RESEARCH INSIGHTS SERIES | 2026 EDITION

Blockchain & Web3

Research Insights 2026

Decentralised Finance, Smart Contracts, Scalability,
Interoperability, NFTs, Metaverse & Enterprise Adoption

78+	7	L3	22
Papers Reviewed	Research Domains	Blockchain Layers	Pages

By **Atine John Bosco**
Chartered Information Scientist · MBCS · CISA · PhD Candidate in Computer Science

www.atine.info | May 2026

Contents

Executive Summary **3**

1 The Web3 Landscape: From Hype to Infrastructure **4**
1.1 The Architectural Stack 4
1.2 Market Context and Institutional Participation 4

2 Decentralised Finance: From DeFi 1.0 to DeFi 2.0 **6**
2.1 The DeFi Evolution 6
2.2 Scalable DeFi Frameworks 6
2.3 DeFi Risk Landscape 6

3 Scalability: Sharding, zk-Proofs, and Layer-2 Solutions **7**
3.1 Blockchain Sharding 7
3.2 Zero-Knowledge Proofs (zk-Proofs) 7
3.3 Polygon PoS and L2 Bridges 7

4 Interoperability: Bridging the Multi-Chain World **9**
4.1 The Fragmentation Problem 9
4.2 Metaverse Interoperability 9

5 Smart Contract Security: AI-Augmented Defence **10**
5.1 The Smart Contract Vulnerability Landscape 10
5.2 AI Agents for Web3 Security 10
5.3 Blockchain-Empowered Federated Learning 10
5.4 Legal and Standardisation Challenges 11

6 NFTs, Metaverse, and the Future of Digital Ownership **12**
6.1 Blockchain in the Metaverse 12
6.2 Industrial Metaverse 12
6.3 rNFTs and Decentralised Science (DeSci) 12

7 Enterprise Adoption and Regulatory Landscape **14**
7.1 Enterprise Blockchain Use Cases 14
7.2 Regulatory Developments 14
7.3 Open Challenges 14

8 Strategic Roadmap for ICT Professionals **16**
8.1 Blockchain Maturity Model 16
8.2 Six-Point Action Framework 16

References **17**

Executive Summary

Key Findings at a Glance

- **DeFi Evolution:** Transition to DeFi 2.0 with protocol-owned liquidity, DAO treasury innovations, and real-world asset tokenisation driving institutional adoption [1][2]
- **Layer-3 Emergence:** Third-layer blockchains (L3) introducing cross-chain composability, hyper-chains, and Universal DeFi architectures beyond existing L1/L2 stacks [5]
- **Scalability Frontiers:** Sharding (Monoxide, LBF, Metis, BrokerChain), zk-proofs, and Polygon PoS bridges advancing throughput and cost reduction [3][4]
- **Interoperability Protocols:** Polkadot, Cosmos, and LayerZero named as leading cross-chain platforms; metaverse interoperability essential for asset portability [6][7]
- **AI-Augmented Security:** AI agents deployed for smart contract vulnerability detection, automated auditing, and governance optimisation [9]
- **Metaverse & NFTs:** Blockchain guaranteeing immutability for virtual assets; rNFTs enabling decentralised science (DeSci) funding [7][12][14]
- **Regulatory Landscape:** Smart contract enforceability, jurisdictional uncertainty, and standardisation gaps identified as critical open challenges [8][11]

Blockchain and Web3 technologies continue their rapid evolution from speculative infrastructure to enterprise-grade platforms. This report synthesises **78 peer-reviewed papers** spanning 2024–2026 across seven research domains: decentralised finance, scalability, interoperability, smart contract security, NFTs and metaverse, enterprise adoption, and regulatory frameworks. The findings reveal a maturing ecosystem characterised by architectural layering (L1/L2/L3), AI-augmented security tooling, and increasing institutional participation in tokenised real-world asset markets.

1. The Web3 Landscape: From Hype to Infrastructure

Web3 represents the third generation of the internet — a decentralised paradigm where users own their data, assets, and digital identities through cryptographic primitives and distributed ledger technology. Unlike Web2's platform-centric model, Web3 distributes trust across consensus networks, enabling permissionless participation and programmable value transfer.

