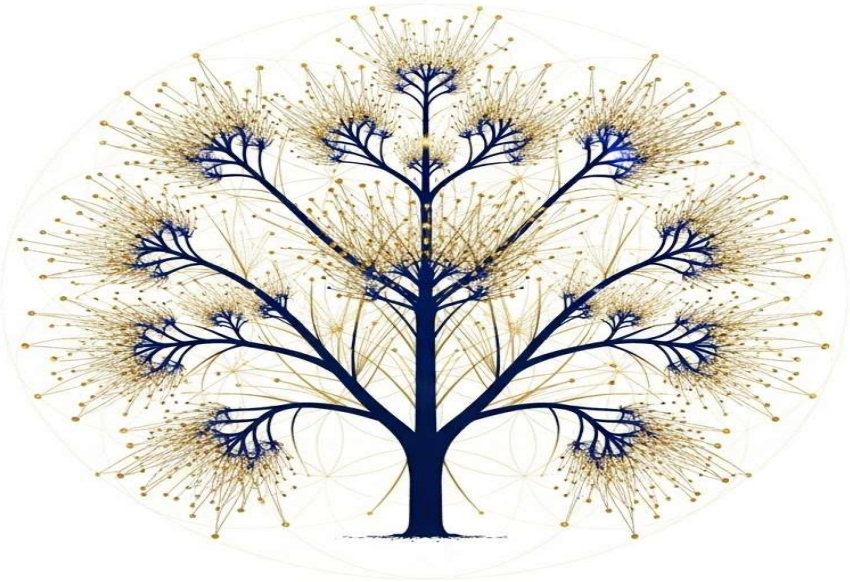
# Tokenized Municipal Instruments Under Distributed Ledger Technology: A Regulatory Sandbox Framework for Market Modernization

This concept paper presents a comprehensive sandbox framework for efficient municipal capital formation, combining automated compliance with democratic governance safeguards. It establishes a resilient architecture that reduces the cost of capital for issuers and enhances settlement certainty, strictly adhering to federal securities laws and MSRB regulations.

**Submission to the U.S. Securities and Exchange Commission (SEC)**

**Date**: November 30, 2025



"*A strategic blueprint for modernizing municipal capital formation, combining automated fiscal transparency with permissioned ledger integrity under a supervised regulatory sandbox.*"

# Tokenized Municipal Instruments Under Distributed Ledger Technology: A Regulatory Sandbox Framework for Market Modernization

**Submitted to:**
U.S. Securities and Exchange Commission
Strategic Hub for Innovation and Financial Technology (FinHub)
100 F Street, NE
Washington, DC 20549

**Submission Date:** November 30, 2025

---

## COVER LETTER

To the Commissioners and Staff of the U.S. Securities and Exchange Commission:

We respectfully submit this Concept Paper and formal request for participation in a regulatory pilot program under the auspices of the Commission's Strategic Hub for Innovation and Financial Technology. This proposal seeks to establish a structured, time-limited sandbox framework for the issuance and settlement of tokenized municipal securities utilizing enterprise-grade distributed ledger technology within a comprehensively regulated environment.

The proposed pilot program is designed to operate under a no-action framework, whereby participating municipal issuers, registered broker-dealers, qualified institutional custodians, and accredited investors may engage in limited-scale transactions involving digitally native representations of traditional municipal debt instruments. The pilot seeks to demonstrate that distributed ledger infrastructure can coexist with, and enhance, existing market frameworks while maintaining full compliance with federal securities laws, Municipal Securities Rulemaking Board regulations, and established investor protection standards.

This submission is motivated by three fundamental objectives: first, to reduce operational friction and settlement risk in municipal debt markets through programmable settlement infrastructure; second, to expand access to municipal finance for mid-sized jurisdictions that face disproportionate issuance costs under current intermediation models; and third, to provide the Commission with empirical data regarding the integration of distributed ledger architecture with traditional custody, clearing, and disclosure frameworks.

We believe this proposal aligns with recent developments in Commission policy, including Chairman Paul Atkins' Project Crypto initiative and the Commission's token taxonomy framework announced in November 2025. The pilot builds upon successful real-world implementations, notably the City of Quincy, Massachusetts' blockchain-based municipal bond issuance facilitated by

JPMorgan Chase in April 2024, which demonstrated institutional viability and attracted investment from BlackRock's iShares Short Maturity Municipal Bond Active ETF.

The pilot is designed as a collaborative engagement with regulatory authorities, providing comprehensive audit trails, structured reporting mechanisms, and clearly defined exit protocols to ensure that investor protection remains paramount throughout the experiment.

We stand ready to engage with FinHub staff to refine this proposal, address technical questions, and demonstrate our commitment to operating within the existing regulatory perimeter while testing carefully designed enhancements to market infrastructure.

We appreciate the Commission's consideration of this application and welcome the opportunity to contribute to the thoughtful evolution of capital formation mechanisms in the digital era.

Respectfully submitted,

Daniel Bruno Corvelo Costa

---

# Table of Contents

**SECTION I: EXECUTIVE SUMMARY & PUBLIC INTEREST JUSTIFICATION**

1.1 Overview and Objectives

1.2 Alignment with Commission Priorities

1.3 Investor Protection and Market Integrity

1.4 Scope and Scale of the Pilot

1.5 Public Interest Benefits

**SECTION II: ARCHITECTURE OF THE TRUSTED MUNICIPAL PROTOCOL**

2.1 Design Principles and Foundational Philosophy

2.2 Technical Infrastructure Specification and Platform Selection

2.3 Post-Quantum Cryptographic Security Architecture

2.4 Identity Verification and Know-Your-Customer Framework

2.5 Oracle Architecture for External Data Integration

2.6 Custodial Architecture and Cryptographic Key Management

2.7 Asset Structure and Legal Framework

2.8 Dual-Mode Settlement Engine

2.9 Payment Infrastructure and Cash Settlement

**SECTION III: LEGAL AND RISK FRAMEWORK**

3.1 The Master Indenture as Legal Wrapper

3.2 Investor Protection Through Programmable Use of Proceeds

3.3 Securities Law Compliance and Registration Framework

3.4 Municipal Securities Rulemaking Board Compliance

3.5 Operational Risk Management and Cybersecurity

**SECTION IV: GOVERNANCE DESIGN & EMERGENCY PROTOCOLS**

4.1 The Emergency Override Mechanism: Design Philosophy

4.2 Authorization and Activation Parameters

4.3 Transparency, Disclosure, and Audit Trail Requirements

4.4 Remediation and Recovery Procedures

4.5 Governance Evolution and Stakeholder Participation

**SECTION V: PILOT PARAMETERS AND IMPLEMENTATION FRAMEWORK**

5.1 Scale, Duration, and Participation Criteria

5.2 Municipal Issuer Selection and Onboarding

5.3 Broker-Dealer and Bank Participation Framework

5.4 Reporting and Performance Evaluation Metrics

5.5 Sunset Provisions and Exit Strategies

**APPENDIX A: MARKET PRECEDENTS AND LESSONS LEARNED**

**APPENDIX B: POST-QUANTUM CRYPTOGRAPHY TECHNICAL SPECIFICATIONS**

**APPENDIX C: SAMPLE MASTER INDENTURE PROVISIONS**

**APPENDIX D: ILLUSTRATIVE MUNICIPAL JURISDICTIONS AND USE CASES**

**APPENDIX E: EXECUTIVE SUMMARY AND PRACTICAL USE CASE**

**APPENDIX F: ENHANCED OPERATIONAL FRAMEWORKS**

**APPENDIX G: STRATEGIC ENHANCEMENTS FOR REGULATORY ROBUSTNESS**

**CONCLUSION**

**REFERENCES AND FUNDAMENTAL STANDARDS**

# GLOSSARY OF KEY TERMS

**Atomic Settlement** A settlement mechanism where the transfer of securities and the corresponding payment occur simultaneously in a single, indivisible transaction. Within the pilot, this eliminates counterparty risk by ensuring that neither leg of the trade can execute without the other.

**Digital Twin** The operational status of the Tokenized Security on the distributed ledger. It functions as a digital representation of the legal obligation established in the Master Indenture, providing automation for payments and recordkeeping without superseding the underlying legal contract.

**Dual-Mode Settlement Engine** A proprietary settlement architecture designed for the pilot that supports two concurrent operation modes: (1) **Atomic Settlement** for instantaneous T+0 execution, and (2) **Netted Settlement** for compatibility with traditional clearing cycles (T+1) preferred by certain institutional intermediaries.

**Emergency Override Protocol** A governance mechanism embedded in the smart contract layer that allows authorized municipal officials, via multi-signature authentication, to pause, reverse, or modify automated operations during force majeure events, national security emergencies, or material technical errors.

**General Obligation Bond (GO)** A long-term municipal debt instrument backed by the full faith and credit and taxing power of the issuing municipality. In the pilot, these are tokenized to automate interest payments and principal repayment upon maturity.

**Hardware Security Module (HSM)** A physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. The pilot requires HSMs certified to FIPS 140-3 Level 3 standards for generating and storing private keys controlling custody wallets.

**Master Indenture** The supreme legal contract executed between the Issuer and the Trustee. It governs the substantive rights and obligations of all parties. In the event of a discrepancy between the blockchain record and the Master Indenture, the Indenture prevails (the "Legal Wrapper" principle).

**ML-DSA (Module-Lattice-Based Digital Signature Algorithm)** A quantum-resistant digital signature algorithm standardized by NIST (FIPS 204). The pilot utilizes ML-DSA-65 and ML-DSA-87 for signing transactions and creating immutable audit trails that remain secure against future quantum computing attacks.

**ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)** A quantum-resistant key encapsulation mechanism standardized by NIST (FIPS 203). It is used in the pilot to establish secure communication channels between validator nodes.

**Municipal Securities Rulemaking Board (MSRB)** The self-regulatory organization (SRO) that adopts rules governing broker-dealers and banks in the municipal securities market. The pilot

operates in full compliance with MSRB rules, including G-17 (Fair Dealing) and G-34 (CUSIP/NIIDS).

**Permissioned Distributed Ledger** An enterprise-grade blockchain infrastructure where network access is restricted to authorized entities. Unlike public blockchains, validation nodes are operated exclusively by regulated financial institutions (banks) subject to rigorous technical standards.

**Revenue Anticipation Note (RAN)** A short-term municipal debt security (maturity of 12 months or less) secured by anticipated specific revenue streams. In the pilot, smart contracts validate that the use of proceeds from RANs aligns with authorized purposes.

**Smart Contract** Self-executing computer code deployed on the distributed ledger that automates the operational terms of the Master Indenture, such as payment distribution and compliance checks. It is treated as an operational tool, not an autonomous legal authority.

**Tokenized Security** A digital asset representing a traditional municipal debt instrument recorded on a distributed ledger. Under the Project Crypto taxonomy and SEC guidance, it is classified unambiguously as a security subject to federal securities laws.

**Validator Node** A server operated by a participating bank or infrastructure provider that verifies transactions, participates in consensus, and maintains a copy of the distributed ledger. Validators must meet federal banking supervision standards.

**Zero-Knowledge Proof (ZKP)** A cryptographic method used in the pilot's privacy architecture to prove the validity of a transaction (e.g., that a buyer has sufficient funds) without revealing sensitive underlying data (e.g., the account balance) to the public network.

# Tokenized Municipal Instruments Under Distributed Ledger Technology: A Regulatory Sandbox Framework for Market Modernization

**Submitted to:** U.S. Securities and Exchange Commission

**Submission Date:** November 30, 2025

---

## SECTION I: EXECUTIVE SUMMARY & PUBLIC INTEREST JUSTIFICATION

### 1.1 Overview and Objectives

This Concept Paper proposes a time-limited regulatory pilot program to evaluate the operational, legal, and economic implications of issuing municipal securities on enterprise-grade, permissioned distributed ledger infrastructure. The pilot seeks to demonstrate that distributed ledger technology, when deployed within a comprehensively regulated framework, can reduce settlement risk, lower transaction costs, enhance transparency, and broaden access to municipal debt markets without compromising investor protection or displacing existing market participants.

The proposal envisions a structured sandbox environment in which participating municipalities issue tokenized representations of traditional municipal instruments—specifically Revenue Anticipation Notes and General Obligation Bonds—to qualified investors through registered broker-dealers acting as placement agents and custodians. These digitally native securities would operate under a dual legal framework: a traditional Master Indenture governing the legal rights and obligations of all parties, and a programmable settlement layer automating compliance, payment distribution, and use-of-proceeds validation.

**Market Precedent and Proven Viability:** This proposal builds upon the successful real-world implementation by the City of Quincy, Massachusetts, which in April 2024 issued approximately ten million dollars in tax-exempt seven-year municipal bonds using JPMorgan Chase's Onyx (Kinexys) blockchain platform. This groundbreaking transaction, which marked the first U.S. municipal bond issuance, settlement, and ownership recording entirely on distributed ledger technology, demonstrated institutional viability when BlackRock's iShares Short Maturity Municipal Bond Active ETF purchased $6.5 million of the issuance in December 2024. The Quincy precedent validates the technical feasibility, regulatory compliance pathway, and institutional investor appetite for tokenized municipal securities.

The pilot is designed to preserve and enhance the roles of incumbent financial intermediaries. Banks participate as on-chain validators, identity verification providers, and qualified custodians. Broker-dealers serve as token distributors, secondary market liquidity providers, and compliance

nodes. Transfer agents maintain master securityholder files utilizing distributed ledger technology as the official record-keeping substrate, subject to existing regulatory oversight under Exchange Act rules. This intermediary-friendly architecture ensures that distributed ledger technology functions as an additive operational layer rather than a disruptive replacement of established market infrastructure.

The proposal addresses three critical public interest objectives. First, it seeks to reduce operational inefficiency in municipal debt issuance, particularly for mid-sized jurisdictions that currently face disproportionate underwriting costs and limited access to capital markets. Second, it aims to demonstrate programmable compliance mechanisms that automate adherence to use-of-proceeds restrictions, disclosure obligations, and investor suitability requirements, thereby reducing regulatory burden while enhancing transparency. Third, it provides the Commission with empirical data regarding the integration of distributed ledger architecture with traditional custody frameworks, settlement protocols, and legal documentation structures.

## 1.2 Alignment with Commission Priorities

This pilot program is directly aligned with the Commission's statutory mandate to facilitate capital formation, maintain fair and orderly markets, and protect investors. The proposal responds to the Commission's ongoing efforts to evaluate emerging technologies in securities markets while ensuring that innovation occurs within the parameters of existing investor protection frameworks.

**Alignment with Project Crypto:** This proposal explicitly aligns with Chairman Paul Atkins' Project Crypto initiative and the Commission's token taxonomy framework announced in November 2025. Under this framework, tokenized securities representing traditional financial instruments—such as the municipal debt instruments proposed herein—are unambiguously classified as securities subject to the full scope of federal securities laws. The proposal embraces this classification and operates entirely within existing regulatory boundaries.

Recent statements from Commission leadership have emphasized the importance of pilot-driven regulatory experimentation as a mechanism for gathering empirical evidence regarding new market structures. The Division of Corporation Finance's April 2025 statement on "Offerings and Registrations of Securities in the Crypto Asset Markets" clarified that blockchain-based tokenization does not alter the nature of underlying securities or diminish disclosure obligations. This pilot operates consistent with that guidance, treating tokenized municipal instruments as securities subject to comprehensive regulatory oversight.

