Fias and the Devv Ecosystem

A Strategic Integration for the Future of AI Commerce

1. Executive Overview

The convergence of artificial intelligence and blockchain technology represents one of the most significant opportunities in the digital economy. Two complementary platforms—Fias and the Devv Ecosystem—have been designed to work together, creating a unified infrastructure for AI monetization and secure digital asset exchange.

Fias is the World's Monetization Platform for AI. It operates as a standalone platform but is built using DevvX blockchain infrastructure, enabling seamless collaboration among diverse AI capabilities with transparent, instant revenue sharing. The platform treats every AI model, agent, API, or human expert as a modular Entity that can be discovered, orchestrated, and monetized automatically.

The Devv Ecosystem comprises DevvX (a high-throughput blockchain protocol), DevvE (the universal liquidity token), and a suite of financial applications including DevvExchange and DevvISE. DevvX provides the only blockchain infrastructure with comprehensive protections suitable for autonomous AI transactions—combining unprecedented speed, cost-efficiency, privacy, and security.

1.1 Two Tokens, Two Purposes

The integration of Fias and DevvX is anchored by two utility tokens, each designed for a distinct but complementary purpose:

FIAS — The Money of AI: The FIAS token powers all economic interactions within the AI monetization ecosystem. Every payment to Entities, every Arche Store transaction, and every micropayment for AI services flows through FIAS. With DevvX's ability to process millions of transactions per second at a fraction of the cost of other blockchains, FIAS enables the real-time micropayment model that AI commerce demands.

DevvE — The Money of Money: DevvE serves as the universal liquidity layer for financial transactions within the Devv Ecosystem. It enables instant exchange of any digital asset to any other—Bitcoin to stablecoins, FIAS to USD, or any token pair—with no counterparty risk and mathematically instantaneous settlement.

Symbiotic Utility: Each token drives utility for the other. As Fias grows and AI transactions increase, DevvX transaction volume grows, enhancing DevvE utility. As DevvX financial

infrastructure matures, it enables more sophisticated Fias payment flows, enhancing FIAS utility. This creates a self-reinforcing growth cycle across both platforms.

1.2 Why This Integration Matters

AI financial infrastructure will be the largest growth category for financial infrastructure in 2026 and beyond (see Appendix for supporting data). AI commerce has unique requirements that existing blockchain infrastructure cannot meet. Autonomous agents need to transact without human oversight. Micropayments must settle instantly across thousands of service providers. And most critically, transactions must be protected against the fraud, theft, and manipulation that have plagued the blockchain industry.

DevvX is the first and only blockchain to solve these challenges comprehensively. Its Contingent Transaction Sets enable trustless agent-to-agent commerce. Its protection suite—including loss protection, theft protection, and fraud protection—makes AI transactions safe for enterprise adoption. Together, Fias and DevvX provide the foundation for a new era of AI-powered finance.

2. Contingent Transaction Sets: The Engine for AI Commerce

At the heart of the Fias-DevvX integration lies a revolutionary capability: Contingent Transaction Sets (CTS). This patented technology fundamentally transforms how AI agents and services can transact, eliminating counterparty risk and enabling true machine-to-machine commerce.

2.1 Understanding Contingent Transaction Sets

A Contingent Transaction Set allows parties to create transactions with programmable conditions that are validated at the consensus level—not through smart contracts, but at the core blockchain protocol itself.

How CTS Works: Party A creates a transaction stating they will send Asset X *if and only if* they receive Asset Y. Party B creates a mirror transaction stating they will send Asset Y *if and only if* they receive Asset X. These two transactions are grouped into a set and submitted to the DevvX validators. The validators verify that all contingencies can be satisfied, and if so, both transactions execute atomically on the same block. If any contingency fails, neither transaction executes.

The result is revolutionary: two parties can exchange both assets and processing-information with no middlemen, no settlement risk, no escrow accounts, and with mathematically instantaneous settlement. The exchange either happens completely, correctly and instantly, or it doesn't happen at all.

2.2 CTS as the Foundation for AI Transactions

CTS transforms AI-to-AI (agent-to-agent) transactions, enabling autonomous commerce at scale:

Data and Compute Exchange: Agent A needs data processing from Agent B. Using CTS, Agent A creates a contingent payment that releases FIAS if and only if Agent B delivers verified output meeting defined criteria. Agent B creates a contingent delivery that provides output if and only if payment is confirmed. Both conditions are validated atomically—no escrow accounts, no intermediaries, no delayed settlement, no possibility of one party defaulting after the other has performed.

Supply Chain Automation: AI agents can manage entire supply chains autonomously. When a delivery is made, IoT devices verify receipt and condition of goods. Ownership of the physical asset (represented as a tokenized NFT) transfers to the buyer if and only if payment transfers to the seller—and both transfers occur only after IoT sensors confirm delivery specifications are met. The entire process executes atomically with full auditability.

Financial Strategy Execution: AI agents managing portfolios can execute complex rebalancing strategies involving multiple asset exchanges. An agent can atomically sell Asset A for Asset B while simultaneously exchanging Asset B for Asset C—all contingent on achieving target prices. If any leg of the strategy fails to meet criteria, the entire transaction set reverts, protecting the portfolio from partial execution risk.

Insurance Automation: AI agents can optimize insurance transactions by linking policy payouts directly to verified events. When IoT sensors confirm a covered incident (weather damage, equipment failure, delivery delay), the insurance payout executes automatically—but only if the sensor data meets cryptographic verification standards. Claims processing that once took weeks happens in seconds without many existing categories of fraud risk.

Healthcare Data Exchange: Medical AI agents can exchange health records contingent on verified proof of authorization. A specialist's AI receives patient records if and only if the patient's AI has verified the referral request and authorization token. The health data transfers atomically with the authorization proof, ensuring HIPAA-compliant exchange without centralized intermediaries.

Energy Grid Trading: AI agents managing microgrids can trade excess renewable energy in real-time. A solar array's agent sells excess capacity to a neighboring facility's agent, with payment contingent on verified power delivery measured by smart meters. Grid balancing that required human operators and day-ahead markets now happens continuously and autonomously.

Data and Intellectual Property Licensing: AI agents can license algorithms, datasets, or creative works with usage-based compensation. The IP transfers for use if and only if payment transfers, and both are contingent on cryptographic proof of the intended use case. Piracy and unauthorized use become structurally impossible.

Cross-Border Trade Compliance: AI customs agents can verify regulatory compliance, tariff calculations, and documentation before releasing goods across borders. The goods clear customs (ownership transfers) if and only if duties are paid and compliance is verified—all atomically, reducing cross-border settlement from days to seconds.

