AVALY.AI

AI Security for Web3 & Decentralized Finance (DeFi)

The Evolving Landscape of AI in Web3 & DeFi

Artificial intelligence is reshaping Web3 and decentralized finance (DeFi), powering algorithmic trading, fraud detection, smart contract risk assessment, and digital asset security.

As platforms like Coinbase, Binance, Aave, and OpenSea integrate AI for financial automation and user analytics, they must also address emerging security threats. Securing AI-driven Web3 applications is not just about cybersecurity—it's about protecting digital assets, ensuring compliance, and maintaining trust in decentralized financial ecosystems.

Algorithmic Trading

Fraud Detection

Smart Contract Risk Assessment

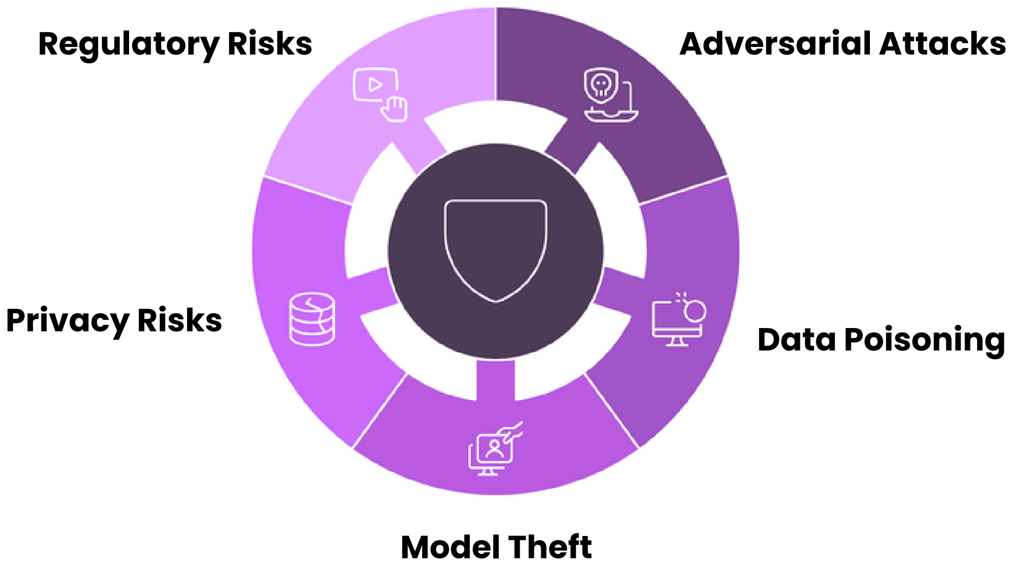
Digital Asset Security

Financial Automation

User Analytics

Security Threats

Key AI Security Challenges in Web3 & DeFi:



- **Adversarial Attacks:** Hackers manipulate AI models to bypass DeFi lending protocols, exploit liquidity pools, or forge fraudulent NFT transactions.
- **Data Poisoning:** Attackers inject false transaction data into AI models, distorting yield farming strategies and stablecoin risk assessments.
- **Model Theft & Reverse Engineering:** Proprietary AI-driven trading algorithms and blockchain analytics tools can be stolen or exploited.
- **Privacy Risks in Decentralized Finance:** AI-driven identity verification (e.g., DeFi KYC) relies on sensitive data, making crypto exchanges and DeFi platforms high-value targets for cyberattacks.
- **Regulatory & Compliance Risks:** AI models must align with crypto regulations, including AML/KYC, FATF guidelines, MiCA, and SEC oversight.

Real-World Examples:

- **AI-Powered DeFi Exploits:** Hackers use adversarial AI to manipulate smart contract logic, extracting funds from automated DeFi protocols.
- **Algorithmic Stablecoin Manipulation: A**ttackers poison AI models that regulate stablecoin pegs, triggering depegging events and financial losses.
- **Deepfake-Based NFT & Crypto Scams:** AI-generated deepfakes impersonate project founders to execute rug pulls or phishing schemes.
- **Regulatory Non-Compliance Risks:** AI-driven blockchain analytics tools fail to detect illicit crypto transactions, leading to legal penalties.