The proposed framework provides the Commission with a controlled environment to observe how distributed ledger technology interacts with existing custody requirements under Exchange Act Rule 15c3-3, disclosure obligations under Securities Act registration or exemption frameworks, and fair dealing standards under Municipal Securities Rulemaking Board Rule G-17.

The pilot is designed to complement the Commission's renewed focus on innovation and capital formation efficiency. By demonstrating that distributed ledger infrastructure can operate within existing regulatory boundaries while reducing settlement risk and operational costs, the pilot provides data-driven insights that may inform future policy deliberations regarding market modernization initiatives.

Importantly, this proposal does not seek regulatory forbearance, exemptions from core investor protection standards, or the creation of novel legal classifications for digital assets. Rather, it operates entirely within the existing securities regulatory framework, treating tokenized municipal instruments as securities subject to the full scope of federal and self-regulatory organization rules. The distributed ledger serves purely as an operational substrate for settlement, recordkeeping, and compliance automation, not as a mechanism to circumvent established regulatory requirements.

## 1.3 Investor Protection and Market Integrity

The pilot framework incorporates multiple layers of investor protection designed to exceed baseline regulatory requirements. Participation is limited to qualified institutional buyers and accredited investors who meet enhanced due diligence standards, ensuring that only sophisticated market participants engage with the pilot during its initial phase. All investors undergo comprehensive know-your-customer and anti-money laundering verification through participating broker-dealers and bank custodians, with identity credentials cryptographically linked to on-chain addresses but maintained in secure off-chain databases compliant with data protection standards.

All tokenized securities issued within the pilot are backed by traditional Master Indenture agreements that establish the legally binding rights and obligations of issuers, investors, and intermediaries. The distributed ledger records serve as operational settlement infrastructure but do not replace or supersede the legal force of the underlying contracts. In the event of any discrepancy between on-chain records and the Master Indenture, the traditional legal instrument prevails, ensuring that established legal principles and judicial remedies remain fully applicable.

The pilot incorporates a governance safety valve in the form of an Emergency Override Protocol, accessible exclusively to duly authorized municipal officials through secure, multi-signature authentication mechanisms. This protocol enables elected officials to pause, reverse, or modify smart contract operations in circumstances involving force majeure events, national security considerations, budgetary emergencies, or material errors in contract execution. All override actions are logged on an immutable audit trail, disclosed to investors in real time, and subject to ex-post review by municipal auditors and bond counsel, ensuring transparency and accountability for any interventions in automated processes.

Settlement risk is minimized through atomic delivery-versus-payment mechanisms that eliminate the temporal gap between securities transfer and cash settlement. However, recognizing that institutional participants may prefer compatibility with existing clearing workflows, the architecture includes a dual-mode settlement engine that supports both instantaneous on-chain settlement and optional net settlement through traditional clearing arrangements. This flexibility ensures that broker-dealers can integrate tokenized securities into existing custody and clearing infrastructure without requiring wholesale operational restructuring.

## 1.4 Scope and Scale of the Pilot

The pilot is intentionally designed as a limited-scale experiment to enable rigorous evaluation of operational performance, regulatory compliance, and market impact without introducing systemic risk. Total issuance volume across all participating municipalities is capped at ten million dollars in aggregate principal amount, with individual issuances limited to a maximum of two million dollars.

This sizing ensures that the pilot remains sufficiently modest to avoid material impact on broader municipal debt markets while providing adequate transaction volume to generate meaningful empirical data.

The pilot duration is proposed as twelve to eighteen months from the date of first issuance, with quarterly reporting to FinHub staff regarding operational metrics, compliance incidents, investor feedback, and technological performance. At the conclusion of the pilot period, a comprehensive assessment will be prepared for Commission consideration, including recommendations regarding potential expansion, modification, or termination of the program based on observed outcomes.

Participation is limited to a defined cohort of market participants selected through a transparent application process. Municipal issuers include mid-sized jurisdictions across diverse U.S. states that have expressed willingness to engage in innovative finance structures while maintaining rigorous adherence to disclosure and fiduciary standards. Participating broker-dealers include registered firms with established public finance practices and demonstrated commitment to regulatory compliance. Bank custodians include federally chartered or state-supervised institutions with existing municipal securities custody capabilities and technical capacity to operate distributed ledger validation nodes.

The pilot operates on a voluntary opt-in basis for all participants. No municipality, broker-dealer, bank, or investor is obligated to engage with tokenized securities, and traditional municipal debt issuance pathways remain fully available throughout the pilot period. This voluntary structure ensures that the experiment does not create market distortions or compel participation by entities lacking technical readiness or institutional appetite for innovation.

## 1.5 Public Interest Benefits

The pilot offers several potential benefits to municipal issuers, investors, and the broader public interest. For municipal issuers, particularly mid-sized jurisdictions that face disproportionate issuance costs under traditional underwriting models, tokenized securities may reduce underwriting spreads, legal documentation expenses, and ongoing administrative burdens through programmable compliance and automated disclosure mechanisms. Enhanced transparency regarding use of proceeds may strengthen public trust in municipal finance and reduce the incidence of funds misallocation or misuse.

For investors, tokenized securities offer the potential for enhanced liquidity through fractional ownership structures and continuous secondary market access, expanding participation opportunities beyond institutional buyers to include a broader base of qualified individual investors. Automated interest payment distribution and transparent on-chain transaction records reduce operational friction and provide real-time visibility into portfolio holdings and cash flows.

For the financial services industry, the pilot provides an opportunity to evaluate distributed ledger integration with existing custody, clearing, and compliance infrastructure without displacing incumbent intermediaries. By demonstrating that banks and broker-dealers can function as on-chain validators and compliance nodes, the pilot illustrates a pathway for technological modernization that leverages existing regulatory relationships and trust frameworks rather than disintermediating established market participants.

For regulatory authorities, the pilot generates empirical data regarding the operational performance, compliance efficacy, and risk characteristics of distributed ledger-based securities settlement. This data informs future policy deliberations regarding market structure evolution, custody standards for digitally native securities, and the interaction between programmable settlement infrastructure and traditional legal frameworks.

For the public, enhanced transparency in municipal finance may strengthen accountability mechanisms, reduce the cost of capital for essential public infrastructure projects, and broaden participation in community investment opportunities. Programmable use-of-proceeds validation ensures that taxpayer-backed borrowing finances the intended public purposes, reducing opportunities for misallocation and enhancing the efficiency of public capital deployment.

---

# SECTION II: ARCHITECTURE OF THE TRUSTED MUNICIPAL PROTOCOL

## 2.1 Design Principles and Foundational Philosophy

The architecture of the Trusted Municipal Protocol is grounded in three foundational design principles: regulatory primacy, operational continuity, and institutional compatibility. These principles guide every technical and operational decision within the framework, ensuring that distributed ledger technology functions as an enhancement to existing market infrastructure rather than a replacement or circumvention of established regulatory frameworks.

**Regulatory Primacy** means that all aspects of the protocol operate within the boundaries of existing securities law, self-regulatory organization rules, and municipal finance regulations. The distributed ledger serves exclusively as an operational substrate for settlement, recordkeeping, and compliance automation. It does not create new legal classifications for securities, does not purport to replace traditional legal instruments, and does not seek exemptions from investor protection standards. The Master Indenture remains the legally binding contract governing the rights and obligations of all parties, with the distributed ledger providing operational efficiency rather than legal authority.

**Operational Continuity** means that the protocol is designed to coexist seamlessly with existing custody, clearing, and settlement infrastructure. Participating broker-dealers and bank custodians can integrate tokenized securities into their current operational workflows without requiring wholesale restructuring of back-office systems. The dual-mode settlement engine ensures compatibility with both instantaneous on-chain settlement and traditional net settlement processes, allowing intermediaries to choose the operational model that best fits their institutional capabilities and risk management frameworks.

**Institutional Compatibility** means that the protocol preserves and enhances the roles of incumbent financial intermediaries rather than disintermediating them. Banks function as on-chain validators, identity verification providers, and qualified custodians, leveraging their existing regulatory relationships and trust frameworks. Broker-dealers serve as token distributors, secondary market liquidity providers, and compliance nodes, maintaining their traditional functions as intermediaries

between issuers and investors. Transfer agents utilize distributed ledger technology as the official master securityholder file, subject to existing regulatory oversight under Exchange Act rules.

## 2.2 Technical Infrastructure Specification and Platform Selection

The Trusted Municipal Protocol operates on enterprise-grade, permissioned distributed ledger infrastructure designed specifically for regulated financial applications. Based on evaluation of current institutional implementations and regulatory precedents, the pilot proposes utilizing infrastructure architecturally similar to **JPMorgan Chase's Onyx Digital Assets platform** (formerly known as JPM Coin and rebranded as Kinexys), which successfully facilitated the City of Quincy's municipal bond issuance in April 2024.

**Platform Architecture:** The distributed ledger infrastructure implements a permissioned blockchain architecture built on principles similar to Hyperledger Besu or enterprise Ethereum variants, optimized for financial institution requirements including:

- **Consensus Mechanism:** Byzantine Fault Tolerant consensus algorithms (such as Istanbul BFT or QBFT) that provide transaction finality, ensuring that confirmed transactions cannot be reversed and enabling real-time settlement with certainty. These consensus mechanisms tolerate up to one-third of validator nodes experiencing failures or malicious behavior while maintaining network integrity.
- **Network Topology:** Permissioned validator network comprising participating financial institutions (banks and designated infrastructure providers), each operating validation nodes subject to rigorous technical and operational standards. Validator participation requires federal banking charter or equivalent regulatory supervision, ensuring institutional accountability.
- **Smart Contract Environment:** Support for institutional-grade smart contract execution using Solidity or similar programming languages, with comprehensive development, testing, audit, and deployment procedures. Smart contracts governing tokenized securities undergo formal verification using automated analysis tools and independent third-party security audits prior to production deployment.
- **Privacy Architecture:** Transaction privacy mechanisms utilizing zero-knowledge proofs or secure multi-party computation to enable transaction validation without exposing sensitive commercial information. Account balances, transaction amounts, and pricing details remain confidential to authorized parties while enabling network-wide consensus on transaction validity.

**Alternative Platform Considerations:** While the pilot proposes JPMorgan Onyx-equivalent architecture as the primary implementation, the framework remains technologically neutral and could accommodate alternative enterprise blockchain platforms demonstrating equivalent capabilities, including:

- **R3 Corda 5.x Enterprise:** Flow-based architecture optimized for financial agreements, with point-to-point transaction privacy and integration with existing banking systems

- **Hyperledger Fabric 2.5+:** Modular architecture supporting pluggable consensus and fine-grained access controls for enterprise deployments
- **Quorum (ConsenSys):** Enterprise Ethereum variant with enhanced privacy and permissioning features

The selection criteria prioritize regulatory compliance capability, institutional adoption precedent, operational reliability, cryptographic security standards, and integration compatibility with existing market infrastructure.

## 2.3 Post-Quantum Cryptographic Security Architecture

Recognizing the long-term security requirements of municipal debt instruments—which may have maturities extending multiple years—and anticipating the emergence of cryptographically relevant quantum computers within the next decade, the Trusted Municipal Protocol incorporates quantum-resistant cryptographic mechanisms aligned with National Institute of Standards and Technology (NIST) post-quantum cryptography standards.

**NIST PQC Standards Integration:** In August 2024, NIST published the first three finalized post-quantum cryptography standards (FIPS 203, 204, and 205), with a fourth standard (HQC) selected for standardization in March 2025 and expected to be finalized by 2027. The pilot framework integrates these quantum-resistant algorithms to ensure long-term cryptographic security:

**FIPS 203 - ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism):** Derived from CRYSTALS-Kyber, ML-KEM provides quantum-resistant key encapsulation for establishing secure communication channels between network participants. The protocol utilizes ML-KEM for:

- Initial key exchange when establishing TLS connections between validator nodes
- Encrypting sensitive data elements in off-chain databases
- Secure communication channels for multi-signature authorization workflows

**FIPS 204 - ML-DSA (Module-Lattice-Based Digital Signature Algorithm):** Derived from CRYSTALS-Dilithium, ML-DSA provides quantum-resistant digital signatures. The protocol utilizes ML-DSA for:

- Signing transaction submissions and smart contract invocations
- Authenticating validator node identities and authorization credentials
- Creating immutable audit trail records with quantum-resistant integrity protection

**FIPS 205 - SLH-DSA (Stateless Hash-Based Digital Signature Algorithm):** Derived from SPHINCS+, SLH-DSA provides an alternative quantum-resistant signature scheme based on different mathematical foundations. The protocol maintains SLH-DSA capability as a backup signature mechanism to ensure cryptographic diversity.

**Hybrid Cryptographic Approach:** During the transition period while post-quantum cryptography implementations mature and undergo real-world testing, the pilot implements a hybrid approach combining traditional elliptic curve cryptography (ECDSA, ECDH) with post-quantum algorithms. This hybrid strategy ensures:

- Security against both classical and quantum computational attacks
- Backward compatibility with existing infrastructure during migration

- Cryptographic agility enabling algorithm updates as standards evolve

**Timeline Alignment with NIST Transition Guidance:** NIST Internal Report 8547 (November 2024) recommends transitioning cryptographic systems away from quantum-vulnerable algorithms by 2035, based on expectations regarding quantum computer development timelines. The pilot framework implements post-quantum cryptography from inception, positioning municipal securities issued during the pilot period with enhanced long-term security appropriate for debt instruments that may remain outstanding for multiple years.

This proactive integration of post-quantum cryptography demonstrates institutional sophistication, addresses legitimate long-term security concerns, and aligns with federal government cybersecurity preparedness initiatives outlined in National Security Memorandum 10 (NSM-10).

## 2.4 Identity Verification and Know-Your-Customer Framework

The identity layer of the Trusted Municipal Protocol operates through a multi-tiered architecture that separates on-chain pseudonymity from off-chain identity verification, ensuring compliance with know-your-customer and anti-money laundering requirements while maintaining operational efficiency and data privacy protections.

All investors participating in the pilot undergo comprehensive identity verification through participating broker-dealers or bank custodians before receiving authorization to transact in tokenized securities. This verification process adheres to existing customer identification program requirements under the Bank Secrecy Act and implements enhanced due diligence standards appropriate for qualified institutional buyers and accredited investors.

Verified identity credentials are maintained in secure off-chain databases controlled by the verifying intermediary, subject to applicable data protection regulations and industry best practices for safeguarding personally identifiable information. Each verified investor receives a unique cryptographic address on the distributed ledger, linked to their verified off-chain identity through secure mapping maintained by the intermediary. This address functions as a pseudonymous identifier for on-chain transactions, enabling settlement and recordkeeping without exposing personally identifiable information on the public ledger.

The separation of on-chain pseudonymity from off-chain identity ensures compliance with privacy regulations while maintaining full traceability for regulatory oversight and law enforcement purposes.

Participating banks function as identity anchors within the protocol, providing attestation services that cryptographically certify the completion of know-your-customer verification without disclosing the underlying identity information. When an investor initiates a transaction, the distributed ledger verifies that the associated cryptographic address has been attested by an authorized bank validator, confirming that appropriate due diligence has been completed. This architecture enables automated compliance verification while preserving the confidentiality of investor identity information and maintaining regulatory oversight through traditional intermediary relationships.

