Your Gateway to a Safer Web3."

KEYSHIELDX

WHITEPAPER

www.keyshiledx.com

TABLE OF CONTENTS

1. ABSTRACT

KEYSHIELDX IS A PIONEERING DECENTRALIZED SECURITY PROTOCOL DESIGNED TO SAFEGUARD THE WEB3 ECOSYSTEM BY LEVERAGING MULTI-PARTY COMPUTATION (MPC) FOR KEY RECOVERY AND SECURE SIGNING, ARTIFICIAL INTELEGENCE-DRIVEN (AI-DRIVEN) SMART CONTRACT AUDITS, AND MULTI-CHAIN PHISHING AND SCAM PREVENTION. KEYSHIELDX DELIVERS USERS WITH A SEAMLESS, USER-CENTRIC SECURITY SOLUTION AND FULL CONTROL. WITH OVER $10 BILLION LOST TO HACKS AND SCAMS IN THE PAST FIVE YEARS (2020–2024, PER INDUSTRY REPORTS), THE NEED FOR ROBUST SECURITY IS UNDENIABLE. KEYSHIELDX EMPOWERS USERS WITH FULL CONTROL OVER THEIR ASSETS WHILE ELIMINATING SINGLE POINTS OF FAILURE.

2. INTRODUCTION

2.1 THE WEB3 SECURITY IMPERATIVE

WEB3 PROMISES A DECENTRALIZED, USER OWNED INTERNET, BUT ITS GROWTH HAS BEEN MARRED BY SECURITY FAILURES. IN 2023, DEFI EXPLOITS DRAINED $2.8 BILLION (CHAINALYSIS), WHILE PHISHING ATTACKS ACROSS BLOCKCHAINS SURGED BY 40%. KEY MANAGEMENT REMAINS A WEAK LINK: CENTRALIZED CUSTODIANS LIKE FTX COLLAPSED IN 2022, AND SELF-CUSTODY RISKS LOSING ASSETS TO LOST KEYS. KEYSHIELDX ADDRESSES THESE PAIN POINTS WITH A HOLISTIC, DECENTRALIZED APPROACH.

2.2 MISSION AND VISION

OUR MISSION IS TO SECURE WEB3 FOR ALL USERS I.E. NOVICES AND EXPERTS ALIKE. BY INTEGRATING CUTTING EDGE CRYPTOGRAPHY, ARTIFICIAL INTELLIGENCE, AND CROSS CHAIN INTEROPERABILITY, KEYSHIELDX AIMS TO REDUCE LOSSES TO ZERO AND FOSTER TRUST IN DECENTRALIZED SYSTEMS. OUR VISION IS A WEB3 WHERE SECURITY IS INVISIBLE YET OMNIPRESENT, ENABLING MASS ADOPTION.

3. PROBLEM STATEMENT

3.1 KEY MANAGEMENT VULNERABILITIES:

OVER 3 MILLION BTC (15% OF SUPPLY) ARE ESTIMATED LOST DUE TO MISPLACED KEYS (GLASSNODE, 2024) YET CENTRALIZED RECOVERY SOLUTIONS UNDERMINE DECENTRALIZATION.