The Principle: Anytime anything needs to be assured before a financial transaction happens—or before important NFTs representing steps in a process are transferred—CTS can be used in conjunction with AI agents to dramatically reduce risk and enable full auditability. The possibilities are truly endless: manufacturing quality assurance, advertising verification, carbon credit trading, legal contract execution, real estate closings, freight logistics, and any multi-party process requiring trust. CTS transforms every industry where verification must precede value exchange.

2.3 Why CTS Transforms AI Commerce

- **Eliminates Counterparty Risk:** In autonomous systems where AI agents manage assets without human oversight, counterparty risk has been a fundamental barrier. CTS removes it entirely.
- **Enables True Machine-to-Machine Economy:** For the first time, AI agents can engage in economic transactions without requiring human approval on every exchange. This unlocks autonomous AI commerce at scale.
- **Removes Manipulation Vectors:** Front-running, MEV (Maximal Extractable Value), and other manipulation techniques that plague other blockchains are structurally prevented by CTS's atomic execution model.
- **Supports Micropayment Economics:** Fias's model requires millions of small payments to flow instantly between Entities. CTS, combined with DevvX's sub-cent transaction costs, makes this economically viable.
- **Eliminates Omnibus Wallets:** Users maintain direct control of their assets throughout the transaction process. There is no need to deposit funds with an exchange or intermediary. "Not your keys, not your crypto" is preserved even in complex multi-party transactions.

3. Security and Safety: Protecting AI Transactions

Blockchain has been too risky for traditional finance—and even more so for autonomous AI commerce. Billions of dollars are lost or stolen every year through private key compromises, exchange hacks, smart contract exploits, and fraud. For AI agents to operate autonomously with real economic value, these risks must be eliminated, not merely mitigated.

DevvX has implemented a comprehensive protection suite that, for the first time, solves blockchain's fundamental security flaws. These protections are essential for safe AI transactions.

3.1 The DevvX Protection Suite

Loss Protection: For the first time in blockchain, there is recourse for private key loss—without requiring trust in a third party. This is critical for AI systems where agent wallets may operate for extended periods. If an organization's AI agent wallet key is compromised or lost, assets are not permanently gone. This breakthrough removes private key management as the sole approach for implementing security.

Theft Protection: DevvX provides recourse for the theft of assets through an innovative approach where users can customize defined "safe use" parameters for their funds. Attackers cannot force improper use of assets, even with access to private keys or through physical coercion. Both hacking and physical force become ineffective. AI agent wallets can be configured with strict operational parameters that prevent unauthorized transfers even if the agent is compromised.

Fraud Protection (DevvProtect): Transactions can be implemented with escrow functionality at the protocol level, allowing recourse if a purchased item is not delivered or if an incorrect receiving address is used. For AI services, this means that if an Entity fails to deliver the specified output, the payment can be reversed through defined dispute resolution mechanisms.

Privacy: DevvX's globally patented privacy solution provides regulatory-compliant privacy—a critical requirement for enterprise AI workflows that may process sensitive data. Users have true privacy on their transactions and wallet holdings, but regulatory bodies can legally access required information when necessary. This is the only type of privacy solution that will ultimately thrive in regulated markets.

Bailment Protection: DevvX's management of wrapped tokens includes a revolutionary approach where DevvX itself is entirely removed from the custody process. Even in the extreme case of platform bankruptcy, users' assets remain fully protected and accessible. This addresses one of the most catastrophic risks in the crypto industry.

3.2 Why These Protections Enable Enterprise AI Adoption

Traditional financial institutions have legitimate concerns about blockchain adoption. The combination of DevvX protections directly addresses each concern:

Enterprise Concern	DevvX Solution
Key loss = permanent asset loss	Loss Protection provides trustless recovery
Hacks and theft are irreversible	Theft Protection prevents unauthorized use
Exchange/platform bankruptcy	Non-custodial CTS + Bailment Protection
Privacy vs. compliance tradeoff	Regulatory-compliant privacy (patented)
Smart contract vulnerabilities	Consensus-level contracts, not smart contracts

With these protections in place, AI agents can operate with institutional-grade security. The "blockchain is too risky" barrier to enterprise AI monetization is removed.

3.3 The IoT Security Challenge: The Missing Link for AI Agent Commerce

IoT devices represent one of the most significant security vulnerabilities in enterprise and financial systems today. As AI agents increasingly rely on IoT sensors to verify real-world conditions before executing transactions—supply chain deliveries, insurance events, energy trades, healthcare data—the integrity of these devices becomes paramount. Without verified device identity, AI agent transactions built on IoT data are built on an unstable foundation.

The scale of this challenge is staggering:

- **Attack Volume:** IoT devices face approximately 820,000 attacks daily, with threat actors increasingly targeting operational technology environments. Ransomware attacks against Operational Technology (OT) systems have surged 46% year-over-year.
- **Breach Impact:** One in three data breaches now involves an IoT device. Breaches involving IoT systems cost between $5-10 million per incident—significantly higher than traditional IT incidents. Healthcare IoT breaches average $10 million per attack.
- **Device Vulnerability:** More than 50% of IoT devices contain critical vulnerabilities that can be exploited. Most devices ship with default passwords, outdated firmware, and no native security. The average device risk score has increased 33% in just one year.
- **Scale Explosion:** The world now has over 18 billion IoT devices, projected to exceed 40 billion by 2030. Machine identities—from IoT devices to AI agents—now vastly outnumber human identities in enterprises, and most operate unseen and overprivileged.

The Core Problem: Traditional systems cannot authenticate device identity. As one security expert noted: "AI depends on trustworthy device data, but many systems cannot authenticate firmware, updates, or sensor outputs, which makes AI decisions inherently risky." Device spoofing, firmware tampering, and supply chain attacks can inject false data that AI agents trust implicitly—leading to fraudulent transactions, corrupted records, and massive financial losses.

For AI agent commerce to reach its potential, there must be cryptographic certainty that when an IoT device reports a delivery has arrived, or a meter reading has been taken, or a health metric has been recorded, that report comes from the authentic device and has not been tampered with.

3.4 DevvX IoT Device Identity: Establishing Trust at the Hardware Level

DevvX solves the IoT identity problem through Devvio's patented IoT device identity technology—a system that establishes cryptographic device identity at the hardware level and maintains an immutable record of every device interaction on the blockchain.

Hardware-Rooted Identity: Each IoT device is assigned a unique cryptographic identity that is bound to the device's hardware. This identity cannot be spoofed, cloned, or transferred. When a sensor reports data, that report is cryptographically signed with the device's unique identity, proving authenticity at the source.