Transfer restrictions embedded in the tokenized securities smart contracts ensure that securities can only be transferred to addresses that have received valid attestation from authorized validators. This

programmable restriction prevents unauthorized secondary market transactions and ensures that all investors, whether in primary or secondary markets, have undergone appropriate verification before acquiring securities. The restriction mechanism operates automatically at the protocol level, eliminating the need for manual compliance checks while maintaining full adherence to transfer eligibility requirements.

## 2.5 Oracle Architecture for External Data Integration

Tokenized municipal securities require integration with external data sources for various operational functions including price discovery, credit ratings, financial reporting, and compliance monitoring. The Trusted Municipal Protocol implements a secure oracle network architecture to ingest off-chain data while maintaining integrity, accuracy, and tamper-resistance.

**Oracle Network Design:** The protocol utilizes a decentralized oracle network comprising multiple independent data providers, each cryptographically attesting to the accuracy of information submitted to the smart contract layer. Critical data elements including:

- **Interest Rate Benchmarks:** Municipal Market Data (MMD) yield curves, Securities Industry and Financial Markets Association (SIFMA) swap index, or other relevant benchmarks for floating-rate securities
- **Credit Ratings:** Moody's Ratings, S&P Global Ratings, or Fitch Ratings assessments, following the proof-of-concept demonstrated by Moody's and Alphaledger in June 2025 for embedding credit ratings into tokenized securities on the Solana blockchain
- **Issuer Financial Data:** Audited financial statements, budget reports, and continuing disclosure filings submitted to the Municipal Securities Rulemaking Board's Electronic Municipal Market Access (EMMA) system
- **Payment Events:** Confirmation of revenue collections, tax receipts, or other cash flows securing the municipal obligations

**Data Validation Mechanisms:** Multiple oracle providers submit data independently, with smart contracts implementing consensus mechanisms requiring agreement among a supermajority of providers before accepting data as authoritative. Discrepancies trigger alerts to the trustee and regulatory authorities for investigation. Data provenance is recorded on the immutable audit trail, enabling ex-post verification of information sources and validation procedures.

**Integration with EMMA:** The protocol implements automated data feeds from the Municipal Securities Rulemaking Board's EMMA system, enabling real-time ingestion of continuing disclosure documents, material event notices, and financial statements. This integration ensures that on-chain records reflect current issuer disclosure while maintaining compatibility with existing reporting infrastructure.

## 2.6 Custodial Architecture and Cryptographic Key Management

The custodial architecture is designed to satisfy possession and control requirements under Exchange Act Rule 15c3-3 while leveraging distributed ledger technology to enhance operational efficiency and transparency. Participating broker-dealers maintain custody of customer fully paid and excess margin securities either through direct control of cryptographic private keys or through qualified custodian arrangements with participating banks.

**Hardware Security Module (HSM) Implementation:** Private keys controlling custody wallets are generated and stored in Hardware Security Modules certified to Federal Information Processing Standards Publication 140-3 Level 3 or higher, ensuring that key material is protected against unauthorized access, extraction, or tampering. HSMs implement tamper-evident physical security mechanisms, role-based access controls, and comprehensive audit logging of all cryptographic operations.

**Multi-Party Computation and Threshold Signatures:** Critical custody operations implement threshold signature schemes utilizing Shamir's Secret Sharing or similar cryptographic techniques, requiring authorization from multiple designated parties before transactions can execute. For example, a three-of-five threshold scheme requires approval from three out of five authorized custodians before securities transfers can proceed, eliminating single points of failure and reducing insider threat risks.

**Cold Storage and Hot Wallet Segregation:** Long-term custody assets are maintained in offline cold storage wallets, with private keys generated in air-gapped environments and stored in geographically distributed secure facilities. Only working capital necessary for daily operational needs is maintained in online hot wallets connected to the distributed ledger network, minimizing exposure to cybersecurity threats while maintaining operational efficiency for routine transactions.

**Custodian Banking Supervision:** Bank custodians operating validation nodes and providing custody services are subject to comprehensive regulatory oversight by federal banking supervisors including the Office of the Comptroller of the Currency, Federal Reserve System, or Federal Deposit Insurance Corporation. Regular safety and soundness examinations assess the adequacy of custody controls, cybersecurity measures, and risk management frameworks, ensuring that digital asset custody meets or exceeds standards applicable to traditional securities custody.

## 2.7 Asset Structure and Legal Framework

Tokenized securities within the pilot program are structured as digital representations of traditional municipal debt instruments, specifically Revenue Anticipation Notes and General Obligation Bonds. These instruments are not novel asset classes or unregistered securities; rather, they are conventional municipal securities issued pursuant to existing legal frameworks and represented in digital form on a distributed ledger substrate.

Each issuance is governed by a Master Indenture, a traditional legal contract executed between the issuing municipality and a duly appointed trustee, establishing the rights and obligations of the issuer, investors, and intermediaries. The Master Indenture specifies the principal amount, interest rate, maturity date, payment schedule, use-of-proceeds restrictions, representations and warranties, covenants, events of default, and remedies available to investors. This legal instrument is enforceable under established contract law principles and subject to judicial interpretation and enforcement through traditional court systems.

The distributed ledger token serves as a digital twin of the Master Indenture, providing operational infrastructure for settlement, payment distribution, and compliance monitoring. The token does not replace or supersede the legal force of the Master Indenture; rather, it automates the operational execution of contractual obligations while the traditional legal instrument governs the substantive

rights and remedies of the parties. In the event of any discrepancy between on-chain records and the Master Indenture, the traditional legal instrument prevails, ensuring that established legal principles and judicial remedies remain fully applicable.

The Master Indenture explicitly defines the relationship between the legal contract and the digital representation, clarifying that ownership of the token constitutes evidence of beneficial ownership of the underlying security as recorded in the Master Indenture. The indenture specifies that transfers of the token on the distributed ledger constitute valid transfers of beneficial ownership, subject to transfer restrictions and compliance requirements embedded in the smart contract. This explicit legal framework ensures that the digital representation operates within established securities law principles governing transfer of ownership, beneficial ownership rights, and enforcement of security interests.

**Revenue Anticipation Notes** issued within the pilot represent short-term borrowing secured by anticipated revenue streams from specific municipal operations, such as tax receipts, utility payments, or fee collections. These notes are structured with maturities of twelve months or less, consistent with traditional municipal short-term borrowing practices. The use-of-proceeds restrictions are encoded in the smart contract, ensuring that borrowed funds are deployed exclusively for the designated purposes and providing real-time transparency regarding fund utilization.

**General Obligation Bonds** issued within the pilot represent long-term borrowing backed by the full faith and credit of the issuing municipality, secured by its general taxing authority. These bonds may be structured with maturities extending to several years, consistent with traditional municipal capital financing practices. The programmable settlement infrastructure automates semiannual interest payments and ultimate principal repayment upon maturity, reducing administrative burden while ensuring timely and accurate payment distribution to investors.

## 2.8 Dual-Mode Settlement Engine

The settlement architecture incorporates a dual-mode engine designed to accommodate both instantaneous atomic settlement on the distributed ledger and traditional net settlement through existing clearing arrangements. This flexibility ensures compatibility with diverse operational preferences among participating intermediaries while demonstrating the technical feasibility of near-instantaneous settlement for securities transactions.

**Atomic Settlement Mode:** The atomic settlement mode operates through delivery-versus-payment mechanisms that cryptographically link the transfer of securities and cash on the distributed ledger, ensuring that both legs of the transaction execute simultaneously and irreversibly. When an investor purchases tokenized securities, the protocol verifies the availability of both the securities in the seller's address and the cash or cash-equivalent digital currency in the buyer's address before executing the transaction. Upon verification, the securities and cash transfer simultaneously in a single atomic operation, eliminating counterparty risk and settlement failure.

This atomic settlement capability enables real-time secondary market transactions with near-zero settlement risk, a significant improvement over traditional two-day or next-day settlement cycles. Investors gain immediate beneficial ownership of purchased securities and immediate liquidity from

sold securities, enhancing market efficiency and reducing capital requirements for broker-dealers maintaining inventory for market-making purposes.

**Netted Settlement Mode:** The netted settlement mode accommodates institutional participants that prefer to integrate tokenized securities into existing clearing and settlement workflows. Under this mode, participating broker-dealers aggregate transactions over a defined settlement cycle and submit net positions to a designated clearing agent for settlement through traditional payment and securities movement mechanisms. The distributed ledger records provisional transactions during the settlement cycle and finalizes ownership transfers upon receipt of settlement confirmation from the clearing agent.

This dual-mode architecture ensures that tokenized securities can operate within the existing infrastructure of the Depository Trust and Clearing Corporation (DTCC) and other registered clearing agencies while simultaneously demonstrating the technical feasibility of instantaneous settlement. Broker-dealers may elect to utilize atomic settlement for certain transactions and netted settlement for others, providing operational flexibility and enabling gradual migration toward more efficient settlement protocols as institutional readiness and risk management frameworks evolve.

**Settlement Fail-Safes:** The settlement engine incorporates comprehensive fail-safe mechanisms to ensure that transactions cannot execute unless all preconditions are satisfied. These preconditions include verification of investor identity attestation, confirmation of transfer eligibility under embedded restrictions, validation of payment instrument authenticity, and verification of sufficient balances in both securities and cash accounts. If any precondition fails, the transaction is rejected automatically at the protocol level, preventing partial execution and ensuring that settlement occurs only when all requirements are fully satisfied.

## 2.9 Payment Infrastructure and Cash Settlement

Cash settlement for tokenized securities transactions operates through multiple pathways designed to accommodate diverse operational preferences while maintaining compatibility with existing payment systems and banking infrastructure. The pilot supports settlement using traditional wire transfers, automated clearinghouse payments, and optionally, fiat-referenced digital currency instruments issued by participating banks.

**Traditional Wire Transfer Model:** Under the traditional wire transfer model, cash settlement occurs through standard banking channels coordinated with securities transfer on the distributed ledger. When an investor purchases tokenized securities, the buyer initiates a wire transfer to the seller's designated bank account, providing transaction reference information that enables the distributed ledger to verify payment completion. Upon confirmation of cash receipt by the designated custodian or settlement agent, the securities transfer executes on the distributed ledger, completing the delivery-versus-payment settlement cycle.

**Automated Clearinghouse Model:** Under the automated clearinghouse model, settlement occurs through batch payment processing coordinated with end-of-day securities position reconciliation. This model accommodates broker-dealers that prefer to net cash movements across multiple transactions and settle on a consolidated basis through existing automated clearinghouse relationships. The distributed ledger records provisional securities transfers during the trading day

and finalizes ownership positions upon receipt of settlement confirmation from the automated clearinghouse operator.

**Fiat-Referenced Digital Currency Model:** Under the digital currency model, participating banks may issue fiat-referenced digital currency tokens representing claims on traditional bank deposits, enabling instantaneous cash settlement synchronized with securities transfer on the distributed ledger. These digital currency instruments are not novel cryptocurrencies or speculative assets; rather, they are digital representations of traditional bank deposit claims, fully backed by reserves maintained at the issuing bank and subject to federal banking supervision.

The digital currency tokens operate on the same distributed ledger infrastructure as the tokenized securities, enabling atomic delivery-versus-payment settlement through smart contract logic that simultaneously transfers securities and cash in a single irreversible operation. The issuing bank maintains reserves equal to or exceeding the outstanding digital currency token balance, ensuring full redeemability at par value upon demand. Token holders may redeem digital currency for traditional bank deposits at any time through the issuing bank, maintaining liquidity and ensuring that digital currency instruments function as perfect substitutes for conventional payment mechanisms.

All payment mechanisms operate within existing anti-money laundering and know-your-customer frameworks, with participating banks and broker-dealers implementing transaction monitoring, suspicious activity reporting, and compliance with Office of Foreign Assets Control sanctions screening requirements. The distributed ledger provides enhanced transparency for regulatory oversight, with all cash and securities movements recorded on an immutable audit trail accessible to authorized supervisory authorities.

---

# SECTION III: LEGAL AND RISK FRAMEWORK

## 3.1 The Master Indenture as Legal Wrapper

The legal architecture of the pilot program is founded upon the principle that traditional legal instruments govern the substantive rights and obligations of all parties, with distributed ledger technology serving exclusively as operational infrastructure. This principle is operationalized through the Master Indenture, a comprehensive legal contract executed in accordance with established municipal finance law and enforceable through traditional judicial mechanisms.

The Master Indenture establishes the issuing municipality as the obligor on the securities, specifies the principal amount and interest rate, defines the payment schedule and maturity date, identifies the designated revenue sources or taxing authority securing the obligation, and articulates the use-of-proceeds restrictions governing the deployment of borrowed funds. The indenture incorporates standard representations, warranties, and covenants consistent with conventional municipal securities documentation, including financial reporting obligations, limitations on additional indebtedness, maintenance of pledged revenues or taxing capacity, and compliance with applicable state and federal law.

The indenture appoints a duly qualified trustee to represent the interests of investors, enforce compliance with indenture covenants, and exercise remedies in the event of issuer default. The trustee is typically a bank or trust company with established expertise in municipal securities administration and fiduciary obligations to investors. The trustee monitors issuer compliance, receives and disburses payments on behalf of investors, maintains records of beneficial ownership, and initiates enforcement proceedings when necessary to protect investor interests.

Critically, the Master Indenture explicitly addresses the relationship between the traditional legal contract and the distributed ledger representation. The indenture specifies that the tokenized security constitutes a digital twin of the legal obligation, providing operational infrastructure for settlement and payment but deriving its legal force exclusively from the underlying contract. The indenture clarifies that ownership of the token constitutes evidence of beneficial ownership under the indenture, subject to the terms and conditions specified in the legal document.

The indenture establishes a hierarchy of authority in the event of any discrepancy between on-chain records and the provisions of the legal contract. The Master Indenture prevails in all circumstances, ensuring that traditional legal principles govern the interpretation of rights and obligations. If a smart contract error results in incorrect payment distribution or unauthorized transfer, the remedies available to aggrieved parties flow from the Master Indenture and applicable law, not from the smart contract code. This hierarchy ensures that established legal frameworks and judicial oversight remain fully applicable to tokenized securities.

The indenture incorporates specific provisions addressing force majeure events, technological failures, and emergency interventions by authorized municipal officials. These provisions authorize the trustee or designated municipal officials to override smart contract operations when necessary to protect investor interests, respond to emergencies, or correct material errors. All such interventions are subject to disclosure requirements, audit trail documentation, and ex-post review by bond counsel and municipal auditors, ensuring transparency and accountability for any deviations from automated processes.

## 3.2 Investor Protection Through Programmable Use of Proceeds

A central feature of the pilot program is the implementation of programmable use-of-proceeds validation, designed to ensure that borrowed funds are deployed exclusively for the purposes specified in the Master Indenture and disclosed to investors at the time of issuance. This mechanism enhances investor protection by reducing the risk of funds misallocation, strengthens public accountability for municipal borrowing, and demonstrates the potential for smart contract technology to automate compliance with contractual restrictions.

