AKWA IBOM STATE BLOCKCHAIN AND DECOUPLED WEB3 SERVICES BILL, 2026

A BILL

FOR A LAW TO REGULATE THE GOVERNANCE, DEVELOPMENT AND RESPONSIBLE ADOPTION OF BLOCKCHAIN, DISTRIBUTED LEDGER TECHNOLOGY AND WEB3 SERVICES IN AKWA IBOM STATE; TO PROMOTE INNOVATION, SECURITY AND CONSUMER PROTECTION; AND FOR RELATED MATTERS.

Sponsor: Hon. (Engr.) Uduak-Obong Ekpo-Ufot

Co-Sponsors:

Rt. Hon. Kufreabasi Edidem

Rt. Hon. (Barr.) Otobong Bob

Rt. Hon Effiong Johnson

Hon. (Dr.) Nsidibe Akata

Hon Sampson Idiong

Hon. (Engr.) Udobia Udo

Hon Lawrence Udoide

Hon. Selina Isotuk Ukpatu

Hon Kenim Onofiok

Hon Precious Selong

Arrangement of Sections

PART I

Preliminary Provisions

1. Application and Scope
2. Relationship with Federal Law and Regulators
3. Objectives
4. Guiding Principles
5. Establishment of the State Blockchain and Web3 Council
6. Functions of the Council

PART II

State Registry For Smart Contract Developers And Web3 Operators

7. Establishment of the Registry
8. Mandatory Verification
9. Smart Contract Vulnerability Vetting
10. Registry Information
11. Public Register and Confidentiality
12. Change Notification
13. Suspension and Cancellation
14. Fees, Charges and Cost Recovery
15. No Blanket Licensing of Technology

PART III

Blockchain Integration In Public Infrastructure

16. Blockchain-Enabled Public Records

17. Digitisation of Land Titles

18. Prevention of Double Allocation and Unauthorised Alteration

19. Legal Effect of Blockchain Records

20. Other Public Infrastructure

21. Interoperability

22. Continuity and Recovery

23. Public-Sector Governance

PART IV

Consumer Protection And Anti-Scam Guardrails

24. Prohibition of Fraudulent Decentralised Schemes

25. Misleading Representations

26. Disclosure of Material Risks

27. Fraudulent Interfaces and Impersonation

28. Consumer Complaints

29. Judicial Redress and Asset Recovery

30. Freezing and Preservation Orders

31. Asset Tracing and Recovery

32. Protection of Legitimate Users

PART V

Responsible Digital Assets And Web3 Services

33. Federal Regulatory Status

34. Custody and Private Keys

35. Smart-Contract Upgrades

36. Decentralised Governance

37. Token and Digital-Asset Disclosures

38. Advertising and Promotion

39. Protection of Vulnerable Persons

40. Environmental and Infrastructure Considerations

41. Technological Neutrality

PART VI

Privacy, Cybersecurity And Technical Assurance

42. Data Protection

43. On-Chain and Off-Chain Data

44. Cybersecurity

45. Technical Audits

46. Serious Incident Reporting

47. Responsible Disclosure

48. Security Classification

PART VII

Innovation, Sandbox And Local Capacity

49. Blockchain and Web3 Regulatory Sandbox

50. Eligibility and Safeguards

51. Innovation and Research

52. Local Capacity and Jobs

53. Public-Private Partnerships

54. Certification

55. Annual Innovation Programme

PART VIII

Compliance, Enforcement, Appeals And Judicial Redress

56. Supervisory Powers

57. Compliance Notice

58. Administrative Sanctions

59. Offences and Penalties

60. Emergency Measures

61. Right to be Heard

62. Administrative Appeal

63. Judicial Review

64. Cooperation with Law-Enforcement

65. Digital Evidence

66. Protection Against Arbitrary Enforcement

PART IX

Financial Reporting And Miscellaneous Provisions

67. Fund and Financing

68. Accounts and Audit

69. Annual Report

70. Confidentiality

71. Regulations

72. Transitional Provisions

73. Review of the Law

74. Savings

75. Interpretation

76. Short Title

A LAW TO REGULATE THE GOVERNANCE, DEVELOPMENT AND RESPONSIBLE ADOPTION OF BLOCKCHAIN, DISTRIBUTED LEDGER TECHNOLOGY AND WEB3 SERVICES IN AKWA IBOM STATE; TO PROMOTE INNOVATION, SECURITY AND CONSUMER PROTECTION; AND FOR RELATED MATTERS.