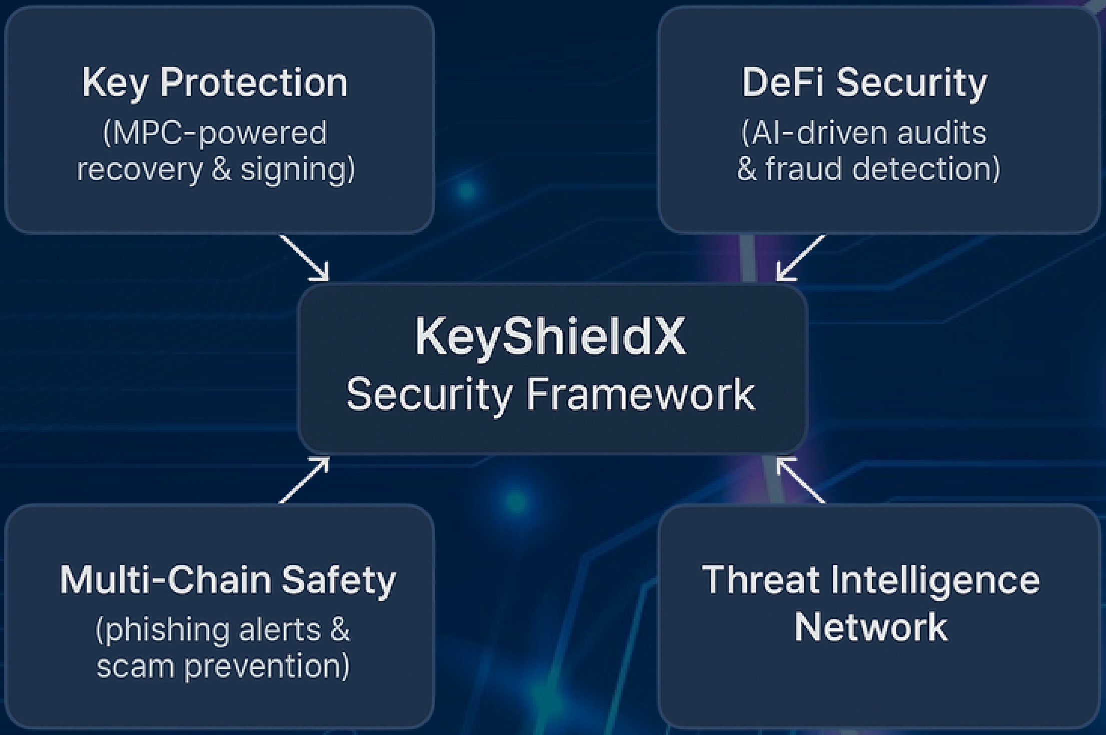
3.2 DEFI EXPLOITS:

SMART CONTRACT BUGS AND FRAUD COST USERS MILLIONS, WITH 2023 SEEING A 50% RISE IN EXPLOITS (PER WEB3 SECURITY REPORTS). THESE SMART CONTRACT BUGS CAUSED APPROXIMATELY A $1.5 BILLION IN LOSSES IN 2024 ALONE, WITH 60% LINKED TO UNAUDITED CODE (CERTIK).

3.3 CROSS-CHAIN RISKS:

PHISHING AND SCAM CONTRACTS ON EMERGING CHAINS LIKE SOLANA AND BINANCE SMART CHAIN ROSE 300% FROM 2022–2024 THUS EXPLOITING FRAGMENTED OVERSIGHT.

4.KEYSHIELDX SECURITY FRAMEWORK



Key Protection (MPC-powered recovery & signing)

DeFi Security (AI-driven audits & fraud detection)

KeyShieldX Security Framework

Multi-Chain Safety (phishing alerts & scam prevention)

Threat Intelligence Network

THE KEYSHIELDX SECURITY FRAMEWORK IS A MULTI-LAYERED WEB3 SECURITY SOLUTION DESIGNED TO PROTECT USERS, DEVELOPERS, AND INSTITUTIONS FROM KEY MANAGEMENT RISKS, SMART CONTRACT VULNERABILITIES, AND MULTI-CHAIN SCAMS. IT INTEGRATES MPC (MULTI-PARTY COMPUTATION) FOR KEY SECURITY, ARTIFICIAL INTELLEGENCE-DRIVEN (AI-DRIVEN) SMART CONTRACT AUDITING, REAL TIME SCAM DETECTION, AND A DECENTRALIZED THREAT INTELLIGENCE NETWORK TO CREATE A SECURE AND TRUSTLESS WEB3 ENVIRONMENT.

