

# WEB3 FOR TRUSTED AI INFRASTRUCTURE

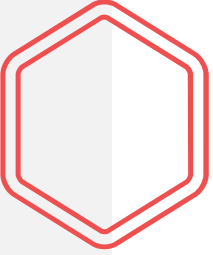


This paper was written with the contribution of  
Marie Sellier and Fabien Aufrechter

# TABLE OF CONTENTS

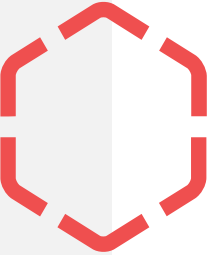
Introduction	03
Gen AI : Major Issues in 2025	04
Web3 Foundations :	05
Web3 & AI : Allowing Decentralization	06
Web3 & AI : Towards Protocolization	07
Web3 - AI integration: improved transparency, integrity and efficiency	08
Web3 & AI ; Use Cases	09
ZKP for AI Security, Privacy & IP Protection	10
ZKP for Data Sovereignty	11
Building Trustworthy AI Infrastructures	12
Conclusion	13
Sources	14

# INTRODUCTION




**The decentralized and transparent nature of blockchain** provides a secure environment for AI development. Blockchain's security features, including cryptographic protocols and consensus mechanisms, prevent unauthorized data alteration and ensure data integrity.... Blockchain also enables secure communication and data processing without relying on centralized servers.

Users regain **control and ownership of their data**. Web3 enables users to have more agency over their data, enhancing privacy and security.



**Smart contracts on the blockchain** can be audited, providing a high level of transparency. This is a significant shift from the "black box" nature of many current AI systems.

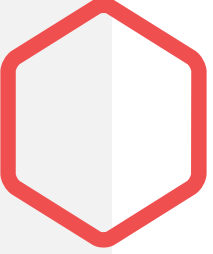
Blockchain enables the **monitoring of training data**, which is crucial for ensuring the integrity of AI models. Standards like C2PA can be used for traceability and verifiability of training data.



**On-chain data storage** allows for secure, verifiable records of data usage and model training. NFTs and smart contracts can be used to certify the origin of AI-generated content and facilitate revenue collection for creators. This helps address the current legal uncertainty about rights ownership.

**Zero-Knowledge Proofs** can be useful to prove that AI has not used specific datasets without revealing the data itself. This protects sensitive information and increases user confidence.

This white paper explores the application of Web3 technologies in AI security and compliance, focusing on:

- **Decentralized AI Data Provenance:** Ensuring training data traceability with blockchain-based verification protocols (C2PA, Ethereum smart contracts).
  - **Intellectual Property Protection:** Addressing copyright issues by enforcing NFT-based licensing and on-chain content authentication.
  - **Regulatory Compliance & AI Governance:** Aligning Web3 principles with laws such as the GDPR and the Ai Act.
  - **AI Security & Privacy:** Strengthening cyber resilience against AI-generated deepfakes, misinformation, and unauthorized model usage.
- 

# GEN AI : MAJOR ISSUES IN 2025

## AI Adoption and Growth

Since the rise of ChatGPT and other GenAI systems, adoption has accelerated across multiple industries. According to Omdia, the GenAI software market is projected to grow from \$6.2 billion in 2023 to \$58.5 billion by 2028 (CAGR: 56%).

## Concerns with Scaling AI Systems

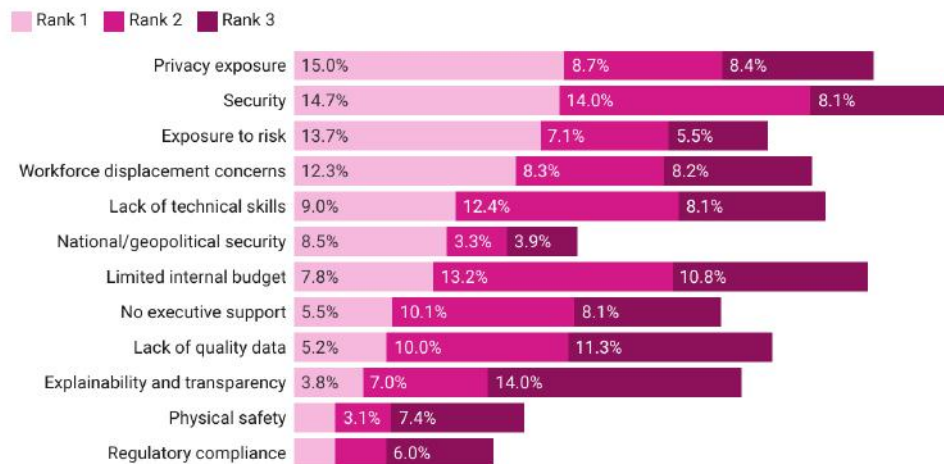
Despite rapid adoption, enterprises face major risks in scaling AI operations:

