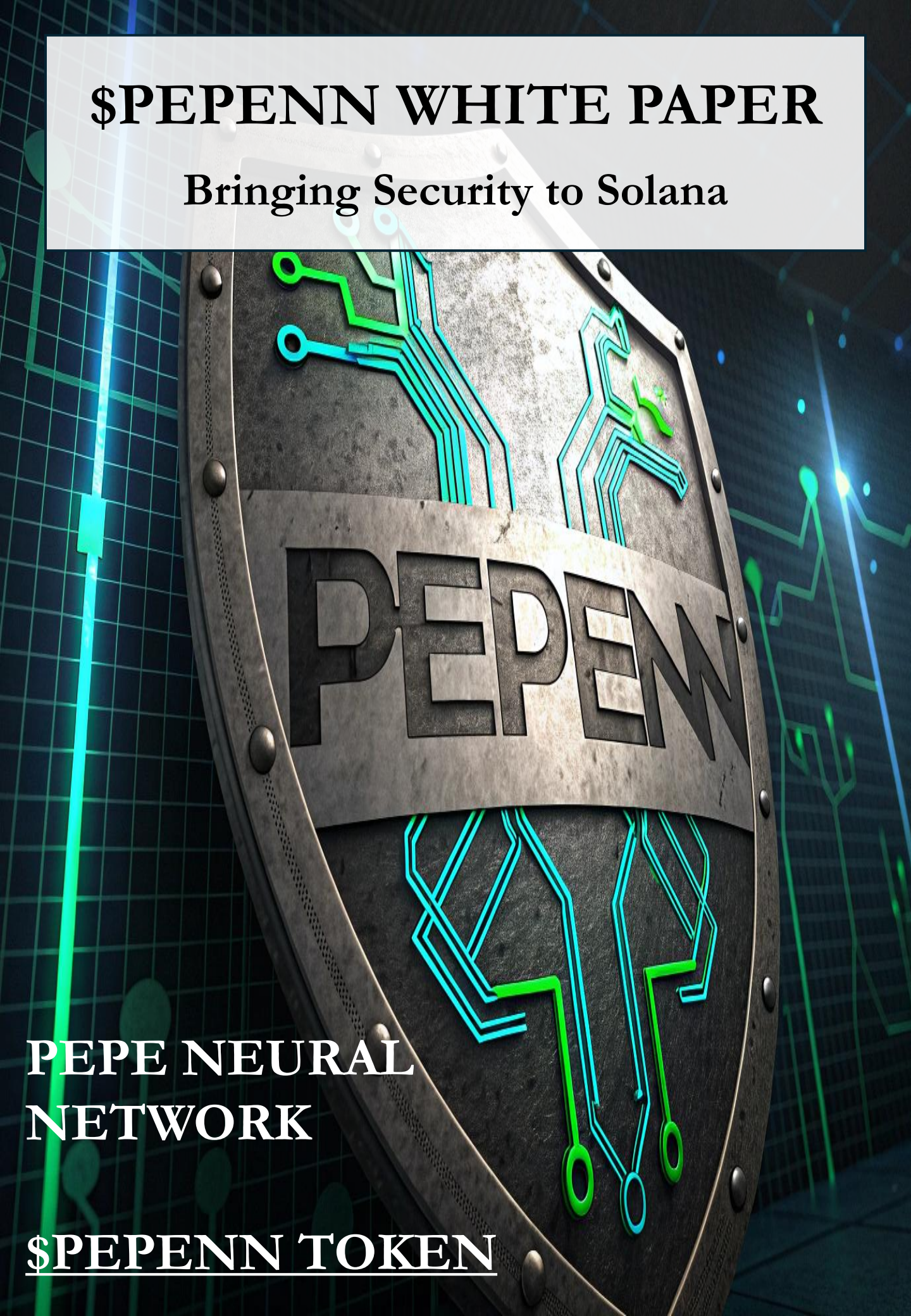
$PEPENN WHITE PAPER

Bringing Security to Solana



PEPE NEURAL NETWORK

$PEPENN TOKEN

Contents

1. Introduction

The explosive growth of decentralized finance (DeFi), NFTs, and blockchain applications has brought significant financial opportunities but has also exposed users to increased security risks. Solana, known for its high throughput and low transaction fees, has rapidly become a leading blockchain for DeFi and NFT ecosystems. However, the lack of native, built-in security mechanisms means that users and projects remain highly vulnerable to a range of attacks and fraud schemes.