KEYSHIELDX OFFERS A FOUR PILLAR SECURITY FRAMEWORK, BUILT ON A DECENTRALIZED ARCHITECTURE:

4.1 KEY PROTECTION (MPC-POWERED RECOVERY AND SIGNING)

TRADITIONAL WALLETS STORE PRIVATE KEYS IN A SINGLE LOCATION, MAKING THEM VULNERABLE TO THEFT, PHISHING, AND USER ERRORS. KEYSHIELDX REMOVES THIS SINGLE POINT OF FAILURE BY IMPLEMENTING MULTI-PARTY COMPUTATION (MPC):

✅ HOW IT WORKS:

- INSTEAD OF STORING THE FULL PRIVATE KEY IN ONE PLACE, MPC SPLITS IT INTO MULTIPLE KEY SHARES ACROSS DIFFERENT NODES OR DEVICES.
- NO SINGLE ENTITY (NOT EVEN KEYSHIELDX) HAS ACCESS TO THE FULL KEY.
- THE KEY SHARES WORK TOGETHER IN A MATHEMATICALLY SECURE WAY TO SIGN TRANSACTIONS AND RECOVER ACCESS WHEN NEEDED.

✅ BENEFITS:

- SECURE AUTHENTICATION & SIGNING – TRANSACTIONS ARE SIGNED WITHOUT EXPOSING THE PRIVATE KEY, PREVENTING UNAUTHORIZED ACCESS.
- ELIMINATES SEED PHRASES – USERS DON’T NEED TO STORE OR REMEMBER A SINGLE SEED PHRASE, REDUCING PHISHING RISKS.
- ENTERPRISE-GRADE SECURITY – SUITABLE FOR INSTITUTIONAL INVESTORS, DAOS, AND ORGANIZATIONS MANAGING LARGE DIGITAL ASSETS.
- WEB3 COMPATIBILITY – CAN BE INTEGRATED WITH POPULAR WALLETS, DAPPS, AND EXCHANGES VIA APIS.

4.2 DEFI SECURITY (AI-DRIVEN AUDITS & FRAUD DETECTION)

THE BIGGEST VULNERABILITY IN DEFI IS SMART CONTRACT EXPLOITS. MALICIOUS ACTORS EXPLOIT CODING ERRORS, FLASH LOANS, AND UNVERIFIED CONTRACTS, LEADING TO BILLIONS IN LOSSES. KEYSHIELDX INTEGRATES AI-POWERED SECURITY AUDITS TO PREVENT THESE RISKS.

✅ HOW IT WORKS:

- AI SCANS SMART CONTRACT CODE BEFORE DEPLOYMENT TO DETECT VULNERABILITIES.
- ON-CHAIN MONITORING FLAGS SUSPICIOUS BEHAVIOR IN REAL TIME.
- ALERTS WARN USERS AND DAPPS ABOUT HIGH-RISK TRANSACTIONS OR CONTRACTS.
- SECURITY INSIGHTS ARE CROWDSOURCED FROM ETHICAL HACKERS (WHITE-HAT CONTRIBUTORS).
- EGRATE AI-POWERED SECURITY ALERTS.

✅ BENEFITS:

- PRE-DEPLOYMENT PROTECTION :– IDENTIFIES CONTRACT FLAWS BEFORE LAUNCH, REDUCING SECURITY RISKS.
- CONTINUOUS THREAT MONITORING :– WATCHES ON-CHAIN ACTIVITY FOR ANOMALIES, PREVENTING FLASH LOAN ATTACKS AND RUG PULLS.
- CROWDSOURCED SECURITY :– WHITE-HAT HACKERS CAN CONTRIBUTE TO IMPROVING SECURITY AND GET REWARDED.
- USER-FRIENDLY WARNINGS :– WEB3 WALLETS AND DAPPS CAN INTEGRATE AI-POWERED SECURITY ALERTS.

4.3 MULTI-CHAIN SAFETY (PHISHING ALERTS & SCAM PREVENTION)

SCAMMERS TAKE ADVANTAGE OF MULTI-CHAIN INTEROPERABILITY BY CREATING FAKE TOKENS, MALICIOUS SMART CONTRACTS, AND PHISHING WEBSITES. KEYSHIELDX PROTECTS USERS FROM THESE THREATS THROUGH AI-DRIVEN SCAM DETECTION AND PHISHING ALERTS.