- Data Privacy & Security: AI systems process vast datasets, often lacking transparent user consent or regulatory compliance mechanisms.
- Legal Uncertainty: Copyright lawsuits (e.g. NYT v. OpenAI ) highlight unresolved issues regarding AI training data usage.
- Regulatory Compliance: The EU AI Act mandates strict traceability and risk assessments for AI models, creating compliance challenges for enterprises.

## Web3 as a Solution

Web3's decentralized security features—\*\*blockchain-based identity management, cryptographic data verification, and smart contract enforcement—\*\*offer an effective solution for securing AI systems and ensuring compliance.

## Which of the below do you perceive as the top three risks to AI within your organization today?



ICT Enterprise Insights 2023-24: n=1,625  
Source: Omdia • Created with Datawrapper

# WEB3 FOUNDATIONS

## Blockchain as a Trust Machine

Blockchain replaces centralized AI control structures with decentralized, immutable ledgers that verify data integrity, ensuring that AI models rely on authentic and verifiable training data.

This approach is fully aligned with the electronic ledger as defined in the eUIDAS 2.0 EU Regulation.

Hence, Blockchain is comparable to a "trust machine," representing a revolution in which trust is no longer placed in third parties but in a shared, decentralized system. This structure allows for information to be validated through "collective participation" rather than bilateral trust.

## Smart Contracts: Automated Compliance & Transactions

Smart contracts are self-executing programs on blockchain networks, ensuring: Automated AI licensing and data-sharing agreements. Tamper-proof compliance enforcement, reducing legal risks.

- On-chain record-keeping for AI-generated content.
- Unlike traditional AI infrastructures that require third-party trust, smart contracts provide autonomous, legally binding execution of AI-related transactions.

Smart contracts are computer programmes that automate the execution of contracts by applying tamper-proof rules that cannot be altered or traced. They operate on the blockchain, enabling transactions to be carried out securely and transparently without the need for a trusted intermediary.

Smart contracts are essential to blockchain technology, especially in converting cryptocurrency into a reliable framework for decentralized applications. Their code operates within a controlled environment, such as a virtual machine, ensuring that transactions are validated, verified, and recorded. Smart contracts allow for the definition of specific application rules for managing digital assets within a decentralized network.

Unlike Bitcoin transactions, which are uniform and solely focused on value transfer, smart contract transactions involve invoking functions defined within the contract's code. Decentralized applications leverage smart contracts to securely store and process information exchanges in a decentralized manner.

Once deployed, a smart contract becomes a permanent and immutable part of the blockchain, embodying the commitments of the parties involved within a secure and automated digital framework.

# WEB3 & AI : ALLOWING DECENTRALIZATION

Web3 technologies provide a new way to govern AI, ensuring transparency, data protection, and decentralization.

## **Blockchain for AI Data Integrity**

Blockchain records AI training data immutably, preventing unauthorized alterations. AI models trained on blockchain-verified datasets ensure provable authenticity. Users can verify where AI-generated content comes from—a key defense against deepfakes and misinformation.

## **Smart Contracts for AI Governance**

AI licensing agreements can be enforced automatically via smart contracts. AI-generated content can be verified, monetized, and tracked transparently. No need for intermediaries—Web3 allows direct, secure AI transactions.

## **Zero-Knowledge Proofs for Privacy & Compliance**

Users can prove their data was not used to train an AI model—without revealing personal information.

Companies can prove regulatory compliance (e.g., GDPR, AI Act) without exposing AI training methods.

AI developers can prove that AI outputs are legitimate without disclosing proprietary models.

For example: a user can check whether an AI-generated image was created by an approved AI model—without seeing the full AI training dataset.

# WEB3 & AI : TOWARDS PROTOCOLIZATION

Ensuring balance between **ethics and innovation** .

As artificial intelligence (AI) continues to evolve, ensuring fairness, security, and accountability is becoming a global priority. While AI has unlocked groundbreaking innovations, concerns around bias, data privacy, copyright violations, and misinformation remain unresolved.