The use-of-proceeds framework operates through designated spending accounts controlled by multi-signature authorization requirements involving the issuing municipality, the indenture trustee, and optionally an independent fiscal monitor or project auditor. When the municipality seeks to disburse borrowed funds for authorized purposes, the designated officials submit a disbursement request specifying the purpose, amount, and recipient. The smart contract verifies that the requested disbursement complies with the use-of-proceeds restrictions specified in the Master Indenture before authorizing the transaction.

Authorized uses of proceeds are encoded in the smart contract at the time of issuance, reflecting the representations made to investors in the offering documents. For Revenue Anticipation Notes, authorized uses typically include funding operating expenses during periods of revenue timing mismatch, maintaining liquidity reserves, or financing specific capital expenditures pending receipt of dedicated revenue streams. For General Obligation Bonds, authorized uses typically include infrastructure construction, equipment acquisition, public facility renovation, or refinancing of existing debt obligations.

Each disbursement of borrowed funds is recorded on the distributed ledger, creating a permanent and immutable audit trail documenting the deployment of proceeds. This audit trail is accessible to investors, the indenture trustee, municipal auditors, regulatory authorities, and potentially the general public, providing unprecedented transparency regarding the use of taxpayer-backed borrowing. The transparency mechanism enhances accountability, reduces opportunities for misallocation or misuse of funds, and strengthens public trust in municipal finance operations.

The programmable use-of-proceeds mechanism does not eliminate the need for traditional oversight by the indenture trustee, municipal auditors, or regulatory authorities. Rather, it provides an additional layer of automated compliance verification that complements existing oversight mechanisms. The trustee retains the authority to review disbursement requests, investigate suspected violations of use-of-proceeds restrictions, and exercise remedies under the Master Indenture if unauthorized disbursements occur. Municipal auditors retain the authority to conduct financial statement audits and assess compliance with debt covenants and use-of-proceeds restrictions.

In the event that unauthorized disbursements occur due to smart contract errors, collusion among authorized signatories, or other failures of the automated system, traditional legal remedies remain fully available. Investors may seek enforcement through the indenture trustee, pursue claims against the municipality or other responsible parties, and invoke judicial oversight to compel compliance or obtain damages. The programmable mechanism enhances compliance but does not replace the legal framework governing investor rights and remedies.

## 3.3 Securities Law Compliance and Registration Framework

All tokenized securities issued within the pilot program are subject to the full scope of federal securities laws, including registration requirements under the Securities Act of 1933 or qualification for exemption therefrom, and ongoing reporting obligations under the Securities Exchange Act of 1934 to the extent applicable. The distributed ledger representation does not alter the characterization of these instruments as securities, does not create novel exemptions from registration or reporting requirements, and does not diminish the applicability of antifraud provisions or investor protection standards.

For municipal securities issued within the pilot, the issuing municipality relies upon the exemption from Securities Act registration provided under Section 3(a)(2), which exempts securities issued by states, municipalities, and political subdivisions thereof. This exemption applies regardless of whether the securities are represented in physical certificate form or as digital tokens on a distributed ledger. The exemption does not relieve the issuer of obligations under antifraud

provisions or municipal securities disclosure requirements established by the Municipal Securities Rulemaking Board.

**Alignment with Division of Corporation Finance Guidance:** The pilot operates consistent with the Division of Corporation Finance's April 2025 statement on "Offerings and Registrations of Securities in the Crypto Asset Markets," which clarified that the method of offering securities—whether through blockchain, smart contracts, or tokenized structures—does not alter underlying legal obligations. The statement emphasized that distributors of tokenized securities must comply with registration, prospectus delivery, and ongoing disclosure requirements applicable to the underlying securities. The pilot framework ensures full compliance with these obligations.

**Project Crypto Taxonomy Consistency:** Under Chairman Paul Atkins' Project Crypto taxonomy framework announced in November 2025, the tokenized municipal instruments proposed herein fall unambiguously within the category of "tokenized securities"—digital assets representing traditional financial instruments that remain subject to comprehensive securities regulation. The framework explicitly stated that "tokenized securities are and will continue to be securities under the federal securities laws." The pilot embraces this classification and operates within the regulatory boundaries appropriate for securities offerings.

Participating broker-dealers comply with Municipal Securities Rulemaking Board rules governing municipal securities transactions, including Rule G-17 requirements for fair dealing with issuers and investors, Rule G-32 requirements for disclosure document delivery, and Rule G-34 requirements for continuing disclosure submissions. Broker-dealers implement comprehensive supervisory procedures to ensure that tokenized securities transactions adhere to the same standards applicable to traditional municipal securities, including suitability determinations, markup disclosure, and confirmation delivery requirements.

The pilot incorporates enhanced disclosure mechanisms designed to ensure that investors receive comprehensive information regarding the structure, risks, and characteristics of tokenized securities. Offering documents include detailed descriptions of the distributed ledger technology, custody arrangements, settlement mechanics, smart contract functionality, Emergency Override Protocol, and potential technological risks. Investors receive clear explanations of the relationship between the Master Indenture and the digital representation, ensuring that they understand the legal framework governing their rights and remedies.

Ongoing disclosure obligations are satisfied through traditional filing mechanisms as well as enhanced real-time transparency provided by the distributed ledger. Issuing municipalities submit continuing disclosure documents to the Municipal Securities Rulemaking Board's Electronic Municipal Market Access system consistent with existing requirements. Additionally, the distributed ledger provides real-time visibility into payment performance, use-of-proceeds deployment, and compliance with indenture covenants, enabling investors to monitor issuer performance on a continuous basis rather than relying exclusively on periodic disclosure filings.

The pilot operates under the supervision of FinHub staff, with participating entities providing regular reporting regarding compliance with securities laws, operational incidents, investor complaints, and technological performance metrics. This supervisory framework ensures that the

Commission maintains visibility into pilot operations and can intervene if investor protection concerns arise or compliance deficiencies are identified.

## 3.4 Municipal Securities Rulemaking Board Compliance

The pilot program operates in full compliance with Municipal Securities Rulemaking Board rules governing dealer conduct, disclosure obligations, and fiduciary responsibilities to municipal issuers. Participating broker-dealers implement comprehensive compliance programs addressing the unique characteristics of tokenized securities while maintaining adherence to established regulatory standards.

Under Rule G-17, participating broker-dealers owe duties of fair dealing to both municipal issuers and investors. In their capacity as underwriters or placement agents for tokenized securities, broker-dealers provide comprehensive disclosure to issuing municipalities regarding the structure, costs, risks, and alternatives to distributed ledger-based issuance. Broker-dealers clarify their role as commercial counterparties with financial interests that may differ from those of the issuer, disclose all material conflicts of interest, and refrain from recommending that issuers avoid retaining independent municipal advisors.

Broker-dealers provide detailed disclosure regarding the material financial characteristics and known risks of tokenized securities when recommending this financing structure to municipalities. These disclosures address technological risks including smart contract vulnerabilities, cybersecurity threats, operational dependencies on distributed ledger infrastructure, and potential limitations on secondary market liquidity during the pilot phase. Broker-dealers also disclose the experimental nature of the pilot, the possibility of technological failures or unforeseen complications, and the importance of obtaining independent legal and financial advice before proceeding with issuance.

In their capacity as intermediaries between issuers and investors, broker-dealers comply with fair dealing obligations to investors under Rule G-17. Broker-dealers provide comprehensive disclosure regarding the structure and risks of tokenized securities, ensure that recommendations are suitable in light of investor sophistication and risk tolerance, and apply fair pricing standards to primary issuance and secondary market transactions. Broker-dealers implement supervisory procedures to monitor compliance with these obligations and to identify potential conflicts of interest or unfair practices.

Under Rule G-32, participating broker-dealers deliver official statements and other offering documents to investors at or prior to the time of trade confirmation, ensuring that investors receive material information necessary to make informed investment decisions. The official statement includes comprehensive disclosure regarding the distributed ledger technology, custody arrangements, settlement mechanics, smart contract functionality, and potential risks. Broker-dealers maintain systems to track document delivery and to ensure that all investors receive required disclosures in a timely manner.

Under Rule G-34, issuing municipalities and participating broker-dealers comply with continuing disclosure obligations by submitting material event notices, annual financial statements, and other required documents to the Municipal Securities Rulemaking Board's Electronic Municipal Market Access system. The distributed ledger provides enhanced real-time transparency complementing

traditional periodic disclosure, enabling investors to monitor issuer performance and compliance with indenture covenants on a continuous basis.

## 3.5 Operational Risk Management and Cybersecurity

The pilot program incorporates comprehensive operational risk management and cybersecurity protocols designed to protect investor assets, ensure system reliability, and maintain the integrity of the distributed ledger infrastructure. Participating entities implement controls addressing technological vulnerabilities, operational dependencies, business continuity planning, and incident response procedures.

Distributed ledger infrastructure operates on enterprise-grade, permissioned blockchain platforms compliant with National Institute of Standards and Technology cybersecurity standards and subject to regular independent security audits. The permissioned architecture restricts network access to authorized validator nodes operated by participating banks and designated infrastructure providers, preventing unauthorized parties from interfering with network operations or compromising data integrity.

Smart contracts governing tokenized securities undergo rigorous testing and formal verification prior to deployment, utilizing automated testing frameworks, manual code review by independent security auditors, and formal mathematical verification techniques to identify potential vulnerabilities or unintended behaviors. Contracts are deployed on test networks and subjected to simulated attack scenarios before production deployment, ensuring that potential security flaws are identified and remediated prior to live operation.

Cryptographic key management protocols implement industry best practices for secure key generation, storage, and operational use. Private keys controlling custody wallets are generated in hardware security modules certified to Federal Information Processing Standards Publication 140-3 Level 3 or equivalent standards, ensuring that key material is protected against unauthorized access or extraction. Multi-signature authorization requirements prevent single points of failure and ensure that critical operations require approval from multiple authorized parties.

Offline cold storage mechanisms protect long-term holdings from online cybersecurity threats by maintaining the majority of custody assets in wallets not connected to internet-accessible systems. Only working capital necessary for daily operational needs is maintained in online hot wallets, reducing exposure to potential cyberattacks or unauthorized access attempts. Regular reconciliation procedures ensure consistency between cold storage holdings and on-chain custody records.

Business continuity and disaster recovery planning addresses potential scenarios including distributed ledger network outages, smart contract failures, custodian system disruptions, and other operational incidents. Participating entities maintain comprehensive incident response procedures, redundant infrastructure components, and tested recovery protocols to ensure rapid restoration of operations following disruptions. Regular testing exercises validate the effectiveness of continuity plans and identify opportunities for improvement.

Cybersecurity incident reporting protocols ensure that material security events are promptly disclosed to FinHub staff, impacted investors, and relevant self-regulatory organizations. Participating entities maintain comprehensive incident logs documenting the nature, scope, and

remediation of security events, enabling regulatory oversight and continuous improvement of security controls.

---

# SECTION IV: GOVERNANCE DESIGN & EMERGENCY PROTOCOLS

## 4.1 The Emergency Override Mechanism: Design Philosophy

The Emergency Override Protocol represents a critical governance innovation designed to address a fundamental tension in programmable securities infrastructure: the need to balance automated execution efficiency with human oversight and accountability. While smart contracts provide operational benefits through deterministic execution and elimination of intermediary discretion, they also introduce rigidity that may prove problematic in extraordinary circumstances requiring rapid intervention by accountable authorities.

The Emergency Override Protocol resolves this tension by providing elected municipal officials with a transparent, auditable mechanism to pause, reverse, or modify smart contract operations when circumstances justify extraordinary intervention. This capability ensures that political accountability and human judgment retain ultimate authority over automated systems, while comprehensive logging and disclosure requirements ensure that override actions remain subject to public scrutiny and ex-post review.

The design philosophy recognizes that smart contracts are operational tools, not autonomous legal authorities. The Master Indenture governs the substantive rights and obligations of parties, with smart contracts automating the execution of contractual terms under normal circumstances. When extraordinary circumstances arise, human authorities acting under legal frameworks established in the Master Indenture and applicable law retain the authority to intervene in automated processes to protect investor interests, respond to emergencies, or correct material errors.

The Emergency Override Protocol is deliberately designed to be used sparingly and under narrowly defined circumstances. Casual or frequent override actions would undermine investor confidence in the reliability of smart contract execution and diminish the operational benefits of programmable infrastructure. Accordingly, the protocol establishes high thresholds for override activation, requires multi-party authorization, mandates comprehensive disclosure, and subjects override actions to ex-post review by independent auditors and legal counsel.

The protocol balances the need for rapid intervention capability with safeguards against arbitrary or unauthorized override actions. Multi-signature authorization requirements ensure that no single individual can unilaterally override smart contract operations, reducing the risk of unauthorized interventions or actions motivated by improper considerations. Real-time disclosure requirements ensure that investors and the public receive immediate notification of override actions, enabling scrutiny and accountability.

## 4.2 Authorization and Activation Parameters

The Emergency Override Protocol may be activated only by duly authorized municipal officials acting pursuant to legal authority established in the Master Indenture, municipal charter, or applicable state law. Authorized officials typically include the chief executive officer of the municipality (such as the mayor or county executive), the chief financial officer or treasurer, and potentially designated members of the legislative body or finance committee with authority over debt management.

Activation requires multi-signature authorization from a specified minimum number of authorized officials, typically three individuals representing different institutional roles within municipal government. This multi-signature requirement prevents unilateral override actions and ensures that multiple perspectives inform the decision to intervene in automated processes. The requirement also reduces the risk that override capability could be exploited by a single compromised or malicious actor.

The protocol may be activated only under narrowly defined circumstances enumerated in the Master Indenture and disclosed to investors in offering documents. Authorized circumstances include:

- **Force Majeure Events:** Natural disasters, terrorist attacks, cyberattacks on critical infrastructure, pandemic public health emergencies, or other extraordinary circumstances beyond the reasonable control of the municipality that materially impair its ability to perform obligations under the Master Indenture
- **National Security Emergencies:** Circumstances in which federal or state authorities direct the suspension of financial transactions for national defense or homeland security purposes
- **Budgetary Crises:** Circumstances in which the municipality faces acute fiscal distress threatening its ability to meet debt service obligations, requiring temporary suspension of payments to enable orderly restructuring or access to emergency liquidity facilities
- **Material Smart Contract Errors:** Circumstances in which smart contract bugs, oracle failures, or other technological malfunctions cause incorrect execution of contractual terms, requiring manual intervention to correct the error and restore proper functioning
- **Court Orders or Regulatory Directives:** Circumstances in which judicial or regulatory authorities order intervention in automated processes

The Master Indenture specifies procedural requirements for override activation, including documentation standards, internal approval processes, consultation with bond counsel and the indenture trustee, and notification timelines. These procedural safeguards ensure that override decisions are deliberate, well-documented, and subject to appropriate legal and financial review before execution.

## 4.3 Transparency, Disclosure, and Audit Trail Requirements

All Emergency Override Protocol activations are subject to comprehensive transparency and disclosure requirements designed to ensure public accountability and enable investor scrutiny of interventions in automated processes. These requirements operate at multiple levels, including real-

time notification to investors and the public, detailed documentation of override rationale and decision-making processes, and ex-post review by independent auditors and legal counsel.