BE IT ENACTED by the Akwa Ibom State House of Assembly as follows—

{Commencement }

PART I

PRELIMINARY PROVISIONS

1. Application and Scope

This Law applies, to the extent within the legislative and administrative competence of the State, to blockchain and distributed ledger technology systems, smart contract deployments, decentralised applications, digital asset and token-related services, and decoupled Web3 services developed, procured, operated, marketed, hosted or deployed in connection with activities within Akwa Ibom State. This Law shall not be construed as regulating matters reserved to the Federal Government or as replacing Federal licensing, monetary, securities, payments, taxation, telecommunications, data-protection or other regulatory regimes.

2. Relationship with Federal Law and Regulators

Nothing in this Law shall derogate from the Constitution of the Federal Republic of Nigeria or the powers of the National Assembly, the Central Bank of Nigeria, the Securities and Exchange Commission, the Nigeria Data Protection Commission, the National Information Technology Development Agency, the Nigerian Communications Commission, the Economic and Financial

Crimes Commission, the Nigeria Police Force, or any other competent Federal regulatory authority. Where an activity is subject to a Federal licence, approval, registration or prohibition, compliance with this Law shall not substitute for that Federal requirement.

3. Objectives

The objectives of this Law are to—

1. Promote responsible blockchain and Web3 innovation and investment
2. Protect residents and public institutions against fraud, scams and material technology risks
3. Support secure digital public infrastructure and trusted digital records
4. Promote transparent, auditable and resilient public-sector use of distributed ledgers
5. Encourage local talent, entrepreneurship, research and employment
6. Position Akwa Ibom State as a responsible hub for blockchain and Web3 innovation.

4. Guiding Principles

Implementation shall be guided by legality, technological neutrality, proportionality, consumer protection, transparency, accountability, privacy, cybersecurity, interoperability, accessibility, innovation, inclusion and respect for property and contractual rights.

5. Establishment of the State Blockchain and Web3 Council

There is established the Akwa Ibom State Blockchain and Web3 Council (AKSBWC), to coordinate policy, standards, innovation and regulatory functions under this Law, subject to applicable Federal law.

6. Functions of the Council

The Council shall—

(a) advise the Governor and House of Assembly on policy

(b) coordinate State blockchain standards and responsible adoption

(c) oversee the Registry and assurance framework

(d) coordinate public-sector blockchain projects

(e) administer the regulatory sandbox

(f) promote research, skills and local innovation

(g) develop model procurement and technical-assurance requirements

(h) monitor compliance

(i) coordinate referrals with Federal authorities

(j) publish an annual State Blockchain and Web3 Report

PART II

STATE REGISTRY FOR SMART CONTRACT DEVELOPERS AND WEB3 OPERATORS

7. Establishment of the Registry

There is established the Akwa Ibom State Registry for Smart Contract Developers and Web3 Operators, managed or administered by the State digital innovation agency under the supervision of the Council.

8. Mandatory Verification

Commercial Web3 operators and developers deploying an App, smart contract or Web3 service specifically targeting Akwa Ibom State residents may be required by regulation to register where the activity falls within State competence. Registration shall be proportionate to the nature and risk of the service and shall not constitute a licence for an activity requiring Federal authorisation.

9. Smart Contract Vulnerability Vetting

An operator required to register a high-impact or public-facing smart contract shall provide evidence of appropriate technical assurance, which may include independent code review, vulnerability assessment, penetration testing, audit reports and remediation records.

10. Registry Information

The Registry may record legal identity, responsible officers, service description, smart-contract addresses and versions where applicable, technical audit status, applicable Federal licences and other prescribed information.