Immutable Device Registry: DevvX can maintain application specific blockchain-based registries of authorized devices. When a device attempts to submit data that will trigger an AI agent transaction, the system verifies the device identity against the registry. Unauthorized devices, spoofed sensors, or tampered firmware cannot inject false data into the transaction stream.

Lifecycle Tracking: From manufacturing through deployment to decommissioning, every device's lifecycle can be recorded on-chain. Firmware updates are verified and logged. Configuration changes are tracked. Any anomaly in device behavior can be detected and flagged before it affects transactions.

Attestation Before Execution: CTS transactions can be conditioned on device attestation. Before an AI agent executes a supply chain payment based on IoT delivery confirmation, the system verifies: (1) the reporting device is authentic, (2) the device firmware is uncompromised, (3) the data transmission has not been altered, and (4) the device was authorized to report on this specific transaction. Only when all attestations pass does the CTS execute.

3.5 Auditable AI Agent Activity: Complete Transaction Provenance

The combination of verified IoT identity and blockchain-recorded AI agent activity creates something unprecedented: complete, auditable provenance for every AI-driven transaction.

Consider the full audit trail for an AI-executed supply chain transaction:

- **Device Identity Record:** Which specific IoT sensors reported delivery confirmation, with cryptographic proof of their authenticity
- **Data Integrity Record:** The exact sensor readings, timestamps, and environmental conditions at the moment of confirmation
- **Agent Decision Record:** Which AI agent processed the data, what decision logic was applied, and what action was triggered
- **Transaction Execution Record:** The complete CTS showing the atomic exchange of payment for goods, with all contingencies verified
- **Participant Identity Record:** All parties to the transaction, with privacy-preserving verification of their authorization

Enterprise Value: This level of auditability transforms AI agent commerce from a trust-based system to a verification-based system. Enterprises can deploy autonomous AI agents with confidence, knowing that every action is traceable, every data input is verified, and every transaction is auditable. Regulators can examine any transaction's complete provenance.

Disputes can be resolved with cryptographic proof. Insurance can be priced based on verified risk data rather than estimates.

The Competitive Moat: No other blockchain platform offers this combination of IoT device identity, AI agent transaction recording, and CTS atomic execution. Enterprises evaluating platforms for AI agent deployment will find that DevvX is the only infrastructure that answers the fundamental question: "How do we know this AI agent is acting on authentic data and recording its actions immutably?"

3.6 AI Agent Security: The Defining Challenge for Enterprise AI

AI agent security has emerged as one of the single biggest barriers to deploying AI at enterprise scale. As autonomous agents move from experimental pilots to production systems that execute trades, access sensitive data, and trigger operational processes, the security implications have become a board-level concern.

The scope of the challenge is unprecedented:

- **The New Insider Threat:** Palo Alto Networks identifies AI agents as "the new insider threat" for 2026. Unlike human insiders, a compromised agent never sleeps, operates at machine speed, and can "silently execute trades, delete backups, or pivot to exfiltrate the entire customer database." A single well-crafted prompt injection can turn an organization's most powerful digital employee into an adversary.
- **Unprecedented Scale:** Gartner predicts 40% of enterprise applications will integrate AI agents by end of 2026, up from less than 5% in early 2025. AI agents move 16x more data than human users—in one documented case, a single agent downloaded over 16 million files while all other users combined accessed just one million.
- **Security Gap:** Despite rapid adoption, only 34% of enterprises have AI-specific security controls in place (Cisco). A Sailpoint survey found 80% of IT professionals have witnessed AI agents acting unexpectedly or performing unauthorized actions.
- **Supply Chain Attacks:** A 2025 supply chain attack on the OpenAI plugin ecosystem compromised agent credentials from 47 enterprise deployments. Attackers used these credentials to access customer data, financial records, and proprietary code for six months before discovery.
- **Top Enterprise Priority:** KPMG's Q4 2025 AI Pulse Survey found that 75% of business leaders cite security, compliance, and auditability as the most critical requirements for agent deployment—the top priority across all surveyed concerns.

The Core Problem: Traditional security architectures were designed for human users and static applications. They cannot handle autonomous entities that reason, adapt, chain decisions across systems, and operate without direct human oversight. As one industry analysis noted: "If an agent can take action, it needs to be governed like any other identity. That means authentication, access control, policy enforcement, and auditability. Otherwise, you're giving system-level powers to something with no identity record, no accountability, and no traceability."

3.7 Blockchain Auditability: The Foundation for Secure AI Agent Operations

DevvX's blockchain architecture directly addresses the AI agent security crisis by providing immutable, cryptographically verified audit trails for every agent action. This transforms AI agents from opaque black boxes into governed, auditable systems that enterprises can deploy with confidence.

Immutable Action Records: Every action taken by an AI agent operating on DevvX is recorded on the blockchain with cryptographic proof. The agent's decision to execute a trade, transfer assets, or trigger a workflow creates a permanent, tamper-proof record. Unlike traditional logging systems that can be altered or deleted by sophisticated attackers, blockchain records are mathematically immutable.

Complete Decision Provenance: DevvX captures the full chain of causation for every agent action: what data inputs triggered the decision, what logic was applied, what external systems were consulted, and what outcome resulted. When regulators, auditors, or security teams need to understand why an agent took a specific action, the complete provenance is available on-chain.

Real-Time Anomaly Detection: Because all agent actions are recorded on-chain, DevvX can enable continuous monitoring for behavioral anomalies. An agent suddenly accessing data outside its normal scope, executing transactions at unusual times, or interacting with unauthorized systems can trigger immediate alerts. The immutable record ensures that attackers cannot cover their tracks by modifying logs.

Cryptographic Agent Identity: Each AI agent operating on DevvX can be assigned a unique cryptographic identity bound to the blockchain. This identity cannot be spoofed or transferred. When an agent takes action, its identity is cryptographically verified—ensuring that the action was taken by the authentic agent and not by an attacker using stolen credentials or impersonating a trusted system.

CTS-Enforced Boundaries: Contingent Transaction Sets can encode agent operational boundaries at the protocol level. An agent's transactions can be conditioned on staying within defined parameters: spending limits, asset types, counterparty restrictions, and time windows. If an agent attempts to exceed its boundaries—whether through compromise or malfunction—the CTS simply fails to execute. The blockchain enforces policy, not just logs violations.