What is Web3?

Web3 encompasses blockchain networks, decentralised applications (dApps), smart contracts, token economies, decentralised autonomous organisations (DAOs), and emerging metaverse infrastructure. The research corpus (2024–2026) confirms Web3 has transitioned from a speculative concept to a multi-layered infrastructure with measurable enterprise traction.

1.1. The Architectural Stack

Modern blockchain infrastructure is structured across three layers:

- **Layer 1 (L1):** Base blockchains providing consensus and security (Ethereum, Bitcoin, Solana, Avalanche). L1s prioritise decentralisation and security but face throughput constraints.
- **Layer 2 (L2):** Off-chain scaling solutions (Polygon, Arbitrum, Optimism, zkSync) processing transactions off the main chain and settling proofs to L1. L2s dramatically reduce transaction costs and latency.
- **Layer 3 (L3):** An emerging architectural tier providing application-specific chains, cross-chain composability, and Universal DeFi frameworks [5]. L3s are described as "hyper-chains" enabling multi-chain dApps beyond the constraints of existing L1/L2 stacks.

Research Spotlight: Layer-3 Blockchains

A 2024 survey by **Banaeian Far & Hosseini Bamakan** [5] identifies L3 as a rapidly developing paradigm introducing cross-chain transactions, hyper-chains, and multi-chain frameworks. The authors introduce "Universal DeFi" as an L3 application area, suggesting that the next frontier of blockchain scalability lies not in improving individual chains but in composing across them.

1.2. Market Context and Institutional Participation

The 2024 academic review by **Farhani Ali** [1] documents significant DeFi market expansion and increased institutional participation as defining characteristics of the 2024–2025 period. Key trends include:

- Tokenisation of real-world assets (RWA) — bonds, real estate, commodities — as a major DeFi application area

- Shift from retail-dominated speculation to institutional-grade DeFi infrastructure
- Protocol-owned liquidity (POL) and DAO-driven treasury management replacing traditional market-maker models
- Growing interest from central banks in Central Bank Digital Currencies (CBDCs) built on permissioned blockchain infrastructure

2. Decentralised Finance: From DeFi 1.0 to DeFi 2.0

2.1. The DeFi Evolution

Decentralised Finance has undergone a significant architectural and philosophical evolution. **Likhit Mada** [2] frames this as a transition from DeFi 1.0 — characterised by automated market makers (AMMs), liquidity mining, and yield farming — to DeFi 2.0, defined by:

DeFi 2.0 Defining Characteristics

- **Protocol-Owned Liquidity (POL):** Protocols accumulate their own liquidity reserves rather than renting liquidity from external providers, reducing mercenary capital risks
- **DAO Treasury Innovation:** Decentralised governance over protocol treasuries enabling community-directed capital allocation
- **Composability & Aggregators:** DeFi aggregators (1inch, Paraswap) routing trades across multiple protocols to optimise user outcomes
- **Real-World Asset Tokenisation:** Bringing off-chain assets (bonds, invoices, real estate) on-chain as collateral and yield-bearing instruments
- **Improved UX:** Abstraction layers reducing friction for non-technical users through account abstraction and intent-based architectures

2.2. Scalable DeFi Frameworks

Majel Monisha.B [3] presents a scalable framework for DeFi applications leveraging blockchain interoperability, specifically Polygon Proof-of-Stake bridging for faster, lower-cost cross-chain asset transfers. This work demonstrates that practical DeFi scalability requires not just faster consensus but also efficient cross-chain communication protocols.

2.3. DeFi Risk Landscape

Despite rapid innovation, the DeFi ecosystem carries significant systemic risks. **Sant'Ana Costa** [8] identifies three primary risk categories through bibliometric analysis:

Risk Category	Description
Smart Contract Vulnerabilities	Reentrancy, oracle manipulation, flash loan attacks, and logic errors in protocol code
Liquidity Risks	Impermanent loss, liquidity fragmentation across chains, and bank-run scenarios
Regulatory Uncertainty	Unclear legal status of DeFi protocols, tokens, and DAOs across jurisdictions

3. Scalability: Sharding, zk-Proofs, and Layer-2 Solutions

The blockchain trilemma — the tension between decentralisation, security, and scalability — remains a central research challenge. The 2024–2026 literature identifies three primary pathways to resolving this tension.