**Web3 technologies**—particularly blockchain, smart contracts, and Zero-Knowledge Proofs (ZKPs)—offer **a way to "protocolize" AI governance**, meaning we can replace centralized oversight with automated, transparent, and secure mechanisms.

Today's AI landscape is highly centralized, meaning a few organizations control how models are trained, what data is used, and how decisions are made.

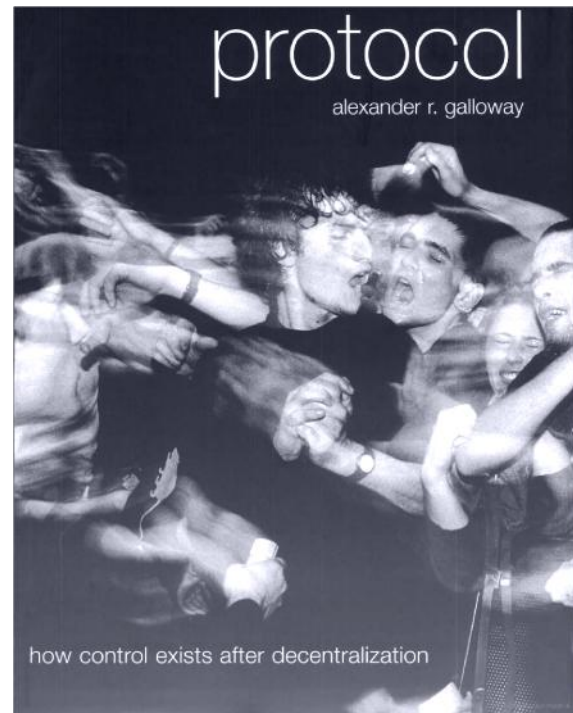
This raises key concerns:

**Lack of Transparency:** Users have no visibility into how AI models are trained or whether datasets are ethically sourced.

**Copyright Violations:** AI systems often crawl copyright protected content without attribution or authorization.

**Deepfake & Disinformation Risks:** AI-generated content can be manipulated and misused without clear authentication.

By protocolizing AI governance, Web3 provides verifiable, automated, and decentralized solutions that balance innovation with responsibility.