✅ HOW IT WORKS:

- AI ANALYZES HISTORICAL SCAM PATTERNS TO DETECT SUSPICIOUS DAPPS, WALLETS, AND TOKEN CONTRACTS.
- WEB3 WALLETS AND BROWSERS DISPLAY REAL-TIME PHISHING ALERTS WHEN USERS VISIT FAKE SITES.
- EXCHANGES AND DAPPS CAN INTEGRATE KEYSHIELDX APIS TO PREVENT FRAUDULENT TRANSACTIONS.

✅ BENEFITS:

- CROSS-CHAIN SCAM DETECTION – IDENTIFIES FRAUDULENT ACTIVITY ACROSS MULTIPLE BLOCKCHAINS.
- REAL-TIME PHISHING ALERTS – WARNS USERS WHEN THEY INTERACT WITH SUSPICIOUS WEBSITES OR CONTRACTS.
- SAFER TRADING & TRANSACTIONS – HELPS PREVENT USERS FROM BUYING FAKE TOKENS OR INTERACTING WITH MALICIOUS SMART CONTRACTS.
- PLUG-AND-PLAY SECURITY – EASILY INTEGRATES WITH WALLETS, EXCHANGES, AND DAPPS.

4.4 THREAT INTELLIGENCE NETWORK

KEYSHIELDX LEARNS AND ADAPTS TO EMERGING WEB3 THREATS USING A DECENTRALIZED THREAT INTELLIGENCE DATABASE. THIS SHARED INTELLIGENCE HELPS USERS AVOID KNOWN SCAMS AND IMPROVE THE OVERALL SECURITY OF THE ECOSYSTEM.

✅ HOW IT WORKS:

- A NETWORK OF NODES COLLECTS REAL-TIME ATTACK DATA FROM VARIOUS CHAINS.
- SECURITY INSIGHTS ARE SHARED ACROSS THE ECOSYSTEM, ALLOWING USERS TO AVOID DANGEROUS CONTRACTS OR ADDRESSES.
- AI CONTINUOUSLY UPDATES FRAUD DETECTION MODELS, MAKING KEYSHIELDX MORE EFFECTIVE OVER TIME.

✅ BENEFITS:

- DECENTRALIZED ATTACK DETECTION – SECURITY DATA IS COLLECTED FROM MULTIPLE SOURCES, REDUCING SINGLE POINTS OF FAILURE.
- ADAPTIVE THREAT PREVENTION – AI-POWERED SECURITY MODELS IMPROVE BASED ON NEW THREATS.
- COLLABORATIVE PROTECTION – DEVELOPERS, WHITE-HAT HACKERS, AND USERS CONTRIBUTE TO STRENGTHENING WEB3 SECURITY.
- REDUCES LOSSES FROM SCAMS – PREVENTS USERS FROM INTERACTING WITH KNOWN EXPLOITERS AND FRAUDULENT ENTITIES.