11. Public Register and Confidentiality

The Council shall publish non-confidential registration information necessary to identify registered operators. Personal, security-sensitive, trade-secret and proprietary information shall be protected.

12. Change Notification

A registered operator shall notify the Registry of material changes to ownership, responsible officers, architecture, control mechanisms or service purpose within the prescribed period.

13. Suspension and Cancellation

The Council may suspend or cancel State registration for material breach, false information, refusal of remediation or serious continuing risk, subject to notice and an opportunity to be heard except in emergencies.

14. Fees, Charges and Cost Recovery

(1) The Council may, subject to regulations made under this Law, prescribe reasonable fees and charges for services provided under this Law, including—

(a) registration of Smart Contract Developers and Web3 Operators;

(b) renewal of registration;

(c) verification and technical assessment of smart contracts;

(d) independent smart-contract security audits;

(e) assessment of high-impact or public-facing decentralised applications;

(f) certification or accreditation of Web3 assurance, audit or testing providers;

(g) applications for participation in the Blockchain and Web3 Regulatory Sandbox;

(h) renewal, amendment or modification of a registration or certification;

(i) technical inspections or assessments undertaken at the request of an applicant; and

(j) any other regulatory or technical service reasonably provided under this Law.

(2) In prescribing fees under subsection (1), the Council shall ensure that the fees are—

(a) reasonable, transparent and proportionate to the service provided;

(b) primarily based on the reasonable cost of providing the relevant regulatory or technical service;

(c) proportionate to the nature, scale, complexity and risk of the blockchain or Web3 activity;

(d) structured to distinguish between small and large operators;

(e) periodically reviewed to take account of inflation, technological development and regulatory costs; and

(f) structured so as not to create an unreasonable barrier to innovation, investment or legitimate technological development in the State.

(3) The Council shall establish different fee categories having regard to the risk and nature of the activity, including—

(a) non-commercial or research activities;

(b) ordinary commercial Web3 services;

(c) high-impact Web3 services;

(d) smart-contract services involving financial or other material consumer risks;

(e) custodial or asset-handling services, where within State competence; and

(f) technical audit, verification and certification services.

(4) The Council shall prescribe reduced fees, deferred payment or fee waivers for eligible—

(a) start-ups;

(b) micro, small and medium-sized enterprises;

(c) early-stage technology companies;

(d) university spin-offs;

(e) locally developed blockchain and Web3 projects that satisfy prescribed criteria.

(5) No registration or regulatory fee shall be payable solely because a person—

(a) conducts academic or scientific research;

(b) develops open-source blockchain software for non-commercial purposes;

(c) develops or tests a smart contract in a controlled research environment;

(d) participates in a State-sponsored innovation programme; or

(e) develops a blockchain solution for a public-interest or humanitarian purpose.

(f) an exemption under this subsection shall not apply where the activity involves commercial deployment or the provision of regulated financial services.

(6) Participation in the State Blockchain and Web3 Regulatory Sandbox shall be free of charge for eligible start-ups, SMEs, academic institutions and public-interest projects.

(7) Where the Council requires an independent audit, penetration test, smart-contract review, cybersecurity assessment or other specialist technical evaluation, the cost shall ordinarily be borne by the applicant or operator.

The Council shall ensure that—

(a) the assessor is suitably qualified;

(b) the assessment fee is reasonable and transparent;

(c) the assessor has no material conflict of interest; and

(d) eligible SMEs and start-ups are not subjected to disproportionate costs.

(8) The Council may prescribe an annual regulatory fee for registered commercial Web3 operators whose activities present continuing regulatory, cybersecurity or consumer-protection risks. The annual fee shall take into account—

(a) the risk classification of the service;

(b) number of registered services;

(c) number of users;

(d) transaction volume, where relevant and lawfully measurable;

(e) technical complexity;

(f) whether the operator provides custodial or asset-handling services; and

(g) the size and financial capacity of the operator.