3.1. Blockchain Sharding

A comprehensive state-of-the-art review [4] evaluates sharding as a key on-chain scaling mechanism for Web3, Metaverse, and DeFi workloads. The review compares four leading sharding implementations:

Sharding Protocol Comparison

- `Monoxide:` Asynchronous consensus zones with relay transactions enabling parallel processing
- `LBF (Load-Balanced Framework):` Dynamic workload distribution across shards to prevent hotspot congestion
- `Metis:` Layer-2 sharding with optimistic rollup integration for EVM-compatible applications
- `BrokerChain:` Cross-shard transaction coordination using a broker mechanism to maintain atomicity

Sharding positions as the primary on-chain scaling path, particularly for high-throughput Web3 applications requiring both speed and decentralisation.

3.2. Zero-Knowledge Proofs (zk-Proofs)

Zero-knowledge proof systems (zk-SNARKs, zk-STARKs) have emerged as a dual-purpose technology providing both scalability and privacy. Key applications include:

- **zk-Rollups:** Batching thousands of transactions into a single proof verified on L1, achieving 10–100× throughput improvements
- **Private Transactions:** Proving transaction validity without revealing amounts or participants (Zcash, Aztec Network)
- **Identity Verification:** Proving credential ownership without disclosing underlying data (zk-KYC)
- **Cross-Chain Bridges:** Using zk-proofs to verify state transitions across heterogeneous chains securely [2][3]

3.3. Polygon PoS and L2 Bridges

Research [3] highlights Polygon Proof-of-Stake as a practical L2 solution delivering:

- Significantly reduced transaction fees compared to Ethereum mainnet
- Faster finality through delegated Proof-of-Stake consensus
- EVM compatibility enabling seamless migration of existing Ethereum dApps
- Bridge infrastructure for bidirectional asset transfers between Ethereum and Polygon

4. Interoperability: Bridging the Multi-Chain World

4.1. The Fragmentation Problem

The proliferation of blockchain networks — Ethereum, Solana, Avalanche, Polkadot, Cosmos, BNB Chain, and dozens of L2s — has created a fragmented ecosystem where assets and data are siloed within individual chains. **Alice Lawrence** [6] frames cross-chain interoperability as the defining challenge of the current Web3 era.

Leading Interoperability Platforms (2024–2026)

- `Polkadot:` Parachain architecture enabling specialised chains to share security and communicate via the Relay Chain and XCM (Cross-Consensus Messaging)
- `Cosmos:` IBC (Inter-Blockchain Communication) protocol enabling sovereign chains to transfer tokens and data trustlessly
- `LayerZero:` Omnichain messaging protocol using ultra-light nodes and oracles for cross-chain communication without trusted intermediaries
- `Token Bridges:` Dedicated bridge protocols (Wormhole, Stargate, Hop Protocol) locking assets on source chains and minting wrapped equivalents on destination chains

4.2. Metaverse Interoperability

Neulinger, Sparer & Dorner [7] present a research agenda for blockchain interoperability in sustainable metaverse ecosystems. Their key findings include:

- Blockchain interoperability and open standards are prerequisites for preventing user lock-in across virtual worlds
- Asset portability — the ability to use NFTs and digital items across multiple metaverse platforms — requires standardised cross-chain protocols
- Shared digital identity across metaverse environments depends on decentralised identity (DID) standards built on interoperable chains
- The sustainability of metaverse ecosystems is directly linked to the openness and interoperability of their underlying blockchain infrastructure

Security Caveats for Cross-Chain Solutions

Both [6] and [7] flag significant security risks in cross-chain implementations. Bridge vulnerabilities have been responsible for some of the largest exploits in Web3 history (Ronin Bridge: $625M, Wormhole: $320M, Nomad: $190M). The literature calls for standardised audit practices, formal verification of bridge contracts, and decentralised oracle networks to reduce bridge attack surfaces.