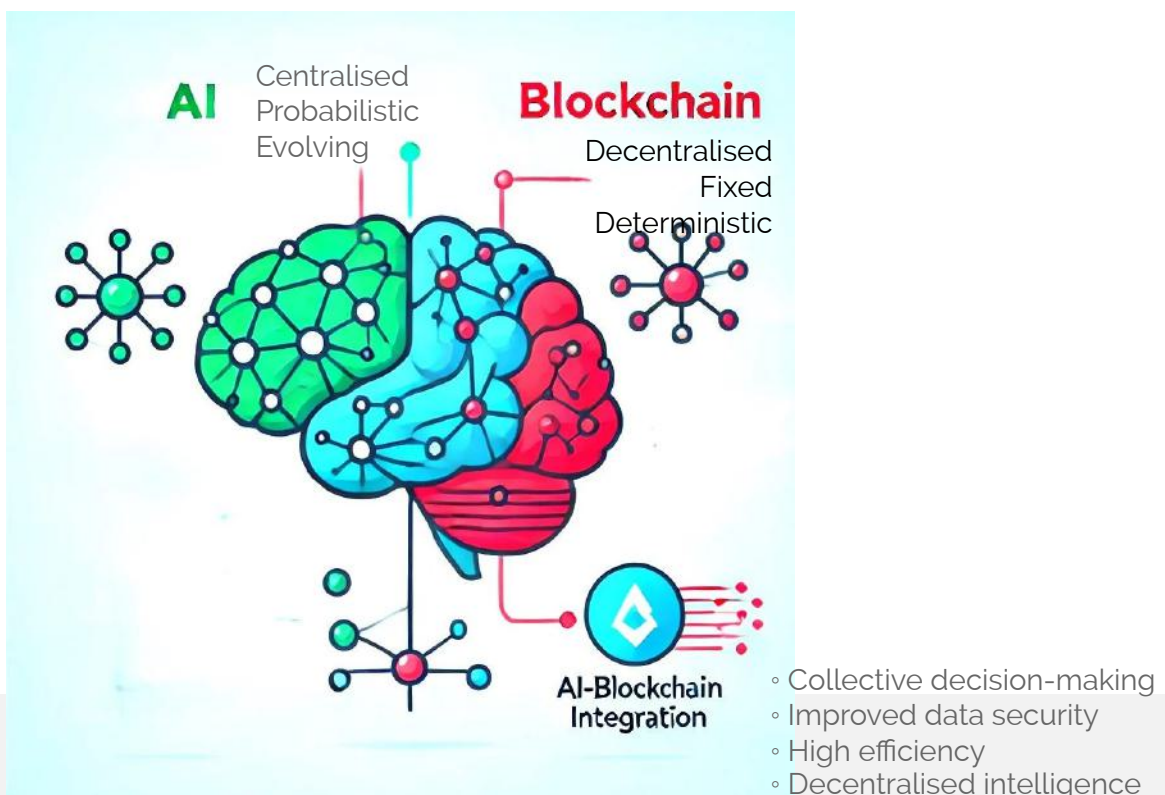


According to Alexander Galloway (Protocol: How Control Exists after Decentralization), protocols do not eliminate control; they redistribute it differently.

# WEB3 - AI INTEGRATION: IMPROVED TRANSPARENCY, INTEGRITY AND EFFICIENCY

Integrating AI & Web 3 provides 3 main benefits :

- **Enhanced Transparency and Auditability:** Blockchain improves the transparency of AI processes by recording decisions and logic in a consistent, auditable database
- **Improved Data Integrity:** Blockchain's data falsification protection reinforces the integrity of information used by AI.
- **Increased Efficiency:** AI and blockchain integration can optimize data storage and transaction validation, leading to greater operational efficiency and broader adoption.





# WEB3 & AI : USE CASES

## Data Monetization

Data monetization would make both AI and advanced blockchain easily accessible to smaller companies. The developing and growing AI technology is costly for organizations, especially those that do not own data sets. A decentralized market would create space for such companies where it is otherwise too expensive, in particular by allowing immediate payments settlement by microcrypto transfers in stable coins or, in the future in Central Bank Digital Currency. (CBDC). Therefore, Blockchain AI is a powerful enabler of data monetization, which is expected to be one of the biggest driving factors for the blockchain AI market.

## Supply Chain Optimization

It enables complete, immutable and transparent tracking of activity throughout the supply chain, facilitating collaboration between the various stakeholders. Like AI, Blockchain can be integrated into any sector, from food traceability (e.g. Walmart) to secure contracts (e.g. Docusign), collaboration in the pharmaceutical industry (e.g. Pfizer) and loyalty programmes (e.g. Burger King).

More precisely, AI can analyse the terms of smart contracts in real time to ensure compliance and optimise the terms in line with changing market conditions.

- AI can use the immutable data stored on the blockchain to generate more accurate and reliable knowledge, improving strategic decision-making at all levels of the supply chain.
- With digital identifiers verified and stored on a blockchain, AI can facilitate secure and automated transactions between parties without preestablished trust, reducing the need for intermediaries

## Financial Management

Automating and analysing financial data frees up accountants for strategic tasks, while improving fraud detection and risk management.

Blockchain facilitates and secures financial transactions, reduces costs and offers innovative ways of tokenising assets, increasing liquidity and diversifying investments.

*Example : J.P.Morgan has broken new ground in the financial sector with its "Cash-Flow Intelligence" tool, based on artificial intelligence, which reduces manual work by 90% for certain clients. With around 2,500 clients using this tool in March 2024, J.P.Morgan is moving closer to being able to charge for this service.*

## Notary services

Tediji integrates blockchain to offer an electronic notarisation solution. This technology ensures that each signed document is recorded immutably and transparently, providing irrefutable proof of the signature without the need for a traditional notary.

# ZERO-KNOWLEDGE TECHNOLOGIES

## FOR AI SECURITY, PRIVACY & IP PROTECTION

Zero-Knowledge Proofs (ZKPs) are a cryptographic technique that allows one party (the prover) to convince another party (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself. This enables **privacy-preserving verification in AI** and Web3 applications, particularly for intellectual property (IP) protection, compliance, and model authenticity.

ZKPs rely on three fundamental properties:

- **Completeness:** If the statement is true, the prover can convince the verifier.
- **Soundness:** If the statement is false, the prover cannot convince the verifier.
- **Zero-Knowledge:** The verifier gains no additional knowledge beyond the truthfulness of the claim.

These properties ensure that AI-generated content, proprietary models, and third-party intellectual property (3PIP) can be verified without exposing sensitive data.