The Key Benefits of Partnering with Avaly.AI

Our AI Security Assessment Approach

Avaly.ai specializes in securing AI models used in cryptocurrency exchanges, DeFi lending, stablecoin risk management, NFT marketplaces, and blockchain infrastructure. Our solutions protect AI-driven Web3 applications without disrupting DeFi protocols, trading operations, or regulatory compliance.

Advanced Vulnerability Analysis

Strengthen AI-powered blockchain security, fraud detection, and smart contract auditing against adversarial threats.

AI Model Threat Detection:	Identify weaknesses in AI-driven risk models for stablecoins, lending pools, and DeFi insurance protocols.
Data Integrity Assessments:	Ensure AI training data remains free from manipulation, bias, or tampering.
Security Stress Testing	Simulate attacks on AI-driven DeFi platforms and NFT marketplaces to evaluate their resilience.

Regulatory & Compliance Alignment

Ensures AI-powered crypto and DeFi systems comply with global financial regulations, minimizing compliance risks.

Aligns with Crypto & DeFi Regulations:	Demonstrates compliance with MiCA, FATF travel rule, SEC, FinCEN, and global AML/KYC guidelines.
Bias & Fairness Audits:	Detect and mitigate biases in AI-driven risk assessment models for decentralized finance and crypto lending.
Explainability & Transparency Solutions:	Implement AI explainability tools, enabling regulators and DeFi users to understand AI-driven financial decisions.

Proactive AI Security Hardening

Future-proofs Web3 AI models against evolving cyber threats through continuous monitoring and proactive security enhancements.

Secure AI Model Lifecycle Management:	Ensures end-to-end security from AI model development to deployment in DeFi, crypto exchanges, and blockchain analytics.
Encryption & Privacy-Preserving Techniques:	Implements advanced encryption, zero-knowledge proofs, and privacy-preserving AI techniques for Web3 applications.
Real-Time AI Monitoring & Incident Response:	Continuously monitors AI-driven blockchain platforms for anomalies and potential security breaches.

Why Avaly.ai is the Leading AI Security Provider for Web3 & Decentralized Finance (DeFi)

1. AI & LLM Model Neutral – Securing Web3 Without Limits

Decentralized finance and Web3 platforms rely on AI-driven algorithms for trading, lending, and token management. Avaly.ai delivers a vendor-neutral approach, allowing crypto exchanges, DeFi protocols, and NFT marketplaces to secure any AI or LLM model without restrictions.

- **Compatible with Any AI & LLM Model**: Secure AI-powered smart contracts, automated trading bots, blockchain risk models, and decentralized identity verification systems.
- **Freedom to Use Any AI Platform**: Avoid vendor lock-in while ensuring state-of-the-art security. Avaly.ai seamlessly integrates with AI models across Layer 1 & Layer 2 blockchains, decentralized applications (dApps), and multi-chain ecosystems.
- **Seamless Integration with Web3 & DeFi Platforms**: Protecting AI-driven crypto exchanges, decentralized lending protocols, stablecoin algorithms, NFT marketplaces, and tokenized asset platforms.

2. Seamless AI Security Integration Across Web3 Ecosystems

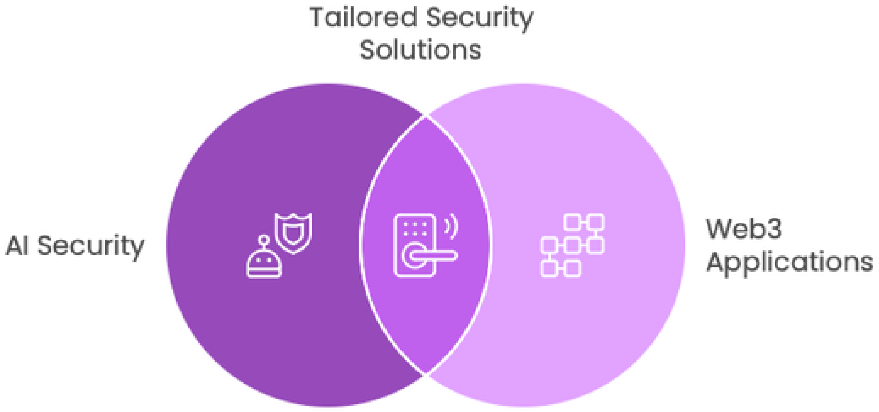
Web3 platforms require AI security solutions that enhance decentralization without introducing friction. Avaly.ai ensures that AI-powered DeFi, crypto, and NFT platforms remain secure—without disrupting automation, liquidity, compliance workflows, or vendor lock-in.