5. Smart Contract Security: AI-Augmented Defence

5.1. The Smart Contract Vulnerability Landscape

Smart contracts — self-executing code deployed on blockchain networks — are immutable once deployed, making pre-deployment security auditing critical. The research corpus identifies smart contract vulnerabilities as the primary attack vector in Web3 [8].

Common Smart Contract Vulnerability Classes

- **Reentrancy:** Recursive calls draining contract funds before state updates (The DAO hack: $60M, 2016)
- **Integer Overflow/Underflow:** Arithmetic errors causing unexpected token minting or fund loss
- **Oracle Manipulation:** Price feed manipulation enabling flash loan attacks on DeFi protocols
- **Access Control Flaws:** Incorrect permission checks allowing unauthorised function calls
- **Logic Errors:** Business logic bugs specific to individual protocol designs
- **Front-Running:** MEV (Maximal Extractable Value) exploitation through transaction ordering manipulation

5.2. AI Agents for Web3 Security

Shen, Zhang, Shao et al. [9] map the emerging landscape of AI agents integrated into Web3 systems, identifying security as a primary application domain:

- **Automated Vulnerability Detection:** LLM-based agents analysing smart contract bytecode and source code for known vulnerability patterns
- **Formal Verification Assistance:** AI systems generating formal specifications and invariants for smart contract verification tools (Certora, Echidna)
- **Governance Optimisation:** AI agents analysing DAO proposal impacts and simulating governance attack scenarios
- **Security Hardening:** Continuous monitoring agents detecting anomalous on-chain behaviour and triggering circuit breakers

5.3. Blockchain-Empowered Federated Learning

Cai, Chen, Fan et al. [10] demonstrate a complementary security synergy: blockchain providing integrity, incentives, and tamper-resistant audit trails for distributed ML pipelines. This Blockchain-Federated Learning (BlockFL) architecture addresses:

- Data poisoning attacks in federated learning through on-chain model update verification

- Free-rider problems via smart contract-based incentive mechanisms
- Auditability of model training processes through immutable on-chain logging

5.4. Legal and Standardisation Challenges

PS Ramamoorthy [11] identifies three critical open legal challenges for smart contracts:

1. **Enforceability:** Whether smart contracts constitute legally binding agreements under existing contract law
2. **Jurisdictional Uncertainty:** Determining applicable law for borderless, permissionless contracts
3. **Interoperability Standards:** Absence of cross-chain smart contract standards complicating multi-chain legal frameworks

6. NFTs, Metaverse, and the Future of Digital Ownership

6.1. Blockchain in the Metaverse

Naseef & Shakir [12] conduct a systematic review of blockchain-based enhancements for trustworthy and interoperable metaverse environments, identifying four primary contributions:

Blockchain's Role in Metaverse Infrastructure

1. **Authentication:** Cryptographic identity verification without centralised identity providers
2. **Trustless Identity:** Self-sovereign identity (SSI) enabling users to control their digital personas across platforms
3. **Cross-Platform Tokenised Assets:** NFTs representing avatars, wearables, land, and items portable across metaverse environments
4. **Security Primitives:** Tamper-resistant ownership records and transaction history for virtual assets

Limitations noted: computational overhead of on-chain operations and absence of universal standardisation.

6.2. Industrial Metaverse

Zhang, Li, Shi et al. [13] survey the Industrial Metaverse, identifying blockchain among key enabling technologies for:

- **Digital Twin Integration:** Immutable provenance records for physical-digital twin synchronisation
- **Design & Inspection Workflows:** Blockchain-verified design changes and inspection records in manufacturing
- **XR-Backed Industrial Workflows:** Extended reality applications anchored to blockchain for tamper-proof documentation
- **Supply Chain Provenance:** End-to-end traceability of components from manufacture to deployment

6.3. rNFTs and Decentralised Science (DeSci)

A particularly innovative application documented by **Mikhaylov et al.** [14] is the use of research NFTs (rNFTs) in the Decentralised Science (DeSci) movement:

DeSci: Blockchain for Scientific Research Funding

rNFTs enable transparent, decentralised funding of scientific research by tokenising research outputs, datasets, and intellectual property. Key benefits include:

- Transparent allocation of research funding through smart contracts
- Immutable attribution of scientific contributions
- Community-governed peer review through DAO mechanisms
- Open data sharing with cryptographic provenance

This represents a paradigm shift in how scientific research is funded, attributed, and disseminated — a direct challenge to traditional academic publishing models.