There are different forms of ZKPs, each suited for specific use cases:

- **Interactive Zero-Knowledge Proofs (IZKPs):** Require multiple rounds of interaction between prover and verifier.
- **Non-Interactive Zero-Knowledge Proofs (NIZKPs):** Allow verification with a single proof, making them more efficient for large-scale AI verification.
- **Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs):** Provide compact, efficient proofs that verify computations without revealing underlying data.

These mechanisms enhance trust in AI-generated outputs, training datasets, and proprietary models while ensuring data privacy and regulatory compliance.

### ZKPs for Intellectual Property Protection in AI

AI Model Ownership Verification:

With increasing legal challenges regarding AI model ownership and dataset provenance, ZKPs enable secure verification of model authenticity without exposing underlying architectures.

Applications:

- **Watermarking AI Models:** ZKPs allow AI developers to embed and prove ownership of watermarked models without revealing proprietary techniques. This prevents unauthorized model replication while ensuring legal protection.
- **Verifying Model Training Integrity:** Regulators or stakeholders can confirm that an AI model was trained on approved datasets without disclosing sensitive training data.

# ZERO-KNOWLEDGE TECHNOLOGIES

## DATA SOVEREIGNTY

**Data Sovereignty and Gen AI :** Generative AI relies on vast datasets, often sourced without clear consent, leading to critical issues:

### **Lack of Control Over Training Data**

AI models are trained on billions of pieces of content, often using copyrighted material without authorization.

Users and creators have no visibility into whether their data has been used, modified, or monetized.

### **The "Right to Be Forgotten" Dilemma**

Once AI models are trained on personal data, there is no way to verify if the data has been removed.

Compliance with regulations like GDPR's right to erasure remains a challenge due to AI's black-box nature.

Lack of Dataset Transparency ; Most AI companies do not disclose the origins of their training data.

Users and regulators cannot verify whether AI models comply with copyright, privacy laws, or ethical standards.

Solution: Zero-Knowledge Proofs (ZKPs) and Web3 for Verifiable AI Data

**Reinventing AI Data Control :** Web3 provides a decentralized, verifiable, and privacy-preserving approach to AI data management.

Blockchain for AI Training Data Traceability:

Decentralized storage ensures that AI training datasets are verifiable and immutable.

Smart contracts enable automated data licensing, ensuring authorized usage of datasets.

ZKPs for Privacy-Preserving AI Data Verification.

Users can prove that an AI model has not used their data—without revealing details about the dataset itself.

Companies can prove compliance with data privacy laws (e.g., GDPR, AI Act) without exposing AI model internals.

### **Smart Contracts for AI Data Deletion & Compliance**

Blockchain-based deletion requests ensure that AI models comply with user rights and legal mandates.

ZKPs allow verification that a specific dataset has been removed without revealing the deleted information.

# BUILDING TRUSTWORTHY AI INFRASTRUCTURES

## The Need for AI Governance in a Decentralized World

As AI starts to shape industries, ensuring transparency, accountability, and regulatory compliance is essential. Traditional AI governance relies on centralized oversight, which often lacks traceability, fairness, and verifiability.

Web3 technologies—blockchain, smart contracts, and Zero-Knowledge Proofs (ZKPs)—offer a more robust, automated, and auditable approach to AI governance. By integrating Web3 principles, we can ensure AI operates within a secure, ethical, and regulation-compliant framework without compromising innovation.

## Implementing Web3-Based AI Governance

To build trustworthy AI systems, companies and institutions must adopt Web3 governance models that prioritize transparency, user control, and automated compliance.

Key recommendations :

- **Smart Contract Automation for Compliance** : AI governance frameworks should integrate smart contracts to enforce regulatory requirements automatically. These contracts can manage data usage permissions, licensing agreements, and audit logs without human intervention.
- **Provenance & Traceability Standards** : Adoption of C2PA standards for verifiable AI-generated content. Blockchain-based audit trails to track AI model modifications and data usage.
- **Decentralized AI Auditing** : Zero-Knowledge Proofs (ZKPs) allow AI companies to prove compliance without revealing sensitive details about their datasets or models. Independent, on-chain verification ensures AI processes remain ethical and unbiased.

## Encouraging International Standards for AI Infrastructure

A global, standardized approach is needed to align AI governance frameworks across different legal jurisdictions.

- **Harmonizing Global AI & Web3 Standards & Norms**

Establish a unified legal framework connecting Web3 standards with AI policies like the EU AI Act, GDPR, and other AI governance models.

Promote interoperability between decentralized AI systems and legal structures.