- **Phishing scams:** Malicious actors trick users into signing fraudulent transactions, leading to irreversible loss of funds.
- **Wallet hacks:** Weak private key security and phishing attacks expose users to direct theft.
- **Smart contract vulnerabilities:** DeFi projects and protocols often experience exploits due to coding errors, flash loan attacks, or rug pulls.
- **Lack of recovery mechanisms:** Once assets are stolen, the irreversibility of blockchain transactions means there is often no recourse.
- **Inadequate fraud detection:** Existing security solutions rely on centralized services or manual user reporting, which is inefficient and reactive rather than proactive.

These security challenges have eroded trust in the ecosystem, discouraged mainstream adoption, and resulted in billions of dollars in losses. A decentralized, intelligent, and proactive security solution is urgently needed to protect users and projects within the Solana ecosystem.

2. PEPENN's Mission

PEPENN is designed to be **the "Chainlink of Security" for Solana**, providing an **on-chain, decentralized, and AI-driven security protocol** that proactively protects users, DeFi protocols, and NFT marketplaces from malicious activities. Unlike traditional centralized security solutions, PEPENN ensures full user control, transparency, and decentralization, making security a fundamental, autonomous layer of the Solana blockchain.

Our mission is to:

- **Provide real-time fraud detection**: Using AI-driven anomaly detection, PEPENN continuously monitors transactions and contract interactions to flag suspicious activities before execution.
- **Enable proactive threat mitigation**: By implementing smart contract firewalls and customizable transaction security policies, users can prevent unauthorized interactions before funds are lost.
- **Offer decentralized recovery mechanisms**: Utilizing multi-signature approvals, encrypted key splitting, and guardian-based recovery, PEPENN introduces a trust less approach to wallet security and recovery.
- **Create a decentralized security governance model**: Through the PEPENN DAO, PEPENN token holders will have the ability to vote on security policies, fraud resolutions, and protocol upgrades, ensuring a community-driven approach to blockchain security.
- **Integrate seamlessly with Solana wallets, DeFi, and NFT platforms**: Our technology will be embedded into Phantom, Solflare, and leading Solana-based applications to provide a seamless, user-friendly security experience.

By providing real-time, autonomous, and AI-enhanced security features, PEPENN aims to establish a new standard for blockchain security, making Solana a safer, more resilient ecosystem for all users and developers.

3. Key Features

3.1 Smart Contract Firewalls

- **Customizable security policies**: Users can define transaction rules such as spending limits, time delays, and authorization requirements to ensure funds are only sent under predetermined conditions.
- **Multi-factor authentication**: High-value transactions require additional authentication layers, such as biometric verification, social consensus, or cryptographic proof-of-ownership.
- **DeFi Interaction Control**: Users can whitelist trusted dApps while automatically blocking interactions with unverified or high-risk protocols, reducing exposure to malicious smart contracts.

3.2 AI-Powered Fraud Detection

- **On-chain machine learning models**: AI continuously analyzes transaction patterns to identify anomalies indicative of fraud, hacks, or abnormal behaviors.
- **Automatic alerts**: PEPENN instantly notifies users if a transaction is flagged as suspicious, allowing them to intervene before funds are lost.
- **Blacklist integration**: The protocol maintains a decentralized registry of known scam addresses, exploiters, and malicious wallets to proactively block fraudulent transactions.

3.3 Delayed Transaction Execution & Rollback

- **Time-lock mechanism**: Users can set a predefined delay for high-value transactions, allowing time to cancel if fraud is detected.
- **Emergency rollback feature**: If an account is compromised, users can cancel pending transactions before they are finalized on the blockchain.
- **Automated risk assessment**: Every transaction is scored based on risk factors, and high-risk transactions require additional manual confirmation before being executed.

3.4 Decentralized Wallet Recovery

- **Guardian-based recovery**: Users designate a trusted group of guardians (friends, family, or DAOs) who can collectively authorize wallet recovery in case of lost access.
- **Shamir's Secret Sharing**: Private keys are split into encrypted fragments distributed among multiple secure nodes, preventing a single point of failure.
- **Zero-trust architecture**: Recovery is executed without exposing full private keys, ensuring users maintain sovereignty over their assets.

3.5 Encrypted Key Splitting & Storage

- **Private key fragmentation**: Keys are broken into multiple encrypted pieces stored across different decentralized nodes, reducing the risk of a single compromise.
- **Multi-layer encryption**: Advanced cryptographic techniques secure key shards, ensuring even if a portion is exposed, the full key remains unrecoverable.
- **Redundant storage**: Key fragments are stored in multiple locations to ensure high availability and prevent loss due to node failures.

3.6 DeFi & NFT Protection Suite

- **Automated smart contract scanning**: PEPENN continuously scans and audits smart contracts to detect vulnerabilities, re-entrancy attacks, and security flaws.
- **Rug pull detection**: AI-powered analysis monitors liquidity pools and trading activity to detect and flag potential exit scams before they occur.
- **Fake NFT detection**: The protocol verifies NFT collections against legitimate registries, alerting users to counterfeit assets and wash trading schemes.