**Real-Time Disclosure:** Automated notification systems alert all investors immediately upon override activation. Notifications include a description of the nature of the emergency or circumstance justifying override, the specific smart contract functions being suspended or modified, the expected duration of the override, and the anticipated impact on investor rights or payment obligations. Notifications are distributed through multiple channels including email, the municipal securities information system, and potentially social media or public website postings.

**Comprehensive Documentation:** Permanent, immutable records are maintained on the distributed ledger audit trail, recording the identity of authorizing officials, the timestamp of activation, the specific smart contract functions modified, the rationale for intervention, and supporting documentation evidencing the existence of circumstances justifying override. This audit trail ensures that override actions are subject to complete historical record and can be reviewed by investors, auditors, regulators, or the public at any time.

**Legal Opinion Requirements:** The Master Indenture requires that override actions be accompanied by written opinions from bond counsel and potentially independent financial advisors, confirming that the circumstances justify intervention under the terms of the indenture and applicable law. These legal opinions provide assurance that override actions are legally authorized and consistent with the municipality's obligations to investors.

**Ex-Post Review:** Regular audits conducted by the municipality's independent auditors as part of annual financial statement audits, or potentially through special-purpose audits commissioned specifically to review override actions, assess whether override activations complied with authorization requirements, whether the circumstances justified intervention under the terms of the indenture, whether proper procedures were followed, and whether investor interests were appropriately protected. Audit reports are publicly disclosed and submitted to the Municipal Securities Rulemaking Board's Electronic Municipal Market Access system, ensuring that investors and the public have access to independent assessments of override actions.

If auditors identify deficiencies in override procedures or unauthorized activations, remedial actions are required and disclosed to investors.

The transparency framework is designed to create strong accountability mechanisms that discourage casual or unjustified override actions while preserving the capability for intervention in legitimate emergencies. By ensuring that all override actions are subject to comprehensive scrutiny and permanent record, the framework balances operational flexibility with investor protection.

## 4.4 Remediation and Recovery Procedures

Following Emergency Override Protocol activation, the pilot framework establishes comprehensive remediation and recovery procedures designed to restore normal smart contract operations as rapidly as possible while ensuring that any harm resulting from the emergency or the override action itself is appropriately addressed.

**Force Majeure Recovery:** When override activation results from force majeure events or national security emergencies, recovery procedures focus on restoring operational capability and resuming automated execution once the extraordinary circumstances have subsided. The municipality works with technology infrastructure providers, the indenture trustee, and participating broker-dealers to assess system integrity, verify data consistency, and implement any necessary repairs or upgrades before reactivating automated processes.

**Smart Contract Error Remediation:** When override activation results from smart contract errors or technological malfunctions, recovery procedures include root cause analysis to identify the source of the error, development and testing of corrective code patches, independent security audit of the proposed fixes, and coordinated deployment of corrected smart contracts. During the remediation period, manual processes substitute for automated execution to ensure continuity of payment and settlement operations.

**Investor Compensation Mechanisms:** When override actions result in harm to investors due to incorrect payment distribution, unauthorized transfers, or other smart contract failures, the Master Indenture establishes make-whole procedures requiring the municipality or responsible parties to compensate investors for losses. Compensation mechanisms may include supplemental interest payments, principal adjustments, or direct financial settlements depending on the nature and magnitude of the harm.

**Trustee Oversight:** The indenture trustee plays a central role in overseeing remediation and recovery procedures, representing investor interests and ensuring that corrective actions are adequate to restore proper functioning and protect investor rights. The trustee has authority to engage independent experts to assess proposed corrective measures, to require additional safeguards or testing before resuming automated operations, and to pursue legal remedies if the municipality or other responsible parties fail to implement adequate remediation.

**Testing and Validation:** Recovery procedures include comprehensive testing of corrected systems before resuming live operations, utilizing test networks and simulated scenarios to validate that fixes effectively address identified issues without introducing new vulnerabilities. Independent security auditors review and approve testing results before production deployment is authorized.

**Post-Recovery Disclosure:** Disclosure provides investors with detailed information regarding the nature of the emergency or error, the corrective actions implemented, the results of testing and security audits, and any changes to operational procedures or risk management protocols implemented to reduce the likelihood of similar incidents in the future. This disclosure ensures that investors can assess whether adequate remediation has occurred and make informed decisions regarding continued holding or disposition of their securities.

## 4.5 Governance Evolution and Stakeholder Participation

The governance framework for the pilot program includes mechanisms for continuous improvement and stakeholder participation in the evolution of operational protocols, risk management procedures, and emergency response frameworks. These mechanisms ensure that the pilot benefits from the collective expertise of participating entities and adapts to emerging challenges or opportunities identified during operation.

**Pilot Governance Committee:** A governance committee comprising representatives from participating municipalities, broker-dealers, bank custodians, the indenture trustee, and potentially investor representatives or independent experts meets on a quarterly basis to review operational performance, discuss incidents or challenges encountered during the period, and consider proposals for protocol enhancements or procedural modifications. The committee serves as a forum for collective problem-solving and knowledge sharing among diverse stakeholders.

**Transparency and Public Input:** Committee deliberations are documented in written minutes that are publicly disclosed, ensuring transparency regarding governance decisions and enabling broader stakeholder input into the evolution of the pilot framework. Proposed modifications to operational protocols or emergency procedures are subject to notice and comment periods during which investors, industry participants, and the public may provide feedback before implementation.

**FinHub Staff Participation:** FinHub staff participate in governance committee meetings as observers and advisors, providing regulatory perspective on proposed modifications and ensuring that protocol evolution remains consistent with investor protection principles and applicable securities law. The Commission retains ultimate authority to require modifications to pilot operations or to terminate the pilot if investor protection concerns arise or compliance deficiencies are identified.

**Sunset Evaluation:** The governance framework includes sunset provisions requiring comprehensive evaluation of the pilot at the conclusion of the initial twelve to eighteen month period. This evaluation assesses operational performance metrics, compliance with securities laws and self-regulatory organization rules, investor satisfaction and protection outcomes, cost-benefit analysis compared to traditional municipal securities issuance, and recommendations regarding potential expansion, modification, or termination of the program.

**Stakeholder Input:** Stakeholder input is solicited as part of the sunset evaluation process, with participating entities, investors, industry associations, and the public invited to provide comments on pilot outcomes and recommendations for future evolution. This inclusive approach ensures that the decision regarding pilot continuation or modification benefits from diverse perspectives and empirical evidence gathered during operation.

---

# SECTION V: PILOT PARAMETERS AND IMPLEMENTATION FRAMEWORK

## 5.1 Scale, Duration, and Participation Criteria

The pilot program is intentionally designed as a limited-scale experiment enabling rigorous evaluation of distributed ledger technology in municipal securities markets while minimizing potential systemic risks or unintended market disruptions. The parameters governing scale, duration, and participant selection reflect a cautious approach prioritizing data generation and empirical learning over rapid expansion or commercialization.

**Issuance Volume Caps:** Total issuance volume across all participating municipalities is capped at ten million dollars in aggregate principal amount, ensuring that the pilot remains sufficiently modest to avoid material impact on broader municipal debt markets. Individual issuances are limited to a maximum principal amount of two million dollars, preventing concentration of pilot activity in a small number of large transactions and enabling participation by multiple municipalities across diverse geographic regions and credit profiles.

**Pilot Duration:** The pilot duration is proposed as twelve to eighteen months from the date of first issuance, providing sufficient time to observe full debt service cycles for short-term Revenue Anticipation Notes and initial payment periods for longer-term General Obligation Bonds. This timeframe enables collection of meaningful operational performance data, evaluation of secondary market liquidity development, and assessment of investor satisfaction and protection outcomes.

**Municipal Issuer Selection:** Participation is limited to a carefully selected cohort of municipal issuers that demonstrate institutional readiness, technical capability, and commitment to regulatory compliance. Municipal issuers are selected through a transparent application process evaluating financial condition, governance quality, technical infrastructure capacity, and commitment to enhanced disclosure and transparency standards. Preferred candidates include mid-sized municipalities across diverse U.S. states with demonstrated track records of fiscal responsibility, transparent governance, and innovative approaches to public finance.

**Broker-Dealer Selection:** Participating broker-dealers include registered firms with established public finance practices, demonstrated expertise in municipal securities underwriting and distribution, robust compliance programs, and technical capacity to integrate distributed ledger infrastructure with existing operational systems. Broker-dealers must demonstrate commitment to fair dealing with both municipal issuers and investors, comprehensive disclosure practices, and rigorous adherence to Municipal Securities Rulemaking Board rules.

**Bank Custodian Selection:** Bank custodians include federally chartered or state-supervised depository institutions with existing municipal securities custody capabilities, strong capital and liquidity positions, established cybersecurity and operational risk management frameworks, and technical expertise in distributed ledger technology. Banks must demonstrate capacity to operate validation nodes on the permissioned network infrastructure, implement secure cryptographic key management protocols, and provide comprehensive custody services meeting Exchange Act Rule 15c3-3 requirements.

**Investor Eligibility:** Investor participation is limited to qualified institutional buyers and accredited investors meeting enhanced due diligence standards appropriate for experimental securities structures. Qualified institutional buyers include institutions with at least one hundred million dollars in securities investments, such as investment companies, insurance companies, pension plans, and other institutional investors with demonstrated sophistication in evaluating and managing investment risks. Accredited investors include individuals or entities meeting net worth or income thresholds established under Regulation D, ensuring that participants possess financial sophistication appropriate for evaluating novel investment structures.

**Voluntary Participation:** The pilot operates on a voluntary opt-in basis for all participants. No municipality, broker-dealer, bank, or investor is obligated to engage with tokenized securities, and

traditional municipal debt issuance pathways remain fully available throughout the pilot period. This voluntary structure ensures that the experiment does not create market distortions or compel participation by entities lacking technical readiness or institutional appetite for innovation.

## 5.2 Municipal Issuer Selection and Onboarding

Municipal issuer selection prioritizes jurisdictions that combine financial stability, governance quality, technical readiness, and commitment to transparency. The selection process evaluates multiple factors to identify municipalities likely to succeed in implementing tokenized securities while providing valuable data regarding operational performance and market acceptance.

**Financial Stability Assessment:** Financial stability is assessed through review of recent audited financial statements, credit ratings from nationally recognized statistical rating organizations, and analysis of debt service coverage ratios, revenue volatility, and fund balance adequacy. Preferred candidates demonstrate strong creditworthiness, diversified revenue bases, and consistent track records of meeting debt service obligations on time and in full.

**Governance Quality Evaluation:** Governance quality is evaluated through assessment of internal control environments, transparency in budgeting and financial reporting, compliance with continuing disclosure obligations for existing debt, and track record of ethical conduct by elected officials and municipal staff. Preferred candidates demonstrate commitment to best practices in public finance management and transparency in stakeholder engagement.

**Technical Readiness Assessment:** Technical readiness is assessed through evaluation of existing information technology infrastructure, cybersecurity capabilities, staff expertise in financial systems administration, and capacity to engage external technical advisors for distributed ledger implementation. Municipalities need not possess in-house blockchain expertise but must demonstrate willingness to invest in necessary technical capacity building and engagement with qualified technology providers.

**Transparency Commitment:** Commitment to transparency is evaluated through assessment of existing public disclosure practices, citizen engagement mechanisms, and willingness to implement enhanced real-time transparency regarding use of proceeds and compliance with indenture covenants. Preferred candidates view tokenized securities not merely as a financing mechanism but as an opportunity to strengthen public accountability and citizen trust in municipal finance operations.

**Comprehensive Onboarding:** Selected municipalities undergo comprehensive onboarding processes including:

- Education regarding distributed ledger technology and smart contract functionality
- Development of internal governance protocols for disbursement authorization and Emergency Override Protocol activation
- Establishment of relationships with participating broker-dealers and bank custodians
- Engagement of bond counsel and financial advisors with expertise in innovative finance structures
- Implementation of necessary technology infrastructure and staff training

**Enhanced Disclosure Development:** Onboarding includes development of comprehensive disclosure documents addressing the unique characteristics and risks of tokenized securities, ensuring that investors receive material information necessary to make informed decisions. Official statements include detailed descriptions of the distributed ledger platform, custody arrangements, settlement mechanics, smart contract functionality, Emergency Override Protocol, and potential technological risks.

## 5.3 Broker-Dealer and Bank Participation Framework

Broker-dealers participating in the pilot serve multiple critical functions including underwriting or placement agent services for primary issuance, secondary market liquidity provision, investor education regarding tokenized securities, and compliance monitoring to ensure adherence to Municipal Securities Rulemaking Board rules and federal securities laws.

**Comprehensive Supervisory Procedures:** Participating broker-dealers implement comprehensive supervisory procedures addressing the unique characteristics of tokenized securities while maintaining consistency with established regulatory obligations. Procedures address suitability determinations for investors considering tokenized securities, disclosure delivery requirements, fair pricing standards for primary and secondary transactions, and supervision of associated person activities related to distributed ledger operations.

**Investor Education:** Broker-dealers engage in extensive investor education efforts to ensure that potential purchasers understand the structure, mechanics, and risks of tokenized securities. Educational materials explain the relationship between the Master Indenture and digital representation, describe custody arrangements and settlement processes, clarify the Emergency Override Protocol and circumstances under which it may be activated, and emphasize the experimental nature of the pilot and the possibility of technological challenges or market acceptance issues.

**Underwriting and Placement Services:** In their capacity as underwriters or placement agents for primary issuance, broker-dealers comply with Rule G-17 fair dealing obligations to municipal issuers by providing comprehensive disclosure regarding the costs, risks, and alternatives to tokenized securities. Broker-dealers assist municipalities in developing disclosure documents, coordinating with technology providers and custodians, and structuring transactions to achieve issuer objectives while maintaining full compliance with applicable regulations.

**Secondary Market Liquidity:** In secondary market activities, broker-dealers provide liquidity services enabling investors to buy or sell tokenized securities outside of primary issuance periods. Broker-dealers maintain inventory in selected securities, post quotations on alternative trading systems or other electronic platforms, and facilitate transactions between buyers and sellers. Secondary market activities are subject to fair pricing obligations, ensuring that markups and markdowns reflect reasonable compensation for services rendered and market conditions.

**Bank Custodian Operations:** Bank custodians participating in the pilot operate distributed ledger validation nodes, provide secure cryptographic key custody services, implement identity verification and attestation functions, and maintain comprehensive operational controls ensuring

asset protection and regulatory compliance. Banks undergo rigorous technical and operational readiness assessments before commencing pilot activities.

**Comprehensive Cybersecurity Frameworks:** Banks implement comprehensive cybersecurity frameworks consistent with federal banking agency guidance on distributed ledger technology and digital asset custody. Controls include segregated key storage in hardware security modules, multi-signature authorization for transaction execution, real-time reconciliation between on-chain records and internal custody systems, and continuous monitoring for suspicious activity or potential security threats.

**Banking Supervision:** Banks provide regular reporting to federal banking supervisors regarding pilot activities, operational performance, risk management procedures, and compliance with custody standards. Supervisors conduct examinations to assess the adequacy of controls and the effectiveness of risk management frameworks, ensuring that pilot activities do not compromise safety and soundness of participating institutions.

## 5.4 Reporting and Performance Evaluation Metrics

The pilot program incorporates comprehensive reporting requirements designed to provide FinHub staff and the Commission with visibility into operational performance, compliance outcomes, investor experiences, and market impacts. Participating entities submit regular reports addressing multiple dimensions of pilot operations and outcomes.