(9) Nothing in this Law shall require a person to pay a fee merely because that person—

(a) uses a blockchain wallet for personal purposes;

(b) holds or transfers a digital asset lawfully;

(c) uses a commercially available Web3 application;

(d) studies blockchain technology;

(e) develops open-source software for non-commercial purposes; or

(f) participates in blockchain research or education.

This is an important protection against over-regulation.

(10) The Council shall publish—

(a) all applicable fees;

(b) the basis upon which each fee is calculated;

(c) applicable exemptions and reductions;

(d) payment procedures;

(e) expected processing times; and

(f) procedures for requesting a waiver or review.

No fee shall be payable unless it has been properly prescribed and publicly published.

(11) The Council may waive, reduce or defer payment of a fee where it is satisfied that—

(a) the applicant is an eligible start-up or SME;

(b) the project has substantial public-interest value;

(c) the project is primarily research-oriented;

(d) the project is being undertaken by an educational institution;

(e) the project is part of an approved innovation programme; or

(f) payment would constitute an unreasonable barrier to legitimate innovation.

(12) Fees collected under this Law shall be accounted for in accordance with applicable public-finance laws. Subject to appropriation and applicable financial controls, funds may support—

(a) blockchain and Web3 regulatory supervision;

(b) cybersecurity infrastructure;

(c) smart-contract testing and technical assurance;

(d) regulatory sandbox activities;

(e) research and development;

(f) blockchain and Web3 skills development;

(g) public awareness and consumer education;

(h) development of technical standards; and

(i) other activities necessary to achieve the objectives of this Law.

(13) The Council shall review the fee structure at least once every three years and may recommend amendments having regard to—

(a) inflation;

(b) changes in technology;

(c) regulatory costs;

(d) the size and maturity of the Nigerian Web3 ecosystem;

(e) international regulatory practice; and

(f) the economic impact of fees on local businesses and innovation.

(14) Nothing in this section shall—

(a) replace a licence, registration or fee payable to a Federal authority;

(b) authorise the Council to impose a fee for a matter outside the legislative competence of the State; or

(c) prevent a person from being subject to fees or charges lawfully imposed by a competent Federal authority.

(d) proposed Schedule — Fees and Charges

No.	Service	Fee
1	Non-commercial/academic registration	Nil
2	Basic commercial Web3 registration	₦100,000
3	Commercial Web3 Operator registration	₦250,000
4	High-impact Web3 registration	₦500,000
5	Registration renewal	50% of applicable registration fee
6	Smart-contract vulnerability assessment	₦250,000–₦750,000
7	High-impact dApp assessment	₦500,000–₦1,500,000
8	Web3 assurance/audit-provider accreditation	₦500,000
9	Material amendment	₦100,000
10	Certificate issuance	₦100,000
11	Certificate replacement/amendment	₦50,000
12	SME/start-up sandbox participation	Nil
13	Academic/public-interest sandbox	Nil

No.	Service	Fee
14	Large-enterprise sandbox	Cost recovery
15	Independent technical assessment	Actual reasonable cost

15. No Blanket Licensing of Technology

Nothing in this Part requires registration merely because a person owns, studies, develops or uses open-source blockchain software for personal, academic or non-commercial purposes.

PART III

BLOCKCHAIN INTEGRATION IN PUBLIC INFRASTRUCTURE

16. Blockchain-Enabled Public Records

Subject to an Act of the National Assembly, the State may use permissioned blockchain or other DLT for public records where it provides measurable benefits in integrity, auditability, resilience, provenance or verification.

17. Digitisation of Land Titles

AKWAGIS, in coordination with competent land authorities, shall implement a permissioned distributed ledger to anchor, timestamp and archive records relating to Certificates of Occupancy and other land instruments. The ledger shall support, but shall not replace, the legal land registry, statutory approvals, survey requirements, conveyancing procedures or judicial processes applicable to land.

18. Prevention of Double Allocation and Unauthorised Alteration

Once an authorised land record has been verified and an integrity proof generated, an unauthorised alteration shall be flagged for investigation and shall have no legal effect unless validated through the designated statutory land-administration process. The system shall generate audit logs and alerts for suspected tampering, duplicate allocation or conflicting entries.