8. TOKENOMICS

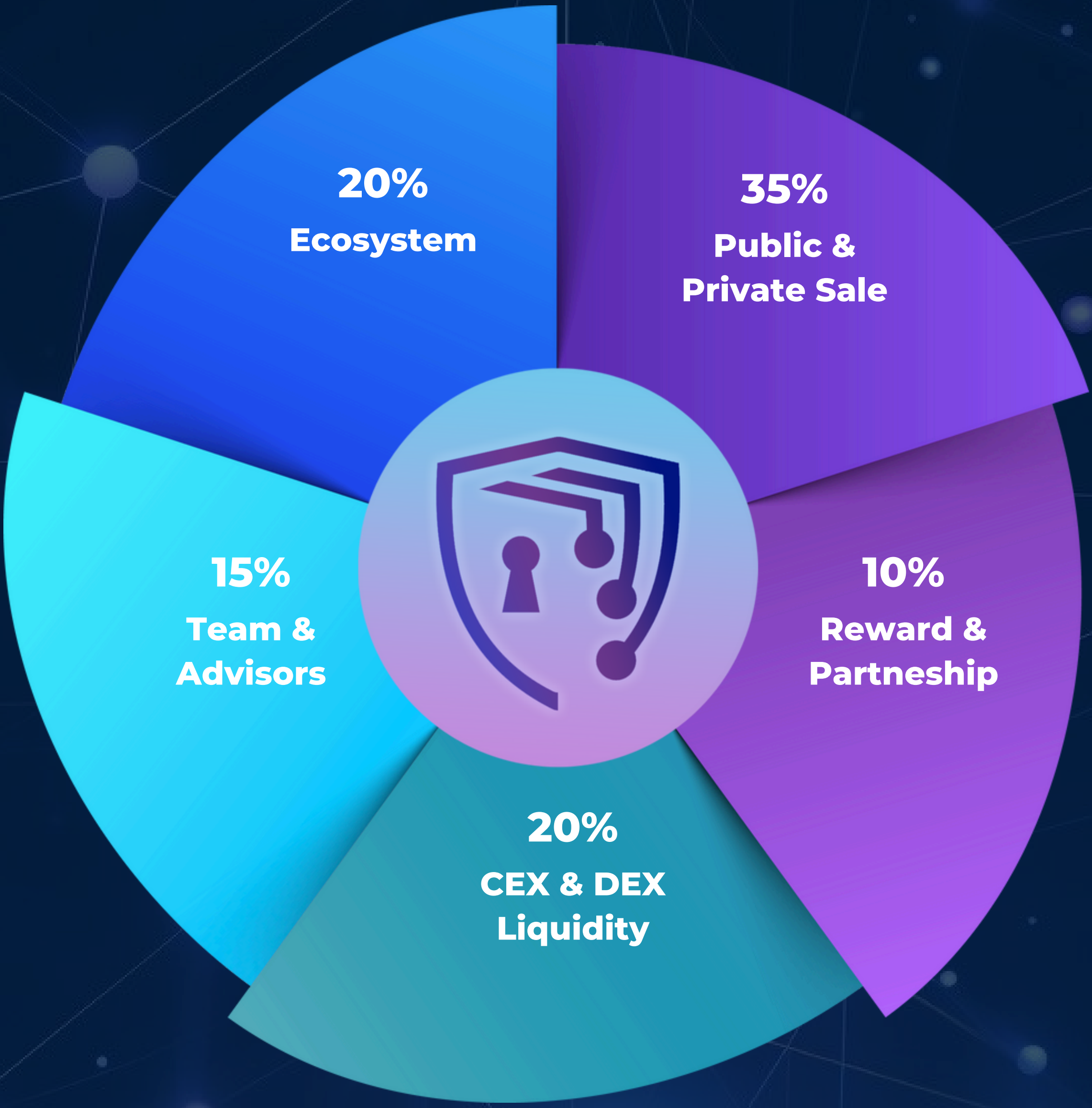
8.1 KSX TOKEN OVERVIEW

THE KSX TOKEN IS THE BACKBONE OF THE KEYSHIELDX ECOSYSTEM, DESIGNED TO POWER DECENTRALIZED SECURITY SOLUTIONS WHILE ENSURING SUSTAINABLE GROWTH AND EQUITABLE DISTRIBUTION. WITH A FIXED TOTAL SUPPLY OF 1 BILLION KSX, KEYSHIELDX INCORPORATES DEFLATIONARY MECHANISMS TO ENHANCE LONG-TERM VALUE.

KSX SERVES MULTIPLE PURPOSES, INCLUDING:

- ENHANCING WEB3 SECURITY – ACCESS TO KEYSHIELDX'S DECENTRALIZED SECURITY FEATURES.
- GOVERNANCE & DECISION-MAKING – KSX HOLDERS PARTICIPATE IN PROTOCOL UPGRADES AND SECURITY INITIATIVES.
- STAKING & INCENTIVES – REWARDS FOR SECURING THE NETWORK AND ENGAGING WITH THE ECOSYSTEM.
- ECOSYSTEM EXPANSION – INTEGRATION WITH WALLETS, DAPPS, AND DEFI PROJECTS TO DRIVE ADOPTION.
-

8.2 TOKEN ALLOCATION



KSX

- **SUPPLY & DISTRIBUTION**

TOTAL SUPPLY: 1 BILLION KSX (FIXED, WITH DEFLATIONARY MECHANISMS)