- **Open-Source & Independent AI Model Audits**

Support third-party, Blockchain-based audits for AI model transparency and risk assessment. Encourage Web3-enabled AI certification systems that verify model fairness and compliance without relying on centralized regulators.

# CONCLUSION

## **Towards a More Secure, Transparent, and Ethical AI Ecosystem ?**

To ensure AI is developed in way to ensure economics growth, trust and safety, companies, regulators, and developers should :

- Adopt Web3 and cryptographic AI governance models to enhance security and compliance.
- Implement ZKPs to protect privacy while enabling regulatory audits.
- Build decentralized AI frameworks that foster trust, accountability, and fairness.

By integrating Web3 technologies into AI governance, we can bring together ethics and innovation —creating an AI future that is balanced, verifiable, and secure for all.

# SOURCES

## Zero-Knowledge Proofs & AI Security

Bayan, T., & Banach, R. (2023, May 4-6). Exploring the privacy concerns in permissionless blockchain networks and potential solutions. 2023 IEEE Smart Information Systems and Technologies (SIST), Astana, Kazakhstan. IEEE.

Mouris, D., & Tsoutsos, N. G. (2020). Pythia: Intellectual property verification in zero-knowledge. IEEE.

Sah, C. P., Kaur, M., & Singh, G. (2024). Efficiency of zero-knowledge proofs: A thorough review and analysis. 2024 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA). IEEE.

Sheybani, N., Ghodsi, Z., Kapila, R., & Koushanfar, F. (2023, September 13). ZKROWNN: Zero knowledge right of ownership for neural networks. arXiv. <https://arxiv.org/abs/2309.06779>

Sun, H., Bai, T., Li, J., & Zhang, H. (2023, December 5). zkDL: Efficient zero-knowledge proofs of deep learning training. arXiv. <https://arxiv.org/abs/2307.16273>

Sun, H., Li, J., & Zhang, H. (2024, April 24). zkLLM: Zero knowledge proofs for large language models. arXiv. <https://arxiv.org/abs/2404.16109>

## AI Governance & Ethical Considerations

Bradley, F. (2025). The policy context of artificial intelligence. In AI and governance (pp. 72-84). De Gruyter. <https://doi.org/10.1515/9783111336435-008>

Galloway, A. R. (2004). Protocol: How control exists after decentralization. The MIT Press.

Gillain, E. (Ed.). (2024). Demystifying artificial intelligence: Symbolic, data-driven, statistical, and ethical AI. Walter de Gruyter. <https://doi.org/10.1515/9783111426143>

Toreini, E., Mehrnezhad, M., & van Moorsel, A. (2024). Fairness as a service (FaaS): Verifiable and privacy-preserving fairness auditing of machine learning systems. International Journal of Information Security, 23, 981-997. <https://doi.org/10.1007/s10207-023-00774-z>

## AI & Business Transformation

Carter, P., Parker, R., Clarke, B. E., Murphy, C., Siman, T., Stergiades, E., Thomason, M., Nadkarni, A., & Jyoti, R. (2024). Generative AI pricing models: A strategic buying guide. IDC.

Child, M., Clemente, D., Fouchereau, R., Helkenberg, R., & Stradling, J. (2025). IDC FutureScape: Worldwide security & trust 2025 predictions — European implications. IDC.

Friego, F., & Char, S. (2024). Business transformation through AI and blockchain. IDATE.

# ABOUT LSW3

The Web3 Security League (LSW3) is a non-profit organization dedicated to fighting against scams, fraud, theft, and other cryptocurrency and blockchain technology-related crimes in France and the European Union. We bring together professionals who defend and help victims, contributing through our expertise and market knowledge to the success of investigations.

## Our 3 working groups:

- Cybersecurity Monitoring, analysis, prevention, awareness of best practices, implementation of standards
- Legal Fighting against fraud and theft, prevention of best practices, legal remedies, networking
- Intellectual Property Fighting against abuse, legal working groups and representative role, proposal of tools and standards

## Our board

Sébastien Martin - CEO & Co-Founder de RAID Square Président

Fabien Aufrechter - VP WEB3 de Vivendi

Dominique Penin Partner White-collar Kramer Levin LLP

David Princay - Managing Director Binance FR

Merlin Égalité - Co-Founder Morpho Labs

Alain Broustail - CEO & Co-Founder Blockchain EZ

Général Christophe Husson ComCyber-MI

Email: [contact@lsw3.fr](mailto:contact@lsw3.fr)