19. Legal Effect of Blockchain Records

A blockchain entry may constitute evidence of integrity and provenance to the extent prescribed by law, but shall not independently create, transfer, extinguish or determine a legal interest in land.

20. Other Public Infrastructure

The State may deploy Distributed Ledger Technology for procurement, certificates, grants, health or education credentials, public audit trails, agricultural provenance and other approved public-interest applications, subject to privacy and other applicable law.

21. Interoperability

Public blockchain systems shall, where reasonably practicable, use open standards and interoperable formats to reduce vendor lock-in.

22. Continuity and Recovery

Critical public blockchain systems shall maintain backup, key-recovery, disaster-recovery and continuity arrangements.

23. Public-Sector Governance

Every material State blockchain deployment shall have a designated MDA owner, documented purpose, security assessment, data-governance plan, continuity plan and responsible officer.

PART IV

CONSUMER PROTECTION AND ANTI-SCAM GUARDRAILS

24. Prohibition of Fraudulent Decentralised Schemes

A person who knowingly launches, promotes, operates or materially assists an unverified token, algorithmic yield pool, digital-asset investment structure, DeFi scheme or other Web3 arrangement for the purpose of defrauding or unlawfully obtaining property commits an offence under this Law, without prejudice to Federal law. Legitimate innovation shall not constitute an offence merely because it uses blockchain, tokens, smart contracts or decentralised architecture.

25. Misleading Representations

No operator shall knowingly make materially false or misleading representations concerning ownership, returns, reserves, security, audit status, regulatory approval, technology capability or risk.

26. Disclosure of Material Risks

A commercial Web3 service targeting consumers in the State shall provide clear disclosure of material risks, fees, contractual terms, withdrawal limitations, smart-contract risks and regulatory status, to the extent required by regulation and applicable Federal law.

27. Fraudulent Interfaces and Impersonation

A person shall not knowingly create or distribute a deceptive website, wallet interface, smart contract, digital identity, token or communication designed to impersonate a legitimate Web3 operator or public institution for fraudulent purposes.

28. Consumer Complaints

The Council shall establish a mechanism for complaints concerning Web3 services within its jurisdiction and refer matters falling under Federal jurisdiction to the appropriate authority.

29. Judicial Redress and Asset Recovery

The High Court of Akwa Ibom State may, in proceedings properly brought before it and subject to the Constitution, issue appropriate orders concerning identifiable digital assets, wallets, accounts, devices or other property connected to fraud or unlawful conduct.

Nothing in this section confers jurisdiction where such jurisdiction is reserved to a Federal court or authority.

30. Freezing and Preservation Orders

Upon sufficient evidence and in accordance with applicable procedural law, a court may order preservation or temporary restraint of identifiable digital assets or hardware infrastructure connected to an alleged offence pending investigation or determination. Orders shall be specific, proportionate and subject to review.

31. Asset Tracing and Recovery

The State may cooperate with law-enforcement, financial-intelligence, cybersecurity and Federal authorities to trace, preserve and recover proceeds of unlawful Web3 activities.

32. Protection of Legitimate Users

No digital asset shall be arbitrarily frozen, seized or confiscated without lawful authority, due process and an identifiable connection to alleged unlawful conduct.

PART V

RESPONSIBLE DIGITAL ASSET AND WEB3 SERVICES

33. Federal Regulatory Status

A person offering a digital-asset, securities, payment, exchange, custody or other regulated financial service shall obtain required Federal licences or approvals. State registration or sandbox participation shall not be represented as Federal approval.

34. Custody and Private Keys

Where a service involves custody or control of customer assets, the operator shall maintain appropriate security, access-control, recovery and incident-response measures, subject to Federal regulation.

35. Smart-Contract Upgrades

Where a smart contract may be upgraded, the operator shall disclose the existence and scope of upgrade authority and maintain appropriate governance and security controls.