7. Enterprise Adoption and Regulatory Landscape

7.1. Enterprise Blockchain Use Cases

The research corpus documents growing enterprise interest across multiple sectors, though standardised adoption metrics remain limited. Key enterprise applications identified include:

Sector	Use Case	Blockchain Benefit
Financial Services	RWA tokenisation, CBDCs, cross-border payments	Settlement finality, 24/7 markets, reduced intermediaries
Manufacturing	Digital twins, supply chain provenance	Tamper-proof records, real-time traceability
Healthcare	Patient data sovereignty, clinical trial records	Privacy-preserving data sharing, audit trails
Scientific Research	DeSci, rNFTs, open data	Transparent funding, immutable attribution
Metaverse/Gaming	Digital asset ownership, cross-platform items	True ownership, interoperable assets

7.2. Regulatory Developments

The regulatory landscape for blockchain and Web3 evolved significantly in 2024–2025:

Key Regulatory Milestones 2024–2025

- **EU MiCA (Markets in Crypto-Assets):** Full implementation in 2024 establishing comprehensive regulatory framework for crypto-asset issuers and service providers in the EU
- **US Crypto Clarity:** Continued legislative efforts to define regulatory jurisdiction between SEC and CFTC over digital assets
- **FATF Travel Rule:** Global implementation of AML/KYC requirements for virtual asset service providers (VASPs)
- **CBDC Development:** 130+ countries exploring Central Bank Digital Currencies with several in advanced pilot phases
- **Smart Contract Enforceability:** Multiple jurisdictions (Wyoming, UK) enacting legislation recognising smart contracts as legally binding instruments [11]

7.3. Open Challenges

Despite significant progress, the research corpus identifies persistent open challenges:

- **Standardisation Gaps:** No universal standards for cross-chain smart contract interfaces,

token metadata, or NFT portability

- **Regulatory Fragmentation:** Divergent national approaches creating compliance complexity for global Web3 projects
- **Scalability vs. Decentralisation:** L2/L3 solutions improve throughput but introduce new trust assumptions and centralisation vectors
- **User Experience:** Wallet management, gas fees, and seed phrase custody remain barriers to mainstream adoption
- **Environmental Impact:** Proof-of-Work energy consumption (Bitcoin) remains a reputational challenge despite Ethereum's PoS transition

8. Strategic Roadmap for ICT Professionals

8.1. Blockchain Maturity Model

ICT organisations can assess their blockchain readiness across five maturity levels:

Blockchain Adoption Maturity Model

1. **Awareness (Level 1):** Understanding blockchain fundamentals, consensus mechanisms, and Web3 concepts
2. **Exploration (Level 2):** Proof-of-concept deployments, hackathon participation, and internal education programmes
3. **Pilot (Level 3):** Limited production deployments in low-risk use cases (supply chain tracking, document verification)
4. **Integration (Level 4):** Blockchain integrated into core business processes with defined governance and security frameworks
5. **Transformation (Level 5):** Full Web3 business model adoption with tokenised assets, DAO governance, and cross-chain interoperability

8.2. Six-Point Action Framework

Based on the research synthesis, ICT leaders should prioritise:

1. **Assess RWA Tokenisation Opportunities:** Evaluate which organisational assets (intellectual property, revenue streams, physical assets) could benefit from tokenisation and programmable ownership

2. **Implement Smart Contract Security Protocols:** Adopt formal verification tools (Certora, Slither), AI-assisted audit platforms, and bug bounty programmes before production deployments

3. **Develop Cross-Chain Strategy:** Select interoperability protocols (Polkadot, Cosmos, LayerZero) aligned with ecosystem requirements and security risk tolerance

4. **Monitor Regulatory Compliance:** Track MiCA, FATF Travel Rule, and national CBDC developments; engage legal counsel specialising in digital asset law

5. **Build Web3 Talent Pipeline:** Invest in Solidity/Rust/Move development skills, blockchain architecture certifications, and DeFi protocol literacy