TOKEN ALLOCATION:

- ECOSYSTEM – 20% (GRANTS, SECURITY INCENTIVES, BUG BOUNTIES)
- TEAM & ADVISORS – 15% (VESTING SCHEDULE TO ENSURE LONG-TERM COMMITMENT)
- PRIVATE SALE & PUBLIC SALE – 35% (EARLY INVESTORS SUPPORTING SECURITY RESEARCH & DEVELOPMENT, PUBLIC LAUNCH, ENSURING DECENTRALIZATION)
- REWARD & PARTNERSHIP – 10% (FOR FUTURE PARTNERSHIPS,STAKING REWARD, INCENTIVES, EMERGENCY FUNDS, AND DEVELOPMENT)
- CEX &DEX LIQUIDITY – 10% (TO MAINTAIN HEALTHY TRADING VOLUME & PRICE STABILITY)

8.3 KSX TOKEN UTILITY

KSX IS MORE THAN JUST A UTILITY TOKEN—IT IS THE FOUNDATION OF WEB3 SECURITY INNOVATION. ITS USE CASES INCLUDE:

- DECENTRALIZED SECURITY – POWERING KEYSHIELDX'S MULTI-PARTY COMPUTATION (MPC) FRAMEWORK, AI-DRIVEN SECURITY AUDITS, AND ANTI-PHISHING TOOLS.
- GOVERNANCE & DECISION-MAKING – KSX HOLDERS CAN VOTE ON SECURITY PROTOCOL UPGRADES, STAKING PARAMETERS, AND ECOSYSTEM DEVELOPMENTS.
- STAKING & REWARDS – HOLDERS CAN STAKE KSX TO EARN REWARDS, PARTICIPATE IN LIQUIDITY POOLS, AND RECEIVE SECURITY INCENTIVES.
- ECOSYSTEM GROWTH – KSX FUELS PARTNERSHIPS WITH WALLETS, DAPPS, DEFI PROTOCOLS, AND INSTITUTIONAL SECURITY PROVIDERS.

BY INTEGRATING A ROBUST GOVERNANCE MODEL, STAKING INCENTIVES, AND SECURITY-DRIVEN UTILITIES, KSX ENSURES LONG-TERM ENGAGEMENT, ADOPTION, AND RESILIENCE IN THE WEB3

8.4 INITIAL DISTRIBUTION & VESTING SCHEDULE

TO MAINTAIN LONG-TERM STABILITY, PREVENT MARKET MANIPULATION, AND ENCOURAGE SUSTAINABLE GROWTH, KEYSHIELDX IMPLEMENTS A STRUCTURED DISTRIBUTION AND VESTING SCHEDULE FOR KSX TOKENS. THIS APPROACH ENSURES THAT TOKENS ARE GRADUALLY RELEASED INTO CIRCULATION, PREVENTING LARGE SELL-OFFS WHILE INCENTIVIZING LONG-TERM PARTICIPATION FROM INVESTORS, CONTRIBUTORS, AND THE COMMUNITY.

KEY HIGHLIGHTS OF THE VESTING STRATEGY INCLUDE:

- PUBLIC SALE – TOKENS ALLOCATED FOR PUBLIC SALE WILL HAVE NO VESTING PERIOD, ENSURING IMMEDIATE LIQUIDITY FOR RETAIL INVESTORS AT LAUNCH.
- PRIVATE SALE – INVESTORS IN PRIVATE ROUNDS WILL EXPERIENCE A 6-MONTH CLIFF FOLLOWED BY AN 18-MONTH LINEAR VESTING PERIOD, ENSURING A STEADY RELEASE WHILE DISCOURAGING EARLY DUMPS.
- TEAM & ADVISORS – A 12-MONTH CLIFF FOLLOWED BY A 3-YEAR LINEAR VESTING SCHEDULE PREVENTS TEAM MEMBERS AND ADVISORS FROM PREMATURELY SELLING TOKENS, ALIGNING THEIR INCENTIVES WITH THE PROJECT'S LONG-TERM SUCCESS.
- ECOSYSTEM & PARTNERSHIPS – A 6-MONTH CLIFF, FOLLOWED BY A GRADUAL RELEASE OVER 3 YEARS, ENSURES FUNDS ARE STRATEGICALLY USED FOR DEVELOPMENT, GRANTS, BUG BOUNTIES, AND EXPANSION EFFORTS.