36. Decentralised Governance

Where material decisions use decentralised governance, the operator shall provide accessible information on governance rules, voting rights, conflicts of interest and emergency powers.

37. Token and Digital-Asset Disclosures

Where required by law, issuers or promoters targeting State consumers shall provide information on purpose, rights, risks, supply, governance, dependencies and technical architecture.

38. Advertising and Promotion

Advertising shall be truthful, not materially misleading and compliant with applicable consumer-protection and Federal financial-sector requirements.

39. Protection of Vulnerable Persons

Safeguards may be prescribed for services likely to be used by minors, elderly persons or other vulnerable consumers.

40. Environmental and Infrastructure Considerations

The Council may issue guidance promoting energy efficiency, responsible infrastructure use and environmental reporting where material.

41. Technological Neutrality

Nothing in this Law shall require a particular blockchain, consensus mechanism, token standard, wallet, cloud provider or architecture unless necessary to meet a lawful security, interoperability or public-interest requirement.

PART VI

PRIVACY, CYBERSECURITY AND TECHNICAL ASSURANCE

42. Data Protection

Processing of personal data through blockchain or Web3 services shall comply with the Nigeria Data Protection Act, 2023 and applicable requirements.

43. On-Chain and Off-Chain Data

Where personal data is involved, operators shall assess whether immutable on-chain storage is appropriate and, where practicable, avoid unnecessary personal data on public or immutable ledgers.

44. Cybersecurity

High-impact Web3 services and State blockchain systems shall implement proportionate controls including secure key management, access control, vulnerability management, logging, incident response, backup and recovery.

45. Technical Audits

The Council may require independent technical audits for State systems or registered high-impact services where necessary to assess security, resilience or consumer risk.

46. Serious Incident Reporting

An operator shall notify the Council of a serious security incident, exploit, unauthorised compromise or material loss of customer or public assets within seventy-two hours of becoming aware of it, subject to Federal reporting requirements.

47. Responsible Disclosure

The Council shall encourage responsible vulnerability disclosure and may establish a coordinated vulnerability-disclosure framework for State blockchain systems.

48. Security Classification

Critical State blockchain infrastructure shall be subject to enhanced security, access-control, continuity and independent-assurance requirements.

PART VII

INNOVATION, SANDBOX AND LOCAL CAPACITY

49. Blockchain and Web3 Regulatory Sandbox

The Council shall establish a controlled sandbox for testing innovative blockchain and Web3 services under defined conditions, duration, user limits and safeguards.

50. Eligibility and Safeguards

Applicants shall demonstrate a legitimate use case, responsible operator, risk assessment, cybersecurity controls and consumer safeguards. The Council may limit transaction value, users, geography, duration or functionality.

51. Innovation and Research

The State may support university-industry research, incubation, grants, technical training, hackathons, open-source projects and other lawful innovation programmes.

52. Local Capacity and Jobs

The Council shall promote local blockchain engineering, cybersecurity, smart-contract auditing, legal, compliance and product-design capabilities.

53. Public-Private Partnerships

The State may enter lawful partnerships with technology companies, universities, financial institutions and other organisations for blockchain infrastructure, research and innovation.

54. Certification

The Council shall establish voluntary technical or responsible-Web3 certification schemes. Certification shall not be represented as a financial or Federal regulatory licence.

55. Annual Innovation Programme

The Council shall publish an annual programme identifying priority blockchain and Web3 challenges in public administration, agriculture, education, health, land administration, commerce and other sectors.

PART VIII

COMPLIANCE, ENFORCEMENT, APPEALS AND JUDICIAL REDRESS

56. Supervisory Powers

The Council may request relevant information, conduct audits, require remediation, inspect State-funded systems and refer matters outside its competence to the appropriate Federal authority.

57. Compliance Notice

Where the Council reasonably believes that an operator is in breach, it may issue a written notice specifying the breach, corrective measures and reasonable compliance period.

58. Administrative Sanctions

The Council shall impose proportionate administrative measures including warning, remediation, suspension or cancellation of State registration or certification, and administrative monetary penalties.