Cross-Agent Accountability: In multi-agent systems where agents collaborate or delegate tasks, DevvX maintains accountability across the entire chain. If Agent A delegates work to Agent B, and Agent B triggers Agent C, the complete delegation chain is recorded. Responsibility can be traced from the final action back to the original authorization—critical for complex enterprise workflows.

The Enterprise Value Proposition: DevvX transforms the AI agent security equation. Instead of deploying agents into opaque environments where security teams cannot see what's happening, enterprises deploy into transparent, governed infrastructure where every action is

recorded, every decision is traceable, and every boundary is enforced at the protocol level. This is not incremental improvement—it is the architectural foundation that makes enterprise-scale AI agent deployment possible.

The Regulatory Imperative: As AI regulations mature globally, auditability will transition from best practice to legal requirement. Organizations deploying AI agents will need to demonstrate: what actions agents took, why those actions were taken, what data informed decisions, and what controls prevented unauthorized behavior. DevvX's blockchain-based audit trail provides this evidence automatically, continuously, and immutably—positioning Fias users ahead of regulatory requirements rather than scrambling to achieve compliance.

3.8 Data Privacy: The Other Critical Barrier to Enterprise AI Deployment

Privacy concerns represent one of the most significant obstacles to enterprise AI adoption. As AI systems require vast amounts of data to train and operate—including sensitive personal information, proprietary business data, and confidential records—organizations face a fundamental tension between AI innovation and data protection.

The scope of the privacy challenge:

- **Top Adoption Barrier:** 40% of organizations cite privacy or data confidentiality concerns as a top AI adoption challenge (IBM). For generative AI specifically, 57% of IT professionals identify data privacy as the biggest inhibitor to adoption—nearly double the 25% who cited it just one year earlier (Deloitte).
- **Erosion of Trust:** Approximately 70% of adults say they don't trust companies to use AI responsibly, and over 80% expect their personal information will be used in ways that would make them uncomfortable (Pew Research). This trust deficit makes reputational damage from privacy incidents costlier than regulatory fines.
- **Privacy Incidents Rising:** Surveys show approximately 40% of companies have already experienced an AI-related privacy event. Meanwhile, 15% of employees admit to pasting sensitive information into public AI chatbots, creating data exposure risks that traditional security cannot address.
- **Regulatory Acceleration:** Gartner forecasts that 75% of the world's population now operates under modern privacy regulation. GDPR fines have totaled €5.65 billion since 2018, with €2.3 billion in 2025 alone—a 38% year-over-year increase. The EU AI Act's full implementation in August 2026 mandates privacy-by-design for high-risk AI systems, with non-compliance triggering fines up to 7% of global annual turnover.
- **Cross-Border Complexity:** 71% of organizations cite cross-border data transfer compliance as their top regulatory challenge, reflecting the complexity of navigating fragmented global frameworks while AI systems process data across jurisdictions. Eighteen U.S. states now have active privacy laws, with more than 1,000 AI-related bills introduced across state legislatures.

The Fundamental Dilemma: Enterprises need AI systems that can process sensitive data effectively while maintaining privacy. Traditional approaches force a binary choice: either keep data completely private (limiting AI utility) or expose data to AI systems (creating privacy and compliance risk). Neither option serves enterprise needs. The privacy-enhancing technologies market is projected to grow from $3-4 billion in 2024 to $12-28 billion by 2030—reflecting urgent enterprise demand for solutions that resolve this dilemma.

3.9 DevvX Regulatory-Compliant Privacy: The Sustainable Solution

DevvX's globally patented privacy solution resolves the enterprise privacy dilemma by providing true transaction and wallet privacy while maintaining the regulatory access that compliance requires. This is not a compromise—it is the only privacy architecture that can succeed in regulated markets at scale.

Regulatory Access When Required: Unlike privacy solutions that make regulatory compliance impossible, DevvX's patented approach allows authorized regulatory bodies to access required information through proper legal channels. When regulators have legitimate need and legal authority, they can obtain necessary information—exactly as they can with traditional financial institutions. This satisfies AML, KYC, and financial reporting requirements across jurisdictions.

Why This Architecture Wins: Privacy solutions that block all access—including legitimate regulatory access—will ultimately be banned or restricted in major markets. The EU, US, UK, and other jurisdictions are actively moving to require financial transparency for anti-money-laundering and tax compliance. DevvX's approach provides the privacy enterprises need while remaining compatible with regulatory frameworks worldwide. This is not a limitation—it is the only sustainable path for enterprise-grade blockchain infrastructure.

Privacy for AI Agent Operations: For AI agents operating on Fias, privacy means that agent strategies, transaction patterns, and asset holdings remain confidential. Competitors cannot observe an agent's trading activity. Business partners cannot see the full scope of an organization's AI operations. Yet when auditors or regulators need to verify compliance, the necessary records are accessible through proper channels.

Cross-Border Compliance by Design: DevvX's privacy architecture addresses the cross-border compliance challenge that 71% of organizations cite as their top regulatory concern. Because the system supports regulatory access in any jurisdiction, organizations can operate globally without the data localization and transfer restrictions that plague other blockchain platforms. The privacy layer works consistently across borders while respecting local regulatory requirements.

Building Trust Through Transparency: As 90% of survey respondents agree, robust privacy laws make customers more comfortable sharing information with AI applications. Both Fias' and DevvX's regulatory-compliant privacy enables enterprises to make credible privacy commitments to their users—commitments backed by cryptographic enforcement rather than policy promises. This transforms privacy from a compliance burden into a competitive advantage.

The Market Reality: For enterprises evaluating blockchain infrastructure for AI deployment, Fias and DevvX combine to create the only platform that answers the fundamental question: "How do we get real privacy while remaining fully compliant?" Privacy-only solutions will face regulatory barriers. Transparency-only solutions expose competitive information. The Fias platform's approach threads this needle—positioning Fias and the DevvX ecosystem to capture enterprise demand that cannot adopt alternatives.

4. Platform Synergies and Strategic Vision

4.1 Building DevvX Applications with Fias Arches

Fias Arches serve as AI-powered development accelerators for the entire DevvX ecosystem. An Arche can decompose complex requests, coordinate multiple AI Entities, and deliver sophisticated solutions—including the creation of new DevvX applications.

Use cases for Arches in DevvX application development include:

- **Financial and Crypto Applications:** Anyone can easily create their own applications using tokens, NFTs, and the Devv Ecosystem financial infrastructure to implement their own bespoke solutions.
- **Automated Compliance:** AI Entities that monitor transactions for regulatory compliance, flagging potential issues and generating required reports.
- **Risk Assessment:** Multi-model analysis of lending positions, collateral values, and market conditions to provide real-time risk scoring.
- **Portfolio Optimization:** Arches that orchestrate specialized models for asset allocation, rebalancing, and performance analysis across Liquidity Caches.
- **Intelligent Market Making:** AI-driven strategies for DevvExchange that adapt to market conditions and optimize spread capture.