- REWARDS & PARTNERSHIPS – TOKENS DESIGNATED FOR STAKING REWARDS AND FUTURE PARTNERSHIPS WILL BE DISTRIBUTED OVER 4 YEARS, ENSURING CONTINUED ENGAGEMENT AND SECURITY INCENTIVES.
- CEX & DEX LIQUIDITY – 50% OF LIQUIDITY TOKENS WILL BE UNLOCKED AT LAUNCH (TGE) TO MAINTAIN MARKET STABILITY, WITH THE REMAINING 50% VESTED OVER 6 MONTHS TO ENSURE HEALTHY TRADING ACTIVITY .

THIS VESTING MODEL GUARANTEES THAT EARLY SUPPORTERS, TEAM MEMBERS, AND ECOSYSTEM PARTICIPANTS REMAIN COMMITTED TO KEYSHIELDX'S LONG-TERM VISION, FOSTERING TRUST AND RESILIENCE IN THE WEB3 SECURITY ECOSYSTEM.

KEYSHIELDX ROADMAP

Q2 2025 – FOUNDATION & LAUNCH

- WHITE PAPER RELEASE & WEBSITE LAUNCH – OFFICIAL DOCUMENTATION OF KEYSHIELDX'S VISION, TECHNOLOGY, AND TOKENOMICS & INTRODUCTION OF THE KEYSHIELDX PLATFORM WITH DETAILED FEATURES AND ROADMAP
- COMMUNITY BUILDING & REWARDS– GROWING THE KEYSHIELDX COMMUNITY & COMMUNITY INCENTIVES TO DRIVE ADOPTION AND AWARENESS
- PRESALE - LAUNCHING PRESALE FOR EARLY SUPPORTERS
- EXCHANGE LISTING

Q3 2025 – EXPANSION & SECURITY SCALING

- MULTI-CHAIN PHISHING DETECTION & SCAM PREVENTION ROLLOUT
- DAO GOVERNANCE FRAMEWORK LAUNCH FOR COMMUNITY PARTICIPATION
- FIRST INSTITUTIONAL PARTNERSHIPS FOR ENTERPRISE SECURITY SOLUTIONS
- LARGE-SCALE MARKETING & ADOPTION CAMPAIGNS

Q4 2025 _ TESTNET LAUNCH

- MPC KEY PROTECTION TRIALS
- AI AUDIT TOOL TESTING IN DEFI
- PHISHING DETECTION INTEGRATION
- TESTING THE TESTNET FOR MASS ADOPTION

Q1 2026 – FULL ECOSYSTEM ROLLOUT

- AI-POWERED ON-CHAIN FRAUD DETECTION SYSTEM
- EXPANSION TO LAYER 2 & MULTI-CHAIN PROTOCOLS
- INTEGRATION WITH DEFI LENDING, STAKING, AND NFT PLATFORMS
- FIRST KEYSHIELDX SECURITY AUDIT REPORTS PUBLISHED

Q2 2026 & BEYOND – MASS ADOPTION & EVOLUTION

- GLOBAL EXPANSION WITH WEB3 SECURITY PARTNERSHIPS
- MOBILE-FIRST KEYSHIELDX APPLICATION FOR SEAMLESS SECURITY
- SDKS & APIS FOR THIRD-PARTY INTEGRATION
- FURTHER RESEARCH INTO QUANTUM-RESISTANT CRYPTOGRAPHY
- STRENGTHENING THE DAO & COMMUNITY-DRIVEN SECURITY INTELLIGENCE

CONCLUSION

KEYSHIELDX IS PIONEERING THE NEXT ERA OF WEB3 SECURITY BY INTEGRATING CUTTING-EDGE MULTI-PARTY COMPUTATION (MPC), AI-DRIVEN AUDITS, AND MULTI-CHAIN THREAT DETECTION INTO A SEAMLESS SECURITY FRAMEWORK. BY ADDRESSING THE MOST PRESSING VULNERABILITIES IN DECENTRALIZED ECOSYSTEMS: SUCH AS PRIVATE KEY MANAGEMENT, DEFI EXPLOITS, AND PHISHING THREATS. KEYSHIELDX EMPOWERS INDIVIDUALS, INSTITUTIONS, AND PROJECTS WITH TRUSTLESS AND RESILIENT SECURITY.