59. Offences and Penalties

A person who knowingly commits an offence under sections 26, 27, 29 or another provision designated by this Law commits an offence.

(1) A person who contravenes a provision of this Law for which no specific penalty is prescribed commits an offence and is liable on conviction—

(a) in the case of an individual, to a fine not exceeding **₦5,000,000** or confinement for a term not exceeding **two years**, or to both

(b) in the case of a body corporate, to a fine not exceeding **₦20,000,000**

(2) A person who knowingly or recklessly—

(a) operates a Web3 service required to be registered under this Law without such registration

(b) submits materially false or misleading information to the Council or the Registry

(c) deliberately conceals a material security vulnerability, exploit or incident affecting users or public infrastructure

(d) falsely represents that a State registration, certification, sandbox admission or approval constitutes a licence or approval from a Federal regulatory authority

(e) knowingly breaches a compliance or suspension order issued under this Law,

commits an offence and is liable on conviction—

(i) in the case of an individual, to a fine of not less than ₦5,000,000 and not exceeding ₦20,000,000, or confinement for a term not exceeding three years, or to both

(ii) in the case of a body corporate, to a fine of not less than ₦20,000,000 and not exceeding ₦50,000,000.

(3) A person who knowingly engages in conduct prohibited under section 26, 27 or 29 of this Law for the purpose of deceiving, defrauding or unlawfully obtaining money, digital assets or other property from another person commits an offence and is liable on conviction—

(a) in the case of an individual, to a fine of not less than ₦10,000,000 or an amount equivalent to three times the value of the benefit obtained or loss avoided, whichever is greater, or confinement for a term of not less than three years and not exceeding seven years, or to both

(b) in the case of a body corporate, to a fine of not less than ₦50,000,000 or three times the value of the benefit obtained or loss avoided, whichever is greater.

(4) Where an offence under subsection (3) involves—

(a) fraud against ten or more persons

(b) an amount exceeding ₦100,000,000

(c) a vulnerable person or persons

(d) deliberate use of a smart contract, decentralised application or digital asset structure to conceal or facilitate the fraud

(e) money laundering, terrorist financing or other serious organised crime

(f) repeated commission of an offence under this Law,

the offender is liable on conviction to—

(i) in the case of an individual, imprisonment for a term of five to ten years, or a fine of not less than ₦50,000,000 or three times the value of the benefit obtained or loss avoided, whichever is greater, or to both

(ii) in the case of a body corporate, a fine of not less than ₦100,000,000 or three times the value of the benefit obtained or loss avoided, whichever is greater.

(5) Where an offence under this Law is a continuing offence, the Council may impose an administrative penalty of up to ₦500,000 for each day during which the contravention continues after the person has been served with a valid compliance notice, subject to regulations made under this Law.

(6) In addition to any fine or imprisonment imposed under this section, the Court may, subject to applicable law—

(a) order restitution or compensation to victims

(b) order the forfeiture of proceeds, property, digital assets, wallets, devices or other instrumentalities connected with the offence

(c) order the closure, suspension or restriction of the offending Web3 service

(d) prohibit the offender from operating a Web3 service within the jurisdiction of the State for a specified period

(e) make any other order necessary to prevent continuing harm or protect affected persons.

(7) Where an offence is committed by a body corporate, any director, manager, partner, beneficial owner or senior officer who knowingly authorised, permitted, participated in or facilitated the commission of the offence also commits the offence and is liable to the applicable penalty, unless that person proves that the offence occurred without their knowledge, consent or connivance and that they exercised reasonable diligence to prevent its commission.

(8) In determining an appropriate administrative or criminal penalty, regard shall be had to—

(a) the nature, seriousness and duration of the violation

(b) the number of persons affected

(c) the financial or other harm caused

(d) whether the conduct was intentional, reckless or negligent

(e) the amount of benefit obtained or loss avoided

(f) whether the offender voluntarily reported the violation

(g) the extent of cooperation with an investigation

(h) steps taken to remedy the violation and compensate victims

(i) previous violations or compliance history

(j) whether the offender is an individual, small enterprise or large commercial operator.