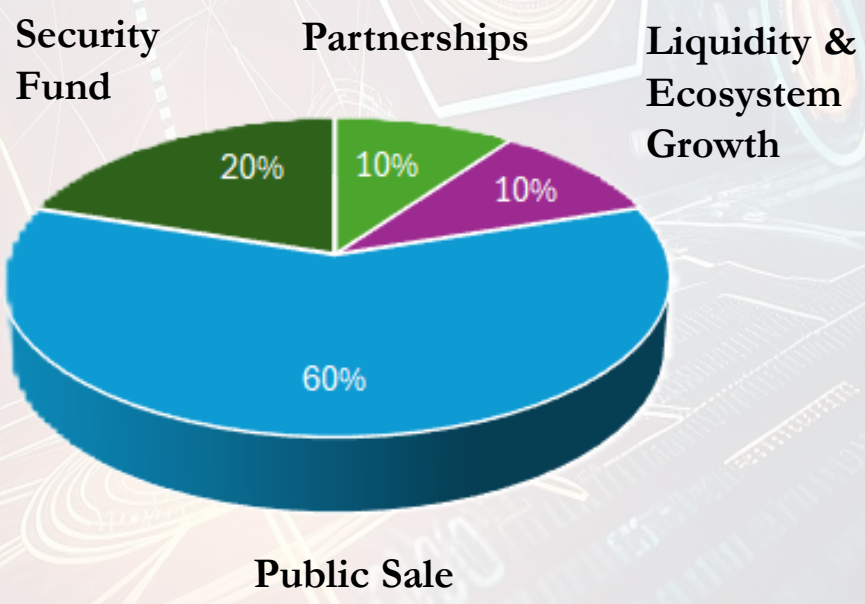
4. PEPENN Tokenomics

4.1 Utility of PEPENN Token

- **Staking for Security**: Users stake PEPENN to access premium protection features.
- **Fraud Bounty Rewards**: White-hat hackers earn PEPENN for identifying vulnerabilities.
- **Governance & Fraud Resolution**: PEPENN holders vote on disputed transactions and fraud cases.
- **Insurance Fund**: Treasury-backed reimbursements for verified security breaches.

4.2 Token Distribution (30_000_000_000 Tokens total)

- **60% Public Sale -** Presale
- **20% Security Fund** - Fraud Reimbursements & Staking Rewards
- **10% Partnerships -** Wallets, dApps, and DeFi protocols
- **10% Liquidity & Ecosystem Growth**



5. Development Roadmap

Phase 1: 0-3 Months (Token Presale & Launch)

- **PEPENN Token Presale:** Launch PEPENN website and community channels.
- **Marketing:** Bitcoin marketing giveaway

Phase 2: 3-9 Months

- **Exchange listing:** Listed on exchanges and liquidity pools added
- **Smart Contract Firewall Prototype:** Develop and test smart contract firewall rules and user-configurable security parameters.
- **AI Fraud Detection Training Begins:** Implement initial AI models for transaction monitoring and fraud prevention
- **PEPENN Governance:** Launch PEPENN DAO for governance participation.
- **Partnerships with Solana Wallets:** Integrate security solutions into Phantom, Solflare, and Backpack wallets for native security.
- **Launch PEPENN Testnet:** Deploy testnet version of the protocol for early user trials and security assessments.
- **dAPP Security:** Establish security monitoring services for dApps.
- **Testing:** Begin closed beta testing with early adopters and community testers.

Phase 3: 9-18 Months

- **Transaction Rollback System on Solana Main-net:** Deploy transaction delay and rollback mechanisms for real-world testing.
- **Wallet Recovery:** Implement decentralized wallet recovery mechanisms.
- **AI Deployment:** Full deployment of AI-driven fraud detection models. Focusing on real-time scanning for rug pulls, scam contracts, and fake NFT collections.
- **Insurance Fund Activation:** Launch PEPENN fraud Insurance Fund.
- **Expansion:** Expand ecosystem partnerships with NFT platforms and major DeFi projects.

Phase 4: 18+ Months

- **Deployment:** Full-scale deployment of PEPENN across Solana ecosystem.
- **Monitoring:** Continuous upgrades and security improvements**.**
- **Cross-Chain Security Expansion:** Extend security solutions to Ethereum, Binance Smart Chain, and other networks.
- **PEPENN DAO Voting:** Enable community governance where PEPENN holders influence security policy decision making and ongoing platform direction.

