recognition and implementation of Electronic Evidence in the Tanzanian and Nigerian Legal Systems" (2019) The Public and International Law Journal, University of Abuja. 1(1).
18. Makulilo, A. B. (2024). Data privacy in Africa: Taking stock of its development after two decades. In *Data Privacy Law in Africa: Emerging Perspectives* (p. 45).
19. Mehar, M., Shier, S., Giambattista, A., Gong, E., Fletcher, G., Kim, H. M., & Laskowski, M. (2017). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *Journal of Cases on Information Technology, 21(1).*

20. Melzi, P., Rathgeb, C., Ruben, T. R., Rodriguez, V., & Busch, C. (2024). An overview of privacy-enhancing technologies in biometric recognition. *ACM Computing Surveys, 36,* 310.
21. Merkle, R. (1988). A digital signature based on a conventional encryption function. In C. Pomerance (Ed.), *Advances in Cryptology – CRYPTO '87* (Vol. 293). Lecture Notes in Computer Science.
22. Mohammed, A., & Varol, N. (2019). A review paper on cryptography. *7th International Symposium on Digital and Forensics and Security.*
23. Mougayar, W. (2016). *The business blockchain: Promise, practice, and the application of the next Internet technology*. Wiley.
24. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review.*
25. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.* Princeton University Press.
26. Oladeji, A. T., James, A., & Wilson, B. (2025). Interoperability challenges in blockchain solutions. *ResearchGate.*
27. Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., & Shimizu, S. (2021). Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks, 7(3),* 295–307.
28. Perera, S., & Weinand, R. (2020). Blockchain technology: Is it hype or real in the construction industry? *Journal of Industrial Information Integration.*
29. Rahardja, U., Hidayanto, N. A., Lutfiani, N., Febiani, D. A., & Aini, Q. (2021). Immutability of distributed hash model on blockchain node storage. *Scientific Journal of Informatics, 8.*
30. Raman, R. N. (2020). The persistence of blockchain technology using digital signature and hash function.
31. Sáez, H. de Ocáriz Borde. (2022). An overview of trees in blockchain technology: Merkle trees and Merkle Patricia tries. *ResearchGate.*
32. Saha, S., Poray, J., & Jana, B. (2019). A study on blockchain technology. *SSRN Electronic Journal.*
33. Solat, S., Calvez, P., & Naït-Abdesselam, F. (2021). Permissioned vs. permissionless blockchain: How and why there is only one right choice. *Journal of Software, 16(3).*
34. Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The carbon footprint of Bitcoin. *Joule, 3(7),* 1647–1661. https://doi.org/10.1016/j.joule.2019.05.012
35. Strehle, E. (2020). Public versus private blockchains. *Blockchain Research Labs Working Paper No. 14.*
36. Taufick, R. D. (2020). Blockchain: The fallacy of blockchain immutability and cartel governance. *Notre Dame Journal on Emerging Technologies.*
37. Tiwari, H., & Asawa, K. (2012). A secure and efficient cryptographic hash function based on NewFORK-256. *Egyptian Informatics Journal, 13(3).*
38. Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytics Journal, 9.*

39. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview (NISTIR 8202). *National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.IR.8202
40. Yao, W., Ye, J., Murimi, R., & Wang, G. (2021). A survey on consortium blockchain consensus mechanisms. *ResearchGate.*
41. Yu, R. F. (2019). *Blockchain technology and applications – From theory to practice.* Independently published.
42. Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys, 52(3),* 1–34. https://doi.org/10.1145/3316481
43. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE 6th International Congress on Big Data.*

Laws and Regulations

44. Central Bank of Nigeria (CBN). (2019, December 20). *Issuance of Consumer Protection Regulations* [Circular to all banks, other financial and non-bank financial institutions].
45. Central Bank of Nigeria (CBN). (2019). *Consumer Protection Regulations.*
46. Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (Nigeria).
47. National Health Act, 2014 (Nigeria).
48. Nigeria Data Protection Act, 2023 (Nigeria).