(9) Nothing in this section shall prevent the prosecution of an offence under any applicable Federal law where the conduct also constitutes an offence under that law.

60. Emergency Measures

Where a Web3 service presents an imminent and serious risk of fraud, material loss, public-infrastructure compromise or other unlawful harm, the Council may issue a temporary suspension or restriction order within its lawful jurisdiction, subject to prompt review.

61. Right to be Heard

Before a final adverse decision, the affected person shall receive notice of the proposed action and reasonable opportunity to make representations, except where immediate interim action is necessary to prevent serious harm.

62. Administrative Appeal

A person dissatisfied with a final Council decision may appeal to an independent Appeals Committee designated by the Council within fourteen business days or such longer period as may be allowed for good cause.

63. Judicial Review

Nothing in this Law shall oust or limit the jurisdiction of a competent court or a person's right to judicial review or other lawful remedy.

64. Cooperation with Law-Enforcement

The Council shall cooperate with the Nigeria Police Force, EFCC, relevant Federal regulators, cybersecurity authorities and other competent agencies in investigating offences and securing digital evidence.

65. Digital Evidence

Records, logs, transaction histories, cryptographic proofs and other reliable digital evidence obtained lawfully may be relied upon in proceedings in accordance with the Evidence Act.

66. Protection Against Arbitrary Enforcement

Enforcement shall be proportionate, evidence-based, technology-neutral and subject to due process. No person shall be penalised merely for using open-source blockchain technology or engaging in a lawful technological or commercial activity.

PART IX

FINANCIAL, REPORTING AND MISCELLANEOUS PROVISIONS

67. Fund and Financing

The Council's activities may be funded through appropriations, lawful grants and donations, prescribed fees and other lawful receipts.

68. Accounts and Audit

The Council shall keep proper accounts and ensure annual audit in accordance with applicable State public-finance and audit laws.

69. Annual Report

The Council shall submit an annual report to the Governor and House of Assembly covering registration, public infrastructure projects, incidents, enforcement, sandbox activities, innovation programmes, finances and recommendations.

70. Confidentiality

Members, officers, consultants and persons acting for the Council shall protect confidential information obtained in official duties and disclose it only as authorised by law.

71. Regulations

The Council may, subject to required approval, make regulations concerning registration, technical audits, risk classification, smart-contract assurance, consumer disclosures, incident reporting, sandbox administration, fees, enforcement procedures and other implementation matters.

72. Transitional Provisions

Affected State systems and operators lawfully existing at commencement shall be given a reasonable period to comply, except where immediate measures are required to prevent serious harm.

73. Review of the Law

The Council shall review this Law not later than three years after commencement and every three years thereafter, considering technology, Federal policy, regulatory experience, innovation, economic impact and consumer protection.

74. Savings

Nothing in this Law shall invalidate or affect any approval, licence, contract, intellectual property right, obligation, offence, penalty or liability created under the Act of the National Assembly.

75. Interpretation

'blockchain' means a distributed ledger in which records are cryptographically linked or otherwise secured against unauthorised alteration;

'distributed ledger technology' or 'DLT' means technology enabling records to be synchronised, shared and maintained across participants;

'smart contract' means software deployed on blockchain or DLT that automatically executes programmed actions;

'Web3 service' means a digital service using decentralised, distributed or user-controlled technologies;

'decoupled Web3 service' means a Web3 service whose interface, data, application logic, identity, storage or other components may operate independently or across multiple providers or protocols rather than depending on a single centralised intermediary;

'digital asset' means a digital representation of value, rights or interests capable of electronic transfer, subject to applicable Federal law;

'decentralised application' or 'dApp' means an application using distributed or decentralised infrastructure;

'operator' includes a developer, provider, deployer or service provider;

'Registry' means the State Registry established under section 9; and

'Council' means the Akwa Ibom State Blockchain and Web3 Council established under this Law.

76. Short Title

This Law may be cited as the Akwa Ibom State Blockchain and Decoupled Web3 Services Law, 2026.