6. Go-To-Market Strategy

6.1 Wallet & DeFi Partnerships

- **Integration with Phantom, Solflare, and Backpack:** Provide built-in security features within popular Solana wallets to increase adoption and usability.
- **Partnerships with DeFi Platforms:** Collaborate with Jupiter, Raydium, and Orca to secure transactions, flag suspicious activities, and prevent unauthorized asset transfers.

6.2 NFT Security Collaboration

- **Verification with Magic Eden & Tensor:** Integrate real-time scam detection to identify fake NFT collections and malicious transactions.
- **AI-powered risk analysis:** Implement automated monitoring to assess NFT authenticity and detect wash trading schemes.

6.3 Influencer & Bounty Campaigns

- **Hack PEPENN Contests:** Engage security researchers and ethical hackers in bounty programs to stress-test the protocol and enhance its security.
- **Influencer partnerships:** Work with blockchain security experts, analysts, and content creators to drive awareness and adoption within the crypto community.
- By executing this comprehensive development and marketing strategy, PEPENN aims to become the leading security protocol in the Solana ecosystem and beyond.

7. Community & Governance

7.1 PEPENN DAO

- The PEPENN DAO enables PEPENN token holders to participate in security governance.
- Community members can propose, discuss, and vote on security policy updates, fraud resolutions, and protocol enhancements.
- Decentralized governance ensures transparency and aligns security measures with community interests.

7.2 Staking & Voting Mechanism

- PEPENN token holders can stake tokens to participate in governance and earn rewards.
- Voting power is weighted based on staked PEPENN tokens and contribution to security discussions.
- Staking rewards incentivize long-term participation and active governance engagement.

7.3 Community Engagement & Education

- PEPENN will launch educational initiatives, webinars, and hackathons to educate users on blockchain security.
- A bounty program will encourage ethical hackers to identify vulnerabilities and enhance the protocol's robustness.
- Community-driven security research and audits will be incentivized to ensure continuous improvement.

By fostering an engaged and knowledgeable community, PEPENN ensures that security remains a shared responsibility, strengthening the ecosystem's resilience against threats.

8. Disclaimer

This document is for informational purposes only and does not constitute financial, legal, or investment advice. Pepe Neural Network and its associated token ($PEPENN) involve risks, and participants should conduct thorough research and consult with financial, legal, and technical professionals before making any decisions related to the protocol.

Risk Disclosure:

Participation in blockchain-based security solutions, including PEPENN, involves significant financial and technical risk. Users should be aware of potential smart contract vulnerabilities, market volatility, and evolving regulatory landscapes.

- Cryptocurrency and digital assets are inherently volatile and can result in partial or total loss of funds.
- Security breaches, unforeseen exploits, or protocol failures may impact PEPENN's functionality.
- Decentralized governance decisions may lead to changes in PEPENN's policies, features, or risk exposure.

Legal Considerations:

The regulatory status of decentralized security protocols, blockchain technologies, and AI-based fraud detection solutions varies across jurisdictions. PEPENN does not guarantee compliance with all legal frameworks. Users are responsible for ensuring compliance with local regulations, tax obligations, and legal requirements in their respective regions.

- PEPENN does not provide insurance, guaranteed asset recovery, or legal protections in case of security breaches.
- The PEPENN DAO and governance mechanisms do not constitute a legally registered entity and operate in a decentralized manner.
- Integration with third-party wallets, DeFi protocols, and NFT platforms is subject to external risks beyond PEPENN's control.

Disclaimer – continued

Project Limitations & No Guarantee of Service:

PEPENN is a security-enhancement protocol and not a financial institution, bank, or regulated entity.

- The availability and effectiveness of PEPENN's security features, including fraud detection, transaction rollback, and wallet recovery, depend on blockchain infrastructure and smart contract function.
- Service disruptions, network congestion, or blockchain failures may impact PEPENN's performance and security guarantees.
- PEPENN reserves the right to modify or discontinue features as needed based on governance decisions, security updates, and evolving threats.

User Responsibility & Wallet Recovery:

By using PEPENN, you acknowledge and accept the risks associated with decentralized security protocols, smart contracts, and digital assets.

- Users retain full control over their wallets, private keys, and transactions.
- PEPENN provides a wallet recovery feature, but recovery is subject to certain conditions, such as multi-signature authentication, proof-of-ownership mechanisms, and PEPENN DAO policies.
- While PEPENN aims to enhance asset recovery in case of theft, loss, or fraud, it does not guarantee full restoration of funds in all circumstances.
- Users must opt into recovery services, and PEPENN is not responsible for assets lost due to user negligence, phishing attacks, or transactions outside of PEPENN's security scope.

By participating in PEPENN, you agree to assume full responsibility for your security and financial decisions. Any engagement with the PEPENN protocol, its features, or governance is at your sole discretion and risk.