This represents the "robots building robots" approach: AI creating AI-powered financial applications, with each new capability expanding the ecosystem's value.

4.2 Financial Ecosystem Integration — Enhanced by AI

The Devv Ecosystem provides comprehensive financial infrastructure that integrates directly with Fias. AI transforms each component from functional to exceptional:

DevvExchange and DevvISE: The DevvISE liquidity provisioning system underlies DevvExchange, utilizing Liquidity Caches where both FIAS and DevvE serve as Shared Digital Assets. Contributors to Liquidity Caches share in revenue from market making, instant payments, lending, and exchange fees.

AI Enhancement: AI agents revolutionize liquidity provision and market making. Instead of static algorithms, AI-driven market makers continuously analyze order flow patterns, cross-

market correlations, and macroeconomic signals to optimize spread capture while minimizing inventory risk. AI agents can predict liquidity demands before they materialize, repositioning assets across Liquidity Caches to capture maximum fee revenue. The result: higher returns for liquidity providers, tighter spreads for traders, and improved capital efficiency across the entire exchange ecosystem.

Lending Capabilities: DevvISE's lending system operates at the consensus level rather than through smart contracts, dramatically reducing risk. Collateral remains in a borrower's account unless there is default—locked but not transferred.

AI Enhancement: AI transforms lending from a rules-based process into an intelligent, adaptive system. AI credit agents analyze on-chain behavior patterns, cross-platform activity, and real-time market conditions to assess borrower risk with unprecedented accuracy. Collateral monitoring agents continuously evaluate asset volatility and correlation risk, adjusting margin requirements dynamically rather than relying on static thresholds. Default prediction models identify stress signals early, enabling preemptive risk mitigation. For borrowers, AI agents optimize borrowing strategies—selecting optimal collateral mixes, timing loan origination to favorable rate conditions, and automatically refinancing when better terms become available.

Instant Payments: When AI services are purchased, the payment flow can utilize DevvE for instant conversion. A user pays in FIAS, which converts instantly to DevvE, then to the recipient's preferred asset—all in a single atomic CTS with no settlement delay and no counterparty risk.

AI Enhancement: AI payment routing agents optimize every transaction for cost, speed, and slippage. When converting between assets, AI analyzes liquidity depth across all available Caches, predicts short-term price movements, and executes through optimal paths—potentially splitting large transactions across multiple routes or timing execution to avoid temporary liquidity gaps. Fraud detection AI monitors transaction patterns in real-time, identifying anomalies before they complete. The combination of DevvX's instant atomic settlement with AI-optimized routing creates a payment system that is simultaneously faster, cheaper, and safer than anything previously possible.

The Compounding Effect: Each AI enhancement improves the others. Better market making attracts more liquidity, which improves payment routing, which increases transaction volume, which generates more data for AI models, which further improves market making. This creates a flywheel effect where AI-enhanced financial infrastructure continuously improves itself—the "robots building robots" principle applied to financial markets.

4.3 Driving Mutual Token Utility

The integration creates powerful network effects that compound across both platforms:

- **Fias Growth → DevvX Volume:** AI transactions on Fias are implemented as payments using DevvX transactions. As Fias scales to millions of daily micropayments, DevvX transaction volume grows proportionally, enhancing DevvE utility and network value.

- **DevvX Infrastructure → Fias Capability:** DevvX's unique protections, CTS functionality, and cost efficiency enable Fias business models and Arches that would be impossible on other blockchains. This infrastructure advantage attracts more AI developers and users to Fias.
- **Liquidity Cache Synergy:** FIAS as an SDA in Liquidity Caches means that FIAS holders can earn revenue from market making and lending while maintaining exposure to AI ecosystem growth.

4.4 Vision: DevvX as the Primary Blockchain for AI

If Fias succeeds as the global standard for AI monetization, DevvX becomes the blockchain of AI—processing potentially billions of daily transactions as AI agents and services transact autonomously worldwide.

This vision is achievable because DevvX offers capabilities no other blockchain can match:

- **Scalability:** Tens of millions of transactions per second through the T1/T2 sharding architecture.
- **Cost:** Less than 1/1,000,000th the cost of Ethereum transactions, making micropayments economically viable.
- **Protection:** The only blockchain with comprehensive loss, theft, fraud, and bailment protections.
- **CTS:** The only blockchain enabling trustless, atomic, multi-party transactions without smart contract risk.

4.5 Conclusion: A Complete Digital Economy

Fias provides the AI layer—a unified framework where any AI capability can be discovered, orchestrated, and monetized. DevvX provides the financial layer—secure, scalable, protected infrastructure for value exchange.

Together, they create something greater than either could achieve alone: a complete digital economy for artificial intelligence. An ecosystem where specialized AI contributors outcompete monolithic systems through capitalism-driven competition. Where thousands of models, agents, and human experts collaborate seamlessly with transparent, instant compensation. Where enterprises can finally adopt AI and blockchain with institutional-grade confidence.

The Money of AI meets The Money of Money. The result is the infrastructure for the next generation of AI-powered finance.

For more information:
Fias Platform: fias.io | DevvX: devv.io

Contact: Tom Anderson, Founder

Appendix: AI Financial Infrastructure — The Largest Growth Category

AI financial infrastructure will be the largest growth category for financial infrastructure in 2026 and beyond. The following data from leading market research firms and industry analysts supports this conclusion.

A.1 Market Size and Growth Rate Comparisons

AI in financial services consistently shows the highest compound annual growth rates (CAGR) among all financial infrastructure categories:

Category	CAGR	Market Size Trajectory
AI in Finance	**30.6%**	$38B (2024) → $190B (2030)
Generative AI in Financial Services	**39.1%**	$1.7B (2023) → $16B (2030)
AI in BFSI (Banking, Financial Services, Insurance)	**24%**	$43B (2024) → $299B (2033)
Overall Fintech Market	16.3%	$417B (2025) → $1.6T (2034)
Embedded Finance	~15%	$7T+ US transaction value by 2026
Payments Infrastructure	~12%	$2.4T (2023) → $3.1T (2028)

Sources: MarketsandMarkets, Grand View Research, SkyQuest, Allied Market Research, Trinetix (2024-2025)

A.2 Key Industry Data Points

MarketsandMarkets (November 2025): "The AI in Finance market is projected to grow from USD 38.36 billion in 2024 to USD 190.33 billion by 2030, at a CAGR of 30.6%, driven by the sector's shift toward AI-first operating models. Financial institutions are adopting cloud-native AI platforms, generative AI, and real-time analytics to modernize legacy systems, reduce costs, and deliver personalized services."