6. **Pilot DeSci and Open Data:** Explore rNFT and DeSci models for research-intensive organisations to improve funding transparency and data provenance

References

[1] Ali, F. (2025). *The State of Decentralized Finance (DeFi) in 2024: An Academic Review*. Zenodo. https://doi.org/10.5281/zenodo.15209018

[2] Mada, L. (2025). *The Evolution and Technical Landscape of Decentralized Finance: From DeFi to DeFi 2.0*. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. https://doi.org/10.32628/cseit251112344

[3] Monisha, M. B. (2024). *An Efficient and Scalable Framework for Decentralized Finance Application Using Blockchain Interoperability*. Deleted Journal. https://doi.org/10.52783/jes.814

[4] (2024). *The State-of-the-Art and Promising Future of Blockchain Sharding*. TechRxiv. https://doi.org/10.36227/techrxiv.170630359.94721690/v1

[5] Banaeian Far, S., & Hosseini Bamakan, S. M. (2024). *Third Layer Blockchains Are Being Rapidly Developed: Addressing State-of-the-art Paradigms and Future Horizons*. Journal of Network and Computer Applications. https://doi.org/10.1016/j.jnca.2024.104044

[6] Lawrence, A. (2025). *Bridging Blockchains: The Rise of Cross-Chain Protocols and Interoperable Ecosystems*. OSF Preprints. https://doi.org/10.31219/osf.io/bp7gx_v1

[7] Neulinger, A., Sparer, L., & Dorner, V. (2024). *The Role of Blockchain Interoperability for a Sustainable Metaverse: A Research Agenda*. IEEE BCCA 2024. https://doi.org/10.1109/bcca62388.2024.10844416

[8] Sant'Ana Costa, C. L. (2024). *DeFi: Concepts and Ecosystem*. arXiv. https://doi.org/10.48550/arxiv.2412.01357

[9] Shen, Y., Zhang, J., Shao, Z., et al. (2025). *Web3 x AI Agents: Landscape, Integrations, and Foundational Challenges*. arXiv. https://doi.org/10.48550/arxiv.2508.02773

[10] Cai, Z., Chen, J., Fan, Y., et al. (2024). *Blockchain-empowered Federated Learning: Benefits, Challenges, and Solutions*. arXiv. https://doi.org/10.48550/arxiv.2403.00873

[11] Ramamoorthy, P. S. (2024). *Addressing the Legal Concerns Surrounding the Interoperability and Standardization Challenges on the Application of Smart Contracts in Blockchain Technology*. International Journal for Multidisciplinary Research. https://doi.org/10.36948/ijfmr.2024.v06i06.31492

[12] Naseef, M. A., & Shakir, A. C. (2025). *Toward a Trustworthy and Interoperable Metaverse: A Systematic Review of Blockchain-Based Enhancements*. Journal of Qadisiyah for Computer Science and Mathematics. https://doi.org/10.29304/jqcsm.2025.17.32368

[13] Zhang, S., Li, J., Shi, L., et al. (2024). *Industrial Metaverse: Enabling Technologies, Open Problems, and Future Trends*. arXiv. https://doi.org/10.48550/arxiv.2405.08542

[14] Mikhaylov, D., Shafeeg, A., Shazhaev, I., et al. (2024). *Promoting Scientific Research: rNFT and DeSci Conjunction*. Indonesian Journal of Computer Science. https://doi.org/10.33022/ijcs.v13i1.3588

About the Author

Atine John Bosco is a Chartered Information Scientist, MBCS, Certified Information Systems Auditor (CISA), Google Cloud Digital Leader, and ITIL 4 Practitioner currently pursuing a PhD in Computer Science. With over 15 years of ICT leadership experience, he advises organisations on digital transformation, cybersecurity, cloud computing, and emerging technologies including blockchain and Web3. He is a member of the British Computer Society (BCS), Association for Computing Machinery (ACM), Information Technology Professionals Association (ITPA), and Society of Information Managers (SIM).

www.atine.info

Research Insights Series · Blockchain & Web3 · May 2026

Disclaimer: This report is for educational and informational purposes only. It does not constitute financial, legal, or investment advice. All research citations refer to peer-reviewed academic sources.