**Quarterly Operational Reports:** Operational reports provide data on issuance volumes, secondary market transaction activity, settlement success rates and failure incidents, custody operations and asset reconciliation, investor onboarding and account activity, and technology infrastructure performance. Reports identify operational challenges encountered during the period, describe corrective actions implemented, and provide recommendations for protocol enhancements or procedural modifications.

**Compliance Reports:** Compliance reports address adherence to securities laws, Municipal Securities Rulemaking Board rules, custody requirements, and pilot-specific protocols. Reports document instances of non-compliance or deficiencies identified, describe remedial actions taken, and provide assurance that participating entities maintain adequate supervisory and compliance programs. Reports also address investor complaints or disputes, describing resolution processes and outcomes.

**Investor Satisfaction Surveys:** Investor satisfaction surveys provide qualitative feedback regarding investor experiences with tokenized securities, including ease of account opening and verification processes, clarity of disclosure materials, functionality of custody and settlement infrastructure, secondary market liquidity availability, and overall satisfaction with the investment experience. Surveys identify areas for improvement and provide insights into factors influencing investor willingness to participate in future tokenized securities offerings.

**Cost-Benefit Analyses:** Cost-benefit analyses compare the economics of tokenized securities issuance with traditional municipal debt issuance, evaluating underwriting costs, legal and documentation expenses, ongoing administrative burdens, and interest rate pricing. Analyses assess whether distributed ledger technology delivers measurable cost savings or efficiency improvements

relative to conventional approaches, providing empirical evidence regarding the value proposition of tokenized securities for municipal issuers.

**Market Impact Assessments:** Market impact assessments evaluate whether pilot activities influence broader municipal debt markets, including potential effects on pricing, liquidity, or investor demand for traditional municipal securities. Assessments monitor for unintended consequences or market distortions that might justify modifications to pilot parameters or expanded regulatory oversight.

**Technology Performance Metrics:** Technology performance metrics address distributed ledger infrastructure reliability, smart contract execution accuracy, settlement processing speeds, system uptime and availability, and cybersecurity incident frequency and severity. Metrics enable evaluation of whether distributed ledger technology delivers on promised operational benefits and identify areas requiring technological enhancements or risk mitigation measures.

## 5.5 Sunset Provisions and Exit Strategies

The pilot program includes comprehensive sunset provisions requiring formal evaluation at the conclusion of the initial twelve to eighteen month period and establishing clear pathways for program continuation, modification, or termination based on observed outcomes.

**Comprehensive Assessment Reports:** At the completion of the pilot period, participating entities prepare comprehensive assessment reports evaluating operational performance, regulatory compliance, investor protection outcomes, cost-benefit results, and overall success in achieving pilot objectives. Reports provide recommendations regarding whether the pilot should continue, expand to include additional participants or larger transaction volumes, modify operational protocols or risk management procedures, or terminate based on identified deficiencies or lack of demonstrated value.

**FinHub Staff Evaluation:** FinHub staff conduct independent evaluations based on submitted reports, stakeholder consultations, and Commission staff observations during the pilot period. Evaluations address whether the pilot demonstrated that distributed ledger technology can operate safely within existing regulatory frameworks, whether operational benefits justify the costs and risks of technology adoption, whether investor protection standards were maintained throughout the pilot, and whether broader expansion or permanent integration into municipal securities markets is appropriate.

**Commission Decision-Making:** The Commission considers staff recommendations and stakeholder input in determining the future of the pilot program. Potential outcomes include permanent authorization of tokenized municipal securities subject to ongoing regulatory oversight, expansion of the pilot to include additional issuers or larger transaction volumes, modification of operational parameters based on lessons learned, continuation of the pilot for an additional evaluation period, or termination if investor protection concerns arose or benefits did not materialize as anticipated.

**Orderly Wind-Down Procedures:** If the pilot terminates, comprehensive exit strategies ensure orderly wind-down of outstanding securities and protection of investor interests. Securities that have not yet matured continue to be serviced according to the terms of the Master Indenture, with

interest and principal payments distributed on schedule through traditional payment mechanisms if distributed ledger infrastructure is discontinued. Investors retain full legal rights and remedies under the Master Indenture and applicable law regardless of the continuation or termination of distributed ledger operations.

**Custody Transition:** Custody arrangements transition to traditional certificated or book-entry form if distributed ledger infrastructure is discontinued, with participating custodians implementing migration procedures to ensure continuity of investor ownership records and elimination of operational dependencies on the distributed ledger platform. Transition procedures are coordinated with investors to minimize disruption and ensure that ownership rights are preserved throughout the migration process.

**Data Preservation:** Data preservation requirements ensure that transaction records, compliance documentation, and audit trails generated during the pilot are retained in permanent, accessible form for regulatory oversight, investor reference, and historical analysis. Archived records enable ex-post evaluation of pilot outcomes and provide empirical foundation for future policy decisions regarding distributed ledger technology in securities markets.

---

# APPENDIX A: MARKET PRECEDENTS AND LESSONS LEARNED

## A.1 City of Quincy, Massachusetts - JPMorgan Onyx Implementation (2024)

In April 2024, the City of Quincy, Massachusetts, situated adjacent to Boston, executed a groundbreaking transaction that represents the most significant real-world precedent for the proposed pilot program. The city issued approximately ten million dollars in tax-exempt seven-year municipal bonds utilizing JPMorgan Chase's Onyx blockchain platform (subsequently rebranded as Kinexys Digital Assets), with JPMorgan serving as the sole underwriter.

**Transaction Structure:** The issuance marked the first U.S. municipal bond transaction in which blockchain technology facilitated the complete lifecycle of issuance, settlement, and ownership recording. The bonds were structured as traditional municipal general obligation securities, backed by the full faith and credit of the City of Quincy, and issued in compliance with existing federal securities laws and Municipal Securities Rulemaking Board regulations.

**Technical Implementation:** The transaction utilized JPMorgan's Digital Debt Service on the Onyx platform, a permissioned blockchain infrastructure designed specifically for institutional fixed-income securities. The platform enabled:

- Delivery-versus-payment settlement in near real-time, eliminating traditional settlement lag
- Elimination of traditional Issuing and Paying Agent intermediaries through blockchain-based automation
- Blockchain-based deposit accounts enabling direct receipt of issuance proceeds by the municipality
- Automated post-execution trade management and coupon payment distribution

**Institutional Validation:** The transaction achieved significant institutional validation when BlackRock's iShares Short Maturity Municipal Bond Active ETF (MEAR) purchased $6.5 million (65%) of the issuance in December 2024. This purchase by a major asset management firm managing approximately $750 million in client assets demonstrated that tokenized municipal securities can attract institutional investor capital and integrate into actively managed investment portfolios.

**Operational Benefits Demonstrated:** According to Eric Mason, CFO of the City of Quincy, the blockchain implementation provided several concrete benefits:

- **Enhanced Transparency:** The complete issuance process, legal documentation, and intrinsic bond details are permanently recorded on the blockchain, providing unprecedented transparency for secondary market participants
- **Improved Liquidity Potential:** While traditional municipal bonds typically trade only once or twice annually, blockchain-based bonds enable more frequent trading, potentially increasing liquidity and reducing the risk premium associated with illiquid holdings
- **Reduced Issuance Costs:** The elimination of certain intermediaries and automation of administrative processes resulted in measurable cost reductions compared to traditional issuance methods
- **T+0 Settlement:** The ability to specify precise settlement times and achieve same-day settlement represents a significant operational improvement over traditional two-day settlement cycles

**Lessons Applicable to This Proposal:**

1. **Regulatory Pathway:** The Quincy transaction successfully navigated existing regulatory frameworks without requiring novel exemptions or special treatment, demonstrating that tokenized municipal securities can comply with Securities Act Section 3(a)(2) exemption and MSRB rules

2. **Institutional Acceptance:** BlackRock's participation validates institutional investor willingness to acquire blockchain-based municipal securities when structured within familiar legal frameworks and offering appropriate risk-return characteristics

3. **Platform Maturity:** JPMorgan's Onyx platform demonstrated production-readiness for institutional fixed-income securities, providing evidence that permissioned blockchain infrastructure has moved beyond proof-of-concept to operational deployment

4. **Gradual Adoption:** The Quincy transaction represents measured innovation—utilizing blockchain for operational efficiency while maintaining traditional legal structures—consistent with the balanced approach proposed in this pilot program

5. **Public Sector Innovation:** The transaction demonstrates that mid-sized municipalities can successfully implement innovative finance structures when supported by appropriate technical expertise and institutional partnerships

## A.2 Additional Market Precedents

**Alphaledger Municipal Bond Recordkeeping (2022):** In December 2022, blockchain startup Alphaledger recorded three U.S. municipal bond issuances on its permissioned blockchain as parallel recordkeeping alongside traditional systems. While these transactions did not achieve the full lifecycle integration of the Quincy deal, they demonstrated early market interest in blockchain applications for municipal finance and validated the technical feasibility of distributed ledger recordkeeping for debt securities.

**Goldman Sachs - Michigan State University (2024, Consideration Phase):** Michigan State University Board of Trustees considered a $38 million municipal bond issuance using Goldman Sachs' proprietary digital assets platform to fund a new multicultural center. While ultimately not executed during the relevant timeframe, this consideration by a major public university and global investment bank demonstrates broad institutional interest in tokenized debt issuance beyond a single institution.

**Moody's Ratings On-Chain Credit Rating Integration (June 2025):** Moody's Ratings and Alphaledger completed a proof-of-concept demonstration embedding municipal bond credit ratings into tokenized securities on the Solana blockchain. The test utilized APIs to move credit rating data from Moody's off-chain systems to blockchain-based securities, demonstrating how traditional financial information services can integrate with tokenized asset infrastructure. This precedent validates the technical feasibility of the oracle architecture proposed in Section 2.5 of this framework.

**New Hampshire Bitcoin-Backed Municipal Bond (November 2025):** The New Hampshire Business Finance Authority approved a $100 million municipal bond backed by Bitcoin collateral, representing the first digital-asset-backed municipal security. While this structure differs significantly from the digital twin approach proposed herein, it demonstrates state-level regulatory willingness to innovate in municipal finance and integrate digital assets with traditional capital markets.

---

# APPENDIX B: POST-QUANTUM CRYPTOGRAPHY TECHNICAL SPECIFICATIONS

## B.1 NIST Post-Quantum Cryptography Standards Overview

The National Institute of Standards and Technology completed a multi-year Post-Quantum Cryptography Standardization Process, publishing the first finalized standards in August 2024 and selecting additional algorithms in March 2025. These standards provide quantum-resistant cryptographic algorithms designed to protect sensitive information against attacks from future quantum computers.

**FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)**
Based on the CRYSTALS-Kyber algorithm, ML-KEM provides quantum-resistant key

encapsulation for establishing secure communication channels. The algorithm offers multiple security levels:

- ML-KEM-512: Security equivalent to AES-128
- ML-KEM-768: Security equivalent to AES-192
- ML-KEM-1024: Security equivalent to AES-256

For the pilot framework, ML-KEM-768 is recommended as the baseline implementation, providing robust security appropriate for financial infrastructure while maintaining reasonable computational efficiency.

**FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA)**
Based on the CRYSTALS-Dilithium algorithm, ML-DSA provides quantum-resistant digital signatures. The algorithm offers multiple security levels:

- ML-DSA-44: Smaller signatures, moderate security
- ML-DSA-65: Balanced security and performance
- ML-DSA-87: Maximum security

For the pilot framework, ML-DSA-65 is recommended for transaction signing and audit trail integrity, with ML-DSA-87 reserved for long-lived cryptographic commitments such as Master Indenture digital signatures.

**FIPS 205: Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)**
Based on the SPHINCS+ algorithm, SLH-DSA provides an alternative quantum-resistant signature scheme utilizing hash functions rather than lattice mathematics. This algorithm serves as a cryptographic diversity mechanism, ensuring that vulnerabilities in lattice-based schemes do not compromise the entire system.

**HQC: Hamming Quasi-Cyclic (Selected March 2025)**
Selected as a backup key encapsulation mechanism, HQC provides quantum-resistant key exchange based on code-based cryptography, offering mathematical diversity from lattice-based approaches. The algorithm is expected to be standardized by 2027 and will be integrated into the pilot framework upon finalization.

## B.2 Implementation Strategy for Pilot Framework

**Hybrid Cryptographic Deployment:** During the transition period, the pilot implements hybrid cryptographic schemes combining traditional and post-quantum algorithms:

- **TLS Connections:** Hybrid key exchange utilizing both ECDH (X25519) and ML-KEM-768, ensuring security against both classical and quantum attacks while maintaining compatibility with existing infrastructure
- **Digital Signatures:** Dual signature schemes utilizing both ECDSA (secp256k1) and ML-DSA-65, providing quantum resistance while maintaining backward compatibility during the transition period

- **Long-Term Commitments:** Critical long-lived cryptographic elements such as Master Indenture digital signatures utilize ML-DSA-87 exclusively, prioritizing long-term security over backward compatibility

**Cryptographic Agility:** The architecture implements cryptographic agility mechanisms enabling algorithm updates as standards evolve and post-quantum cryptography implementations mature:

- Smart contract interfaces accept multiple signature algorithms, enabling graceful migration as new algorithms are standardized
- Validator nodes support algorithm negotiation, allowing participants to select preferred cryptographic schemes within approved parameters
- Audit trails record which algorithms were used for each cryptographic operation, enabling forensic analysis if vulnerabilities are discovered

**Performance Considerations:** Post-quantum algorithms generally require larger key sizes and signatures compared to traditional elliptic curve cryptography:

- ML-KEM-768 public keys: approximately 1,184 bytes (vs. 32 bytes for X25519)
- ML-DSA-65 signatures: approximately 3,309 bytes (vs. 64 bytes for ECDSA)

The pilot framework accounts for these increased sizes in data structure design and network bandwidth provisioning.

**Timeline Alignment:** Implementation follows NIST transition guidance (NIST IR 8547) recommending migration from quantum-vulnerable algorithms by 2035. By implementing post-quantum cryptography from pilot inception, municipal securities issued during the program benefit from enhanced long-term security appropriate for debt instruments with multi-year maturities.

---

# APPENDIX C: SAMPLE MASTER INDENTURE PROVISIONS

## C.1 Digital Twin Status of Tokenized Security

### Section [X].1 - Representation of Obligation on Distributed Ledger

The Issuer has authorized the representation of this Obligation on a permissioned distributed ledger technology platform operated by authorized Validator Nodes pursuant to the Technology Services Agreement dated as of [Date]. The digital representation, referred to herein as the "Token" or "Tokenized Security," constitutes operational infrastructure for settlement, payment distribution, and compliance monitoring as contemplated by this Indenture.

The Token serves as evidence of beneficial ownership of this Obligation but does not replace, supersede, or diminish the legal force of this Indenture or the rights and remedies of Owners established herein. The substantive rights and obligations of the Issuer, the Trustee, and the Owners flow exclusively from this Indenture and applicable law, with the Token providing operational mechanisms for executing the terms and conditions specified herein.