AS THE BLOCKCHAIN INDUSTRY EVOLVES, SECURITY WILL BE PARAMOUNT TO ENSURING MAINSTREAM ADOPTION. KEYSHIELDX IS NOT JUST A PRODUCT BUT A MOVEMENT TOWARD A SAFER, MORE TRANSPARENT, AND DECENTRALIZED FUTURE. THROUGH COMMUNITY-DRIVEN GOVERNANCE, CONTINUOUS INNOVATION, AND STRATEGIC PARTNERSHIPS, WE ARE COMMITTED TO LEVELING UP WEB3 SECURITY FOR USERS ACROSS THE GLOBE.

WITH THE KSX TOKEN AT THE CORE OF OUR ECOSYSTEM, KEYSHIELDX PROVIDES INCENTIVES FOR PARTICIPATION, REWARDS FOR SECURITY CONTRIBUTORS, AND DECENTRALIZED GOVERNANCE TO ENSURE THAT OUR PLATFORM REMAINS ADAPTIVE, SCALABLE, AND TRULY DECENTRALIZED. JOIN US IN SHAPING THE FUTURE OF WEB3 SECURITY—WHERE PROTECTION MEETS DECENTRALIZATION.

DISCLAIMER

THE INFORMATION PROVIDED IN THIS DOCUMENT IS FOR INFORMATIONAL AND EDUCATIONAL PURPOSES ONLY AND DOES NOT CONSTITUTE FINANCIAL, INVESTMENT, OR LEGAL ADVICE. KEYSHIELDX DOES NOT GUARANTEE THE SUCCESS OR PROFITABILITY OF ANY INVESTMENT RELATED TO ITS PLATFORM, PRODUCTS, OR THE KSX TOKEN. CRYPTOCURRENCY AND BLOCKCHAIN RELATED INVESTMENTS ARE HIGHLY SPECULATIVE AND CARRY INHERENT RISKS, INCLUDING BUT NOT LIMITED TO MARKET VOLATILITY, REGULATORY CHANGES, AND POTENTIAL SECURITY THREATS. USERS AND INVESTORS SHOULD CONDUCT THEIR OWN RESEARCH, DUE DILIGENCE, AND SEEK PROFESSIONAL FINANCIAL ADVICE BEFORE PARTICIPATING IN ANY ASPECT OF THE KEYSHIELDX ECOSYSTEM.

KEYSHIELDX OPERATES AS A DECENTRALIZED SECURITY SOLUTION, AND WHILE EVERY EFFORT IS MADE TO ENHANCE SECURITY, NO SYSTEM IS ENTIRELY IMMUNE TO CYBER THREATS OR UNFORESEEN VULNERABILITIES. THE TEAM WILL CONTINUOUSLY UPDATE AND IMPROVE SECURITY MEASURES; HOWEVER, USERS ARE RESPONSIBLE FOR THEIR OWN SECURITY PRACTICES, INCLUDING PROPER KEY MANAGEMENT AND VIGILANCE AGAINST SCAMS.

BY ENGAGING WITH KEYSHIELDX, ITS PRODUCTS, OR THE KSX TOKEN, YOU ACKNOWLEDGE AND ACCEPT THE RISKS INVOLVED. THE PROJECT'S ROADMAP, TOKENOMICS, AND SECURITY FEATURES ARE SUBJECT TO MODIFICATIONS BASED ON MARKET CONDITIONS, TECHNOLOGICAL ADVANCEMENTS, AND COMMUNITY GOVERNANCE DECISIONS.

STAY INFORMED. STAY SECURE. WELCOME TO KEYSHIELDX.