- **Strengthen AI Security Without Compromising Decentralization**: Avaly.ai integrates effortlessly with SIEM systems, blockchain analytics tools, and DeFi security frameworks, enhancing Web3 AI protections.
- **Turn Compliance into a Competitive Advantage**: Our AI security solutions help Web3 projects meet FATF, AML/KYC, MiCA, and SEC compliance requirements, ensuring transparency in AI-driven decentralized finance operations.
- **Protect AI at Every Stage of the Blockchain Lifecycle:** From algorithmic stablecoin issuance to AI-driven DeFi lending models, Avaly.ai safeguards decentralized financial applications from AI-specific attack vectors.
- **Supercharge Web3 Security with AI Threat Intelligence**: With an ever changing landscape of threats and scams targeting DeFi, Avaly.ai empowers your SOC to monitor, detect, and respond to cyber threats to prevent AI-driven exploits.
- **Secure AI in Multi-Chain & Hybrid Environments—Without Gaps**: Whether securing AI models on Ethereum, Solana, Binance Smart Chain, or Layer 2 rollups, Avaly.ai ensures smart contract integrity, decentralized governance security, and AI-driven fraud prevention.

3. Web3-Specific AI Security: Built for DeFi, Crypto & NFTs

Unlike traditional cybersecurity firms, Avaly.ai specializes in AI security for Web3 applications, DeFi platforms, and blockchain ecosystems. We understand the industry's decentralized nature, unique attack vectors, and evolving regulatory landscape—delivering security solutions tailored for AI-powered DeFi and crypto applications.

- **Eliminate AI-Driven DeFi & Crypto Fraud:**
  AI is transforming trading bots, liquidity pools, and decentralized lending models. Avaly.ai secures AI models against adversarial attacks, price oracle manipulation, and AI-powered phishing scams.
- **Secure the Future of AI in Web3 & Blockchain:**
  Whether operating in decentralized finance, crypto exchanges, NFT marketplaces, or stablecoin governance, Avaly.ai ensures AI models remain secure, tamper-proof, and regulatory-compliant.
- **Web3-Specific AI Security—Not a One-Size-Fits-All Approach:**
  We work exclusively with DeFi protocols, crypto exchanges, blockchain infrastructure providers, and NFT platforms—delivering tailored AI security solutions that align with the risks of decentralized ecosystems.



4. A Team of Top Research & Industry AI Security Experts

Our team consists of leading AI researchers, cybersecurity experts, and academic pioneers—bringing cutting-edge AI security advancements directly from research into real-world financial applications. Avaly.ai is a highly skilled PhD-led research team, with expertise in adversarial AI, LLM red teaming, Reinforcement Learning security, Autonomous Cybersecurity, blockchain, and financial cybersecurity.

Secure Your AI-Driven Web3 & DeFi Operations

AI threats are growing—don't wait until it's too late. Partner with Avaly.ai today to safeguard your AI systems from adversarial attacks, regulatory risks, and financial fraud.

Contact us now for a tailored AI security assessment!

🌐 **Learn about us: www.avaly.ai**

Let's Talk

For more information or to schedule a consultation, please reach out:

Reza Parizi
(Ph.D.)

Co-founder & President
✉ reza@avaly.ai

Ali Dehghantanha
(PhD, CISSP, CISM)

Co-founder & CEO
✉ ali@avaly.ai

Farzin Gholamrezae
(MSc)

Director of Business Development
✉ farzin@avaly.ai

Wilma Vieira

Marketing & Communications Manager
✉ wilma@avaly.ai

AVALY.AI