**Section [X].2 - Hierarchy of Authority**

In the event of any discrepancy, conflict, or inconsistency between the provisions of this Indenture and the operational behavior of the Token or associated smart contracts, the provisions of this Indenture shall prevail and control in all respects. No automated execution of smart contract functions shall diminish the obligation of the Issuer to perform its covenants under this Indenture, nor shall any failure of smart contract operations excuse the Issuer from performance of its obligations.

The rights and remedies of Owners established in this Indenture, including without limitation the right to receive timely payment of principal and interest, the right to enforce covenants and representations, and the right to pursue judicial remedies in the event of default, shall remain fully enforceable regardless of the operational status of distributed ledger infrastructure or the accuracy of on-chain records.

**Section [X].3 - Transfer of Beneficial Ownership**

Transfer of the Token on the distributed ledger platform in accordance with the transfer protocols specified in the Technology Services Agreement shall constitute valid transfer of beneficial ownership of the corresponding principal amount of this Obligation, subject to the transfer restrictions and eligibility requirements specified herein and in the applicable smart contract code.

All transfers of beneficial ownership, whether effectuated through distributed ledger operations or through traditional book-entry mechanisms, shall be recorded in the registry maintained by the Trustee or its designated Transfer Agent, which shall serve as the authoritative record of beneficial ownership for purposes of determining entitlement to payments, voting rights if applicable, and notices under this Indenture.

**Section [X].4 - Emergency Override Authority**

The Issuer, acting through the authorized officials specified in Schedule [X] hereto, is hereby authorized to suspend, modify, or terminate the operational functioning of the Token and associated smart contracts in circumstances including but not limited to: force majeure events rendering automated execution impossible or impractical; national security emergencies requiring immediate suspension of financial operations pursuant to governmental directive; material errors in smart contract execution causing incorrect payment distribution, unauthorized transfers, or other operational failures; budgetary emergencies threatening the Issuer's ability to meet its obligations hereunder; or court orders or regulatory directives requiring intervention in automated processes.

Any exercise of emergency override authority shall be effectuated through multi-signature authorization mechanisms requiring approval from no fewer than three authorized officials representing separate institutional roles within the Issuer's governance structure. All override actions shall be promptly disclosed to Owners, the Trustee, and applicable regulatory authorities, shall be documented in comprehensive written records preserved for audit and review, and shall be subject to ex-post examination by the Issuer's independent auditors as part of annual financial statement audits.

The emergency override authority established herein shall not diminish the Issuer's obligations under this Indenture or excuse performance of any covenant or representation. Exercise of override

authority in response to operational failures shall be accompanied by diligent efforts to remediate the underlying failures, restore proper functioning, and compensate Owners for any harm resulting from such failures or the override actions themselves.

**Section [X].5 - Technology Risk Acknowledgment and Quantum Cryptography**

The Issuer has disclosed to Owners in the Official Statement dated [Date] the use of distributed ledger technology for operational infrastructure supporting this Obligation. Owners acknowledge that distributed ledger technology and smart contract operations involve technological risks including but not limited to software defects, cybersecurity vulnerabilities, operational dependencies on third-party infrastructure providers, and potential limitations on system availability or performance.

To address long-term cryptographic security concerns, the distributed ledger infrastructure implements post-quantum cryptographic algorithms aligned with National Institute of Standards and Technology Federal Information Processing Standards 203, 204, and 205, providing quantum-resistant key encapsulation and digital signature capabilities. This implementation ensures that cryptographic protections securing the Token and associated transactions remain robust against both classical and quantum computational attacks throughout the term of this Obligation.

Notwithstanding the foregoing technology risk acknowledgment, nothing herein shall diminish the Issuer's obligation to make timely payment of principal and interest on this Obligation, to comply with covenants and representations specified herein, or to provide Owners with the rights and remedies established in this Indenture and applicable law. In the event that distributed ledger infrastructure becomes unavailable or inoperable for any reason, the Issuer shall implement alternative mechanisms for payment distribution, ownership recordkeeping, and discharge of its obligations hereunder through traditional banking and securities transfer systems.

---

# APPENDIX D: ILLUSTRATIVE MUNICIPAL JURISDICTIONS AND USE CASES

## D.1 Municipal Participation Framework

The pilot program is designed to accommodate participation by mid-sized municipalities across diverse U.S. jurisdictions, enabling evaluation of tokenized securities performance across different geographic regions, economic conditions, revenue structures, and governance frameworks. While the final cohort of participating municipalities will be determined through a competitive application process, the following jurisdictions represent illustrative examples of potentially suitable participants based on demonstrated commitment to innovation, strong governance practices, and appropriate scale for pilot experimentation.

**Illustrative Jurisdiction A - Austin, Texas**

A rapidly growing municipality with strong economic fundamentals, diversified revenue base including property taxes, sales taxes, and utility revenues, established track record of innovative

public finance approaches, and demonstrated commitment to technology adoption in municipal operations.

**Potential Use Case:** Issuance of Revenue Anticipation Notes secured by utility revenue streams (water and wastewater systems) to finance infrastructure upgrades, with programmable use-of-proceeds validation ensuring funds are deployed exclusively for capital improvements rather than operating expenses. The transparent on-chain audit trail strengthens public accountability and demonstrates efficient use of taxpayer-backed borrowing.

**Illustrative Jurisdiction B - Rochester, New York**

A mid-sized municipality with moderate growth trajectory, mixed industrial and service economy, established municipal finance practices, and ongoing infrastructure investment needs in aging urban systems.

**Potential Use Case:** Issuance of General Obligation Bonds to finance public facility renovations or equipment acquisitions for essential city services, with enhanced real-time transparency regarding project progress and use-of-proceeds deployment strengthening public accountability and citizen trust in municipal borrowing.

**Illustrative Jurisdiction C - Santa Monica, California**

A municipality with advanced digital government initiatives, strong commitment to transparency and citizen engagement, diversified revenue base including property taxes, tourism-related receipts, and parking revenues, and demonstrated capacity for innovative approaches to public finance.

**Potential Use Case:** Issuance of Revenue Anticipation Notes secured by parking revenue or tourism-related fees to finance seasonal working capital needs, with real-time transparency regarding revenue collections and debt service coverage strengthening investor confidence and potentially reducing borrowing costs through enhanced credit visibility.

These illustrative jurisdictions are provided solely for purposes of demonstrating the types of municipalities suitable for pilot participation based on financial stability, governance quality, technical readiness, and alignment with pilot objectives. Final participant selection will occur through a transparent application process evaluating multiple candidates against established criteria, with no commitment or obligation on the part of the mentioned jurisdictions to participate in the pilot program.

---

# APPENDIX E: Executive Summary and Practical Use Case

### 1. The Concept on a Single Page

The **"Trusted Municipal Protocol"** is a proposed regulatory sandbox framework designed to modernize municipal capital formation in the United States. Unlike unregulated crypto-asset projects, this infrastructure utilizes distributed ledger technology (DLT) to enhance—not replace—existing legal protections and financial intermediaries.

**The Three Pillars of the Proposal:**

- **Regulatory Primacy (The "Digital Twin"):** The Token is solely an operational representation. The traditional legal contract (*Master Indenture*) remains the supreme authority. In the event of a discrepancy between the code and the contract, the contract prevails.
- **Institutional Continuity:** Banks and Broker-Dealers retain their essential roles as validators, custodians, and distributors, but with greater operational efficiency and T+0 settlement capabilities.
- **Future-Proof Security:** The protocol features the pioneering use of post-quantum cryptography (NIST FIPS 203/204/205) to ensure that long-term debt instruments remain secure against future computational threats.

---

**2. Practical Example: The "City of Lakeview" Bond Issuance**

To illustrate the protocol's mechanics, we describe the complete lifecycle of a hypothetical issuance within the pilot program.

**Scenario:** The **City of Lakeview** (a mid-sized jurisdiction) needs to raise **$2 million** to renovate its water treatment plant. The municipality opts to issue tokenized *Revenue Anticipation Notes* (RANs).

**Phase 1: Issuance and the "Digital Twin"** The City and the Trustee execute the traditional *Master Indenture*, establishing the binding legal rules. A smart contract is deployed on the permissioned network, creating 2,000 tokens (face value of $1,000 each) that serve as "Digital Twins" of the legal debt. **Golden Rule:** The code reflects the "Use-of-Proceeds" restrictions defined in the legal documents: funds may only be spent on water infrastructure.

**Phase 2: Distribution and Sale (The Intermediary Role)** A Pension Fund (Qualified Institutional Buyer) wishes to purchase $500,000 of these notes. They access the system through their regular Broker-Dealer. The Broker performs KYC/AML checks and attests to the fund's identity *off-chain*. The Fund's digital wallet receives an on-chain approval "visa" from the validator, enabling it to transact.

**Phase 3: Atomic Settlement (The Efficiency Moment)** The Fund submits the buy order. The system instantly verifies three conditions: (A) Does the buyer have sufficient funds? (B) Does the seller have the notes? (C) Are both parties compliant? **Action:** In a single indivisible transaction (*Atomic Settlement*), cash moves to the City's account and tokens move to the Fund's custody. Counterparty risk is effectively eliminated.

**Phase 4: Transparency in Use of Funds** The City attempts to withdraw $100,000 to pay the waterworks contractor. The smart contract automatically verifies the recipient and approves the transaction. Subsequently, the City attempts to withdraw $50,000 to cover a general payroll deficit (an unauthorized use). The smart contract automatically **blocks** the transaction, as it violates the pre-programmed use-of-proceeds restrictions.

**Phase 5: The "Safety Valve" (Emergency Protocol)** *Situation:* A severe technical error is detected in the interest rate oracle, or a national cyberattack occurs. **Action:** The Mayor and the City Treasurer, utilizing multi-signature authentication (multi-sig), activate the **"Emergency Override Protocol."** The smart contract is paused. Settlement reverts to manual/traditional modes until the system is audited and restored. All actions are recorded in an immutable log for public audit.

---

### 3. Technical and Compliance Summary

The protocol is built on a robust architecture designed to meet enterprise standards and regulatory requirements.

- **Infrastructure:** The system operates on a **Permissioned Blockchain** (e.g., Onyx or Hyperledger variants), ensuring that the network is operated exclusively by regulated financial institutions (banks) rather than anonymous validators.
- **Security:** To address long-term risks, the protocol employs **Hybrid Post-Quantum Cryptography** (ML-DSA combined with ECDSA). This protects the system against future quantum computing attacks, aligning with the White House National Security Memorandum 10 (NSM-10).
- **Custody:** Compliance with **SEC Rule 15c3-3** (Customer Protection) is strictly maintained through the use of Hardware Security Modules (HSMs) certified to FIPS 140-3 Level 3 standards and offline cold storage protocols.
- **Identity:** The architecture utilizes a model of **Off-Chain Identity with On-Chain Pseudonymity**. This preserves investor privacy in compliance with data protection laws while ensuring full traceability for regulatory oversight.
- **Settlement:** The system features a **Dual-Mode Settlement** engine. This provides flexibility by supporting both instantaneous Atomic Settlement (T+0) and Netted Settlement (T+1), allowing participants to integrate via legacy clearing systems if preferred.

**Final Note:** This pilot does not seek exemption from securities laws; rather, it seeks the opportunity to demonstrate that technology can fulfill them more efficiently, transparently, and securely.

---

# APPENDIX F: ENHANCED OPERATIONAL FRAMEWORKS

**Tokenized Municipal Instruments Under Distributed Ledger Technology**
**Supplemental Technical Documentation**

## F.1 CYBERSECURITY INCIDENT RESPONSE FRAMEWORK

### F.1.1 Incident Classification Matrix

The pilot program implements a tiered incident response structure with defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) aligned with industry best practices for financial market infrastructure.

**Severity Level 1: Critical (Smart Contract Exploit / Validator Compromise)**

**Definition:** Incidents threatening investor assets, smart contract integrity, or consensus mechanism security.

**Response Parameters:**

- **RTO:** 4 hours maximum for containment and failover
- **RPO:** Zero transaction loss (all transactions either fully executed or fully rolled back)
- **Activation Threshold:** Confirmed unauthorized access to custody wallets, smart contract vulnerability exploitation, or Byzantine validator behavior

**Response Protocol:**

1. **Immediate Actions (0-15 minutes):**
    - Automatic Emergency Override Protocol activation
    - Pause all smart contract operations on affected securities
    - Isolate compromised validator nodes from consensus network
    - Notify SEC FinHub staff and participating broker-dealers
2. **Investigation Phase (15 minutes - 2 hours):**
    - Forensic analysis by designated cybersecurity incident response team
    - Identify attack vector and scope of compromise
    - Verify integrity of backup systems and cold storage assets
    - Engage external security auditors (Trail of Bits, OpenZeppelin, or equivalent)
3. **Remediation Phase (2-4 hours):**
    - Deploy patched smart contracts to test network
    - Verify fixes through automated formal verification tools
    - Restore operations using validated backup state
    - Execute reconciliation procedures with affected investors
4. **Recovery Phase (4-8 hours):**
    - Gradual resumption of automated operations under enhanced monitoring
    - Real-time disclosure to all investors via EMMA and direct notification
    - File Suspicious Activity Report (SAR) if fraud suspected

**Disclosure Requirements:**

- Public disclosure within 4 hours of incident detection
- Detailed incident report within 48 hours
- Post-incident review within 30 days

---

**Severity Level 2: High (Oracle Failure / Network Partition)**

**Definition:** Incidents affecting data integrity or network availability without direct threat to custody.

**Response Parameters:**

- **RTO:** 24 hours for full service restoration
- **RPO:** Last confirmed block state (maximum 10 minutes of transaction history)
- **Activation Threshold:** Oracle data discrepancy exceeding ±5%, network partition affecting >33% of validators

**Response Protocol:**

1. **Automatic Failover (0-30 minutes):**
    - Switch to backup oracle data providers
    - Reroute transactions through operational validator nodes
    - Activate dual-mode settlement (revert to netted T+1 if atomic T+0 unavailable)
2. **Root Cause Analysis (30 minutes - 12 hours):**
    - Validate oracle data sources against authoritative references (MSRB EMMA, Bloomberg)
    - Diagnose network partition cause (DDoS, infrastructure failure, consensus bug)
    - Coordinate with validator node operators for synchronized recovery
3. **Restoration (12-24 hours):**
    - Restore primary oracle connections with enhanced validation
    - Re-establish Byzantine Fault Tolerant consensus with all validators
    - Verify blockchain state consistency across all nodes

**Disclosure Requirements:**

- Notification to affected investors within 12 hours
- Public disclosure if service interruption exceeds 6 hours

---

**Severity Level 3: Medium (Performance Degradation / Minor Bugs)**

**Definition:** Incidents affecting user experience or operational efficiency without security implications.

**Response Parameters:**

- **RTO:** 72 hours for optimization
- **RPO:** Not applicable (no data loss risk)
- **Activation Threshold:** Transaction processing delays >15 minutes, user-reported smart contract errors

**Response Protocol:**

- Standard bug fix deployment cycle

- Performance tuning and capacity scaling
- Enhanced monitoring deployment

**Disclosure Requirements:**

- Quarterly reporting in FinHub operational metrics submission

---

### F.1.2 Validator Node Failover Architecture

**Byzantine Fault Tolerant Consensus Parameters:**

- Minimum 4 validator nodes required (tolerates 1 Byzantine failure)
- Optimal configuration: 7 validators (tolerates 2 Byzantine failures)
- Geographic distribution: Minimum 3 different data center regions

**Failover Sequence:**

```
IF validator_unavailable OR validator_byzantine_detected THEN
    consensus.exclude_node(compromised_validator)
    IF remaining_validators >= minimum_quorum THEN
        consensus.continue_with_reduced_set()
    ELSE
        emergency_override.activate("network_partition")
        settlement.fallback_to_manual_mode()
    END IF
END IF
```

**Validator Restoration Requirements:**

- Full security audit before re-admission to consensus
- Blockchain state synchronization and verification
- Graduated re-integration (observer mode → backup validator → primary validator)

---

### F.1.3 Communication Protocols During Incidents

**Stakeholder Notification Hierarchy:**

**Tier 1 - Immediate (within 30 minutes):**

- SEC FinHub designated staff contact
- Indenture Trustee
- Affected municipal issuer officials
- Primary broker-dealers

**Tier 2 - Rapid (within 4 hours):**

- All registered investors via email and EMMA notice
- Municipal Securities Rulemaking Board (MSRB)
- Backup validator node operators

**Tier 3 - Standard (within 24 hours):**

- Public disclosure via municipal issuer website
- Press release if incident affects >$1M principal amount
- Industry notification via SIFMA channels

**Communication Channels:**

- Primary: Encrypted email with PGP signatures
- Secondary: Direct phone contact with designated officials
- Tertiary: Automated notification via smart contract event logs

---

## F.2 SECONDARY MARKET LIQUIDITY MECHANISMS

### F.2.1 Market-Making Requirements for Participating Broker-Dealers

To ensure adequate secondary market liquidity during the pilot program, participating broker-dealers agree to maintain continuous two-sided markets subject to the following minimum standards:

**Quotation Standards**

**Bid-Ask Spread Maximums:**

- Investment-grade securities (rated A- or higher): **≤25 basis points**
- Non-investment grade securities (rated BBB+ or lower): **≤50 basis points**
- Unrated securities: **≤75 basis points**

Spreads measured as percentage of mid-market price based on most recent comparable transaction or MSRB EMMA reference data.