ResearchAndMarkets (January 2026): "The Global Artificial Intelligence (AI) in BFSI Market is projected to expand substantially, rising from USD 24.31 Billion in 2025 to USD 60.09 Billion by 2031, achieving a CAGR of 16.28%. Key drivers include the urgent need for operational efficiency and rising demand for sophisticated fraud detection systems."

NVIDIA State of AI in Financial Services (2024): "91% of financial services companies indicated they are pushing artificial intelligence innovation to improve client interactions and business operations."

JPMorgan Chase Technology Investment: "JPMorgan Chase committed to a total technology budget of $17 billion in 2024, highlighting the strategic priority of artificial intelligence and modernization to maintain market leadership."

Google Cloud ROI of AI Report (September 2025): "53% of financial services executives stated that their firms are actively employing AI agents in production to enhance risk management and drive growth, indicating a swift sector-wide pivot toward autonomous intelligence."

S&P Global (Late 2025): "43% of banks were deploying AI in internal functions like risk, compliance, and fraud prevention—while only 9% used it directly in customer-facing channels. This shows AI is becoming foundational infrastructure, not a cosmetic add-on."

A.3 2026: The Inflection Point

Multiple industry analysts identify 2026 as the year AI transitions from experimentation to enterprise-wide deployment in financial services:

FinTech Magazine (December 2025): "The 2026 trend will be a shift from AI pilots to enterprise-wide programmes. Successful firms will adopt modular AI architectures, adopt governance controls and measure outcomes through live business metrics."

BobsGuide (December 2025): "The agentic AI systems refined in 2025 will move from the back office to the front line, giving rise to Agentic Commerce. Visa and Mastercard are expected to roll out standardized frameworks to support AI-driven transactions, meaning consumers' AI agents will be empowered to browse, select, and transact on their behalf in real-time."

BDO 2026 Fintech Predictions: "Early use cases of AI are no longer enough to move the needle in financial services and many fintechs are now laying the groundwork for advanced AI use in 2026. Agentic AI differs from traditional automation because it can plan, reason, and take multi-step actions without explicit step-by-step instructions."

A.4 Why AI Outpaces Other Financial Infrastructure Categories

- **Multiple Application Domains:** Unlike payments (single function), AI touches fraud detection, risk management, compliance, customer service, trading, lending, underwriting, and more—creating compounding investment across the entire financial services value chain.
- **Compounding Investment:** 89% of financial institutions plan to increase AI spending in the next two years, according to industry surveys. This creates a sustained multi-year investment cycle.
- **Regulatory Tailwinds:** EU AI Act Phase 2 compliance requirements (August 2026), US state-level AI disclosure requirements, and DORA (Digital Operational Resilience Act) are creating mandatory infrastructure investment.
- **Agentic AI Emergence:** 2026 marks the transition from AI as an analytical tool to AI agents that can autonomously execute transactions, manage portfolios, and interact with financial systems—requiring entirely new infrastructure layers.

- **Cost Reduction Imperative:** Financial services companies spend millions annually on compliance, anti-money laundering, and fraud investigations. Agentic AI can dramatically reduce these costs, creating clear ROI that justifies infrastructure investment.

A.5 Implications for Fias and DevvX

The data confirms that AI financial infrastructure represents the largest growth opportunity in financial services. This positions the Fias-DevvX integration at the center of the fastest-growing market segment:

- **Fias provides the AI monetization layer** that enables the thousands of specialized AI models, agents, and services that financial institutions need to deploy.
- **DevvX provides the transaction infrastructure** with the speed, cost-efficiency, and protection features required for AI agent-to-agent commerce at scale.
- **Contingent Transaction Sets** enable the trustless, atomic transactions that autonomous AI agents require—a capability no other blockchain provides.

As financial institutions shift from AI pilots to enterprise-wide deployment, and as agentic AI enables autonomous financial transactions, the demand for secure, scalable AI financial infrastructure will accelerate. Fias and DevvX are positioned to capture this growth by providing the only integrated platform purpose-built for AI commerce.

A.6 Industry Leaders on AI Agents and Blockchain Payments

Leaders across the crypto, fintech, and technology industries have converged on a common vision: AI agents will coordinate and transact through blockchain-based payment rails. The following quotes from industry executives support this thesis:

Michael Novogratz — CEO, Galaxy Digital

"In the not so distant future, the biggest user of stablecoins is going to be AI. You're going to pick up your phone and say buy my groceries and your grocery agent who knows what you like to eat, knows if you're on a diet, it's gonna know which groceries to buy and from where. And they're not gonna send a wire instruction or a Venmo, they're gonna send a digital currency over a crypto rail."

— Bloomberg TV interview, Goldman Sachs Asia Leaders Conference, September 2025

Brian Armstrong — CEO, Coinbase

"x402 is a big step forward. AI agents can now transact value, not just exchange info... Agents can actually pay each other now, with x402 powering the stablecoin rail."

— X (Twitter), September 2025

Armstrong has also noted that AI agents will likely default to using stablecoins for payments because they cannot open bank accounts or pass traditional Know Your Customer (KYC) checks like humans. "The infrastructure exists, and usage is rapidly growing."

John D'Agostino — Head of Institutional Strategy, Coinbase

"If we're going to move to this world and have this wonderful advantage of these agents acting at infinitely fast speeds, they have to act on infinitely fast and scalable money rails. And that's what blockchain and crypto is."

— CNBC interview, September 2025

D'Agostino compared trying to run AI agents on traditional financial systems to "trying to stream a movie on a dial-up modem. It just doesn't work."

Jorn Lambert — Chief Product Officer, Mastercard

"2026 is when agent-native commerce goes mainstream. We'll move beyond assistants — AI agents will research, negotiate, and complete secure purchases on behalf of consumers."

— Bloomberg interview, December 2025

Sandeep Nailwal — Co-founder, Polygon

"By 2026, the internet will think, verify and move money automatically through one shared system. AI makes decisions, blockchains prove them and payments enforce them instantly — without human middlemen. 2025 will be remembered as the last year AI, payments and blockchains operated as if they were separate systems."