**Minimum Quote Sizes:**

- Standard quote: **$100,000 notional minimum** (100 tokens @ $1,000 face value)
- Enhanced quote for investment-grade: **$250,000 notional minimum**

**Uptime Requirements:**

- Market hours: 9:00 AM - 4:00 PM ET, Monday-Friday (excluding federal holidays)
- Minimum uptime: **95% during market hours**
- Advance notice required for scheduled maintenance (48 hours minimum)

---

**Price Improvement Obligation**

Broker-dealers must demonstrate price improvement versus:

1. **Primary benchmark:** Last comparable trade reported on MSRB EMMA system

2. **Secondary benchmark:** Yield-to-maturity of comparable municipal securities with similar:
    - Credit rating (within one notch)
    - Maturity date (within 6 months)
    - Geographic region
    - Security type (GO bond vs. Revenue bond)

**Price Improvement Verification:**

- Executed trade yield must be ≥5 basis points better for buyers (lower yield = better price)
- Executed trade yield must be ≤5 basis points worse for sellers (higher yield = better price)
- Verification against Bloomberg Municipal Bond Index or equivalent

**Exception Conditions:**

- Market disruption (defined as >100 basis points movement in MMD AAA index in single day)
- Credit event affecting issuer (rating downgrade, default notice)
- Force majeure activation of Emergency Override Protocol

---

### F.2.2 Alternative Trading System (ATS) Integration

The pilot program encourages integration with SEC-registered Alternative Trading Systems to enhance price discovery and execution quality.

**Supported ATS Models**

**Model 1: Request-for-Quote (RFQ) System**

- Investor submits quote request with desired quantity and direction (buy/sell)
- Multiple broker-dealers respond with firm quotes within 60 seconds
- Investor selects best execution
- Settlement via atomic T+0 or netted T+1 based on investor preference

**Model 2: Central Limit Order Book (CLOB)**

- Continuous display of aggregated bids and offers from multiple broker-dealers
- Limit orders, market orders, and stop orders supported
- Price-time priority matching engine
- Real-time market depth visibility

**Model 3: Periodic Auction**

- Daily batch auction at 2:00 PM ET for price discovery
- All orders submitted during accumulation period (12:00 PM - 2:00 PM)
- Single clearing price maximizes executed volume
- Atomic settlement immediately post-auction

**ATS Connectivity Standards**

**Technical Requirements:**

- FIX Protocol 5.0 or higher for order routing
- ISO 20022 messaging for settlement instructions
- RESTful API for real-time market data distribution
- WebSocket connections for order book updates

**Regulatory Compliance:**

- Full compliance with Regulation ATS (17 CFR 242.300-303)
- Fair access requirements for all qualified investors
- Order display and execution obligations
- Recordkeeping and reporting to SEC per Rule 301(b)(2)

---

### F.2.3 Liquidity Metrics and Reporting

**Quarterly Liquidity Assessment:**

Participating broker-dealers submit the following metrics to FinHub staff:

1. **Quoted Spread Analysis:**
    - Average bid-ask spread (time-weighted during market hours)
    - Maximum spread observed
    - Percentage of time spread exceeded maximum threshold
2. **Market Depth:**
    - Average quote size at best bid/offer
    - Total quoted liquidity within 10 basis points of mid-market
    - Number of price levels with active quotes
3. **Execution Quality:**
    - Average time to execution (from order submission to confirmation)
    - Percentage of orders receiving price improvement
    - Fill rate (percentage of orders fully executed vs. partial fills)
4. **Transaction Costs:**
    - Effective spread (difference between execution price and mid-market at order time)
    - Realized spread (difference between execution price and mid-market 5 minutes post-trade)
    - Price impact (market movement caused by large orders)

**Public Disclosure:**

- Aggregated liquidity statistics published monthly on pilot program website
- Individual broker-dealer performance metrics remain confidential to SEC
- Annual liquidity report comparing pilot securities vs. traditional municipal bonds

---

### F.2.4 Investor Access Mechanisms

**Fractional Ownership Structure**

To enhance retail investor access in future pilot expansion phases:

**Minimum Investment Amounts:**

- Phase 1 (current): $1,000 per token (institutional focus)
- Phase 2 (potential): $100 fractional tokens (accredited investors)
- Phase 3 (potential): $10 micro-tokens (retail investors subject to additional protections)

**Fractional Token Implementation:**

```
Smart Contract Logic:
- Base unit: 1 token = $1,000 face value (indivisible for Phase 1)
- Fractional unit: 0.01 token = $10 face value (Phase 2+)
- Ownership registry tracks balances to 2 decimal places
- Interest payments distributed proportionally to fractional holdings
```

**Custody Considerations:**

- Fractional tokens held in omnibus accounts by registered broker-dealers
- Individual beneficial ownership recorded in subsidiary ledger
- Full Exchange Act Rule 15c3-3 customer protection applicable

---

## F.3 CROSS-LEDGER INTEROPERABILITY STANDARDS

### F.3.1 Multi-Platform Operational Scenarios

While the pilot program initially operates on a single permissioned ledger (JPMorgan Onyx or equivalent), the framework anticipates future scenarios requiring interoperability:

**Scenario 1: Multiple Municipalities on Different Platforms**

**Challenge:**

- City A issues tokenized bonds on JPMorgan Onyx
- City B issues tokenized bonds on Goldman Sachs Digital Assets Platform
- Investor holds portfolio of both and desires unified custody/reporting

**Interoperability Requirements:**

- Cross-platform ownership verification via cryptographic proofs
- Standardized data export formats for portfolio aggregation
- Common API standards for broker-dealer integration

**Scenario 2: Platform Migration**

**Challenge:**

- Municipality wishes to migrate existing tokenized securities from Platform X to Platform Y
- Must preserve investor ownership rights and transaction history
- Cannot create service disruption or settlement risk

**Migration Protocol:**

- Atomic snapshot of ownership registry at migration timestamp
- Cryptographic commitment to historical blockchain state
- Dual-operation period with synchronized registries
- Gradual investor opt-in to new platform

**Scenario 3: Cross-Chain Atomic Swaps**

**Challenge:**

- Investor wishes to exchange tokenized municipal bond A for tokenized municipal bond B
- Securities exist on different distributed ledgers
- Requires simultaneous settlement to eliminate counterparty risk

**Technical Solution:**

- Hash Time-Locked Contracts (HTLCs) for cross-chain atomicity
- Trusted third-party escrow or decentralized oracle network
- Time-bound settlement windows with automatic rollback

---

### F.3.2 Data Portability Standards

To prevent vendor lock-in and ensure long-term investor protections, the pilot program commits to the following data portability standards:

**Ownership Record Export Format**

**Standard:** W3C Verifiable Credentials Data Model 1.1

**Implementation:**

```
{
  "@context": ["https://www.w3.org/2018/credentials/v1"],
  "type": ["VerifiableCredential", "MunicipalBondOwnership"],
  "issuer": "did:ethr:0x[contract_address]",
  "issuanceDate": "2026-01-15T00:00:00Z",
  "credentialSubject": {
    "id": "did:investor:0x[wallet_address]",
    "security": {
      "cusip": "MUNIXXXXXXX",
      "issuer": "City of Lakeview",
```

```
      "quantity": 500,
      "faceValue": 1000,
      "currency": "USD"
    },
    "acquisitionDate": "2026-01-15T14:30:00Z",
    "blockchain": {
      "network": "JPMorgan Onyx",
      "blockNumber": 12345,
      "transactionHash": "0xabc...def"
    }
  },
  "proof": {
    "type": "ML-DSA-65-Signature-2025",
    "created": "2026-01-15T14:30:05Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:ethr:0x[contract]#key-1",
    "signatureValue": "z58DAdF...xyzAB"
  }
}
```

**Benefits:**

- Platform-agnostic ownership verification
- Compatible with emerging digital identity standards (DID)
- Quantum-resistant signature scheme (ML-DSA-65)
- Machine-readable for automated portfolio management systems

---

**Transaction History Export Format**

**Standard:** ISO 20022 camt.053 (Bank-to-Customer Statement) extended for tokenized securities

**Key Fields:**

- Transaction date/time with microsecond precision
- Counterparty identification (pseudonymized for privacy)
- Transaction type (primary issuance, secondary purchase, interest payment, redemption)
- Settlement mode (atomic T+0 vs. netted T+1)
- Blockchain reference (block number, transaction hash)

- Cryptographic proof of transaction finality

**Export Frequency:**

- On-demand export via investor portal or broker-dealer API
- Automatic monthly statement generation
- Complete historical export available upon platform shutdown

---

**F.3.3 Technical Interoperability Framework**

**Layer 1: Blockchain Connectivity**

**Supported Standards:**

- **ISO 22739:** Vocabulary for distributed ledger technology
- **ISO/AWI 23257:** Reference architecture for DLT systems
- **ISO/AWI 23455:** Legally binding smart contracts (under development)

**Protocol Bridges:**

- Native atomic swaps via Hash Time-Locked Contracts (HTLCs)
- Relay chain architecture for cross-ledger message passing
- Interledger Protocol (ILP) for payment settlement coordination

**Layer 2: Identity and KYC Interoperability**

**Challenge:** Investor verified on Platform A must be recognizable on Platform B without re-verification

**Solution: Federated Identity with Privacy Preservation**

**Implementation:**

```
Investor completes KYC at Broker-Dealer X
    ↓
BD X issues Verifiable Credential (VC) with attestations:
    - Accredited investor status ✓
    - AML screening completed ✓
    - Jurisdiction: United States ✓
    - Validity period: 12 months ✓
    ↓
Investor presents VC to Platform Y
    ↓
Platform Y verifies:
    - Cryptographic signature from trusted BD X
```

```
    - Credential not revoked (check revocation registry)
    - Validity period not expired
    ↓
Platform Y grants trading authorization WITHOUT seeing PII
```

**Privacy Mechanism:** Zero-Knowledge Proofs

- Investor proves "I am accredited" without revealing net worth
- Investor proves "I passed AML screening" without revealing identity
- Platform verifies proofs cryptographically without trusted intermediary

**Standards Compliance:**

- W3C Decentralized Identifiers (DIDs) specification
- W3C Verifiable Credentials Data Model
- NIST SP 800-63-3 Digital Identity Guidelines

---

**Layer 3: Smart Contract Interoperability**

**Challenge:** Smart contracts on different platforms use different programming languages (Solidity vs. Daml vs. Chaincode)

**Solution: Common Business Logic Layer**

**Approach:**

- Abstract core settlement logic into platform-independent specification
- Use formal methods (TLA+, Alloy) to specify business rules
- Generate platform-specific smart contracts from common specification

**Example - Use-of-Proceeds Validation:**

**Platform-Independent Specification (pseudocode):**

```
RULE validate_disbursement:
    INPUT: request(amount, purpose, recipient, signers)

    CHECK purpose IN approved_uses_list
    CHECK length(signers) >= minimum_signatures
    CHECK all(signers) IN authorized_officials

    IF all_checks_pass THEN
        RETURN approve(request)
    ELSE
```

```
        RETURN reject(request, reason)
    END IF
END RULE
```

**Platform-Specific Implementations:**

- Solidity (Ethereum/Onyx): Compiled smart contract
- Daml (Corda): Daml template with validation logic
- Chaincode (Hyperledger Fabric): Go implementation

**Verification:**

- Formal equivalence checking ensures all implementations match specification
- Cross-platform test suite validates identical behavior

---

### F.3.4 Governance for Interoperability Standards

**Pilot-Phase Governance**

**Technical Standards Committee:**

- Representatives from participating municipalities (2 seats)
- Representatives from broker-dealers (2 seats)
- Representatives from platform providers (2 seats)
- SEC FinHub observer (non-voting)
- Independent technical experts (2 seats)

**Mandate:**

- Review and approve data export formats
- Evaluate cross-platform migration requests
- Recommend updates to interoperability standards
- Coordinate with international standards bodies (ISO/TC 307)

**Meeting Frequency:** Quarterly, with emergency sessions as needed

**Decision-Making:** Consensus-based, with fallback to supermajority (7 of 10 votes)

---

**Post-Pilot Institutionalization**

If pilot demonstrates success and SEC authorizes permanent framework, interoperability governance transitions to:

**Option 1: Industry Consortium**

- Similar to DTCC governance model
- Funded by participating platforms and broker-dealers
- Operates as SRO subject to SEC oversight

**Option 2: Integration with Existing SRO**

- MSRB expands mandate to include tokenized securities standards
- Leverages existing regulatory relationships and expertise
- Maintains continuity with traditional municipal bond market

**Option 3: New Self-Regulatory Organization**

- Dedicated SRO for digital securities (all asset classes, not just municipals)
- Modeled on FINRA but focused on blockchain/DLT systems
- Requires Congressional authorization and SEC rulemaking

---

### F.4 IMPLEMENTATION TIMELINE

**Phase 1: Pilot Program (Months 1-18)**

**Interoperability Focus:**

- Establish data export standards
- Document APIs for broker-dealer integration
- Create reference implementations for common operations

**Deliverables:**

- Technical standards documentation (ISO-format)
- Open-source SDK for secondary market connectivity
- Quarterly interoperability assessment reports to SEC

**Phase 2: Expansion (Months 19-36, if approved)**

**Interoperability Focus:**

- Enable cross-platform ownership verification
- Pilot cross-