— Entrepreneur, December 2025

Sundar Pichai — CEO, Google/Alphabet

Responding to the Google-Coinbase partnership on the Agentic Payments Protocol (AP2), Pichai stated that "the best way to build the AI agent ecosystem is by keeping it open and collaborative." Google's AP2 protocol, built with Coinbase, enables AI agents to pay each other using stablecoins.

A.7 Market Validation: The x402 Protocol

The emergence of the x402 protocol in 2025 provides concrete evidence of the AI-blockchain payments convergence:

- **Rapid Adoption:** Technology leaders including Google Cloud, AWS, and Anthropic adopted x402 for AI agent payments.
- **Transaction Growth:** x402 logged nearly 500,000 transactions in a single week (October 2025), with a record 239,505 transactions in one day—representing 10,780% growth from four weeks earlier.
- **Industry Collaboration:** More than 60 companies, including American Express, Mastercard, PayPal, and Salesforce, are working on solutions for AI agent payments.
- **VanEck Projection:** Blockchain networks could host over one million AI agents by the end of 2025, with approximately 10,000 AI agents already earning millions of dollars weekly through blockchain activities.

A.8 Why DevvX Is Uniquely Positioned

While x402 and other protocols demonstrate the market demand for AI agent payments, DevvX offers capabilities that address the fundamental limitations these early protocols face:

- **Contingent Transaction Sets:** Unlike simple payment protocols, CTS enables complex multi-party atomic transactions where AI agents can exchange value with guaranteed execution—essential for agent-to-agent commerce where trust cannot be assumed.
- **Protection Suite:** AI agents managing wallets face the same theft and loss risks as human users. DevvX's loss protection, theft protection, and fraud protection ensure agent wallets remain secure even if compromised.
- **Consensus-Level Security:** Unlike smart contract-based systems vulnerable to exploits, DevvX's protections operate at the consensus level, eliminating entire categories of attack vectors and bringing tax strategy advantages.
- **Cost Efficiency:** At less than 1/1,000,000th the cost of Ethereum transactions, DevvX makes micropayments between AI agents economically viable at any scale.

The vision articulated by industry leaders—AI agents transacting autonomously via blockchain rails—is precisely what the Fias-DevvX integration enables, with protections and capabilities no other platform can match.

A.9 IoT Security: The Critical Challenge for AI Agent Commerce

The following statistics from industry research firms demonstrate why IoT device identity is essential for AI agent transactions (see Section 3.3):

- **Attack Frequency:** IoT devices face approximately 820,000 attacks daily (Asimily, 2025). Ransomware attacks on operational technology surged 46% year-over-year.
- **Breach Involvement:** One in three data breaches now involves an IoT device (Verizon DBIR 2024).
- **Financial Impact:** 34% of IoT breaches result in costs between $5-10 million (Forrester). Healthcare IoT breaches average $10 million per incident. Industrial sector breaches average $5.56 million.
- **Device Vulnerability:** More than 50% of IoT devices contain critical exploitable vulnerabilities (IoT Security Foundation). Average device risk scores increased 33% from 2024 to 2025 (Forescout).
- **Scale:** Over 18 billion IoT devices globally in 2025, projected to exceed 40 billion by 2030 (Statista). The IoT market reached $714 billion in 2025.
- **Identity Crisis:** "Machine identities—from workloads and service accounts to IoT devices and AI agents—now vastly outnumber human identities in the enterprise, and most operate unseen and overprivileged." (Delinea, December 2025)

- **The Trust Gap:** "AI depends on trustworthy device data, but many systems cannot authenticate firmware, updates, or sensor outputs, which makes AI decisions inherently risky." (Integrity Security Services CEO, December 2025)

DevvX's patented IoT device identity technology directly addresses these challenges, providing the cryptographic device authentication that AI agent commerce requires.

A.10 AI Agent Security: The Enterprise Deployment Barrier

The following data demonstrates why AI agent security has become one of the defining challenges for enterprise AI deployment (see Sections 3.6-3.7):

- **Enterprise Priority:** 75% of business leaders cite security, compliance, and auditability as the most critical requirements for AI agent deployment (KPMG Q4 2025 AI Pulse Survey).
- **Adoption Acceleration:** 40% of enterprise applications will integrate AI agents by end of 2026, up from <5% in early 2025 (Gartner).
- **Security Gap:** Only 34% of enterprises have AI-specific security controls in place (Cisco State of AI Security 2025).
- **Unexpected Behavior:** 80% of IT professionals have witnessed AI agents acting unexpectedly or performing unauthorized actions (Sailpoint).
- **Data Movement:** AI agents move 16x more data than human users. One documented case: a single Glean agent downloaded 16 million files while all other users combined accessed one million (Obsidian Security).
- **Attack Reality:** A 2025 supply chain attack on the OpenAI plugin ecosystem compromised 47 enterprise deployments, with attackers accessing customer data and financial records for six months undetected (Stellar Cyber).
- **The Insider Threat:** "AI agents represent the new insider threat to companies in 2026... A single well-crafted prompt injection or tool-misuse vulnerability can give adversaries an autonomous insider at their command." (Palo Alto Networks, December 2025)
- **Top Security Challenge:** "For many CISOs, agentic AI security is now one of their most significant security challenges." (CyberArk, January 2026)

DevvX's blockchain-based auditability, cryptographic agent identity, and CTS-enforced operational boundaries provide the security infrastructure that enterprise AI agent deployment requires.

A.11 Data Privacy: The Critical Barrier to Enterprise AI Adoption

The following data demonstrates why data privacy has become one of the most significant obstacles to enterprise AI deployment (see Sections 3.8-3.9):

- **Top Adoption Barrier:** 40% of organizations cite privacy or data confidentiality concerns as a top AI adoption challenge (IBM). For generative AI specifically, 57% of IT

professionals identify data privacy as the biggest inhibitor—nearly double the rate from the previous year (Deloitte).

- **Consumer Trust Deficit:** 70% of Americans don't trust companies to use AI responsibly, and 81% assume organizations will use their personal information in ways that would make them uncomfortable (Pew Research, F5).
- **Privacy Incidents:** Approximately 40% of companies have already experienced an AI-related privacy event. 15% of employees admit to pasting sensitive information into public AI chatbots (Protecto).
- **Regulatory Enforcement:** GDPR fines have totaled €5.65 billion since 2018, with €2.3 billion in 2025 alone—a 38% year-over-year increase. 75% of the world's population now operates under modern privacy regulation (Gartner, Secure Privacy).
- **Cross-Border Challenge:** 71% of organizations cite cross-border data transfer compliance as their top regulatory challenge. 18 U.S. states now have active privacy laws, with 1,000+ AI-related bills introduced across state legislatures (DPO Centre).
- **EU AI Act Impact:** Full implementation in August 2026 mandates privacy-by-design for high-risk AI systems. Non-compliance triggers fines up to 7% of global annual turnover (Secure Privacy).
- **Privacy Tech Market:** The global privacy-enhancing technologies market reached $3-4 billion in 2024, projected to grow to $12-28 billion by 2030-2034 at 19-25% CAGR, reflecting urgent enterprise demand (Secure Privacy).
- **Trust Enables Adoption:** 90% of survey respondents agree that robust privacy laws make customers more comfortable sharing information with AI applications (Secure Privacy).

DevvX's patented regulatory-compliant privacy solution provides true transaction and wallet privacy while maintaining the regulatory access that compliance requires—the only sustainable architecture for enterprise AI deployment.

Data sources and quotes compiled January 2026. Market projections reflect analyst consensus at time of publication.

FORWARD-LOOKING STATEMENTS AND IMPORTANT DISCLOSURES

This document contains forward-looking statements within the meaning of applicable securities laws. These statements relate to future events or future performance and reflect management's current expectations, assumptions, and beliefs regarding the Fias platform, DevvX blockchain, and the broader markets for artificial intelligence, blockchain technology, and digital assets. A number of the descriptions represent long term planning and capabilities.

Forward-looking statements in this document include, but are not limited to, statements regarding: projected market growth for AI financial infrastructure, AI agents, and privacy-enhancing technologies; anticipated enterprise adoption of AI agents and blockchain-based payment systems; expected regulatory developments affecting AI and digital assets; the potential capabilities and market positioning of the Fias platform and DevvX blockchain; and industry trends and analyst projections cited herein.

These forward-looking statements are based on information available as of the date of this document and involve known and unknown risks, uncertainties, and other factors that may cause actual results, performance, or achievements to differ materially from those expressed or implied. Such factors include, but are not limited to:

- Changes in regulatory environments affecting AI, blockchain, digital assets, or data privacy in any jurisdiction
- Technological developments that could affect the competitive landscape or render current approaches obsolete
- Market adoption rates for AI agents, blockchain payments, and related technologies differing from projections
- Cybersecurity threats, technological failures, or vulnerabilities not yet identified
- Changes in economic conditions, capital markets, or investor sentiment toward AI and blockchain technologies
- The ability to attract and retain users, developers, and ecosystem participants
- Competition from existing and emerging platforms, protocols, and technologies
- Risks inherent in early-stage technology development and commercialization
- Third-party research, projections, and analyst estimates proving inaccurate

The market data, industry statistics, and third-party projections cited in this document are derived from sources believed to be reliable but have not been independently verified. Such data reflects conditions as of the dates indicated and may not reflect current market conditions. Analyst projections and market forecasts are inherently uncertain and subject to revision.

No representation or warranty, express or implied, is made as to the accuracy, completeness, or fairness of the information contained herein. Readers should not place undue reliance on forward-looking statements. Devvio, Inc. and Fias Inc. and their affiliates undertake no obligation to update or revise any forward-looking statements, whether as a result of new information, future events, or otherwise, except as required by applicable law.

IMPORTANT NOTICE REGARDING DEVVE AND FIAS TOKENS

DevvE and FIAS are utility tokens designed to facilitate transactions, access services, and participate in the DevvX and Fias ecosystems, respectively. Neither DevvE nor FIAS is intended to be, nor should it be construed as, a security, investment contract, equity interest, profit-sharing arrangement, or any other form of security under the laws of the United States or any other jurisdiction. The tokens are not registered under the Securities Act of 1933, as amended, nor under any state securities laws, nor under the securities laws of any foreign jurisdiction, and there is no intention to register them as such.

This document does not constitute: (a) an offer to sell or a solicitation of an offer to buy any securities; (b) an offer to sell or solicitation of an offer to buy DevvE or FIAS tokens in any jurisdiction where such offer or solicitation would be unlawful; (c) investment, legal, tax, or financial advice of any kind; or (d) a recommendation to purchase, hold, or sell any tokens or digital assets.

DevvE and FIAS tokens: (i) do not represent any ownership interest, equity stake, or voting rights in Devvio, Inc., Fias Inc., or any affiliated entity; (ii) do not entitle holders to dividends, profit distributions, or any share of revenues or earnings; (iii) do not represent a debt obligation or promise of repayment; (iv) are not redeemable at the option of the holder for cash or other assets; and (v) confer no rights beyond those expressly set forth in the applicable token documentation and platform terms of service.

The value of DevvE and FIAS tokens, if any, may fluctuate significantly and may decline to zero. Past performance is not indicative of future results. There is no guarantee that any market or liquidity will exist for these tokens, nor any assurance that tokens will be listed on any exchange or trading platform. Any acquisition of tokens involves substantial risk, including the risk of complete loss.

GEOGRAPHIC AND REGULATORY RESTRICTIONS

This document is not directed at, and the tokens described herein are not intended for, distribution to or use by any person or entity in any jurisdiction or country where such distribution or use would be contrary to applicable law or

regulation, or where Devvio, Inc. or Fias Inc., or their affiliates would be subject to any registration, licensing, or authorization requirement.
The regulatory status of blockchain technology, digital assets, and token-based systems varies substantially across jurisdictions and remains unsettled in many regions. Laws and regulations applicable to digital assets are evolving rapidly and may change in ways that adversely affect the DevvX and Fias ecosystems, the utility of DevvE and FIAS tokens, and the rights of token holders. No assurance can be given that current interpretations of applicable laws will not change or that new laws or regulations will not be enacted that could materially and adversely affect the tokens, the platforms, or their users.
Recipients of this document are responsible for determining their own legal and regulatory obligations related to digital assets in their respective jurisdictions. Neither Devvio, Inc. nor Fias Inc., nor any of their affiliates makes any representation regarding the legality of acquiring, holding, or using DevvE or FIAS tokens in any jurisdiction.

NO INVESTMENT ADVICE
This document is for informational purposes only. Nothing contained herein shall be construed as investment, legal, tax, accounting, or financial advice. You should consult your own legal, financial, tax, and other professional advisors before making any decision to acquire, hold, or dispose of any digital assets or tokens. Any investment decision should be made based solely on your own independent due diligence and assessment of your individual circumstances, risk tolerance, and investment objectives.
Devvio, Inc., Fias Inc., and their affiliates expressly disclaim any fiduciary duty to any recipient of this document. No attorney-client, advisor-client, or other professional relationship is created by the distribution of this document or any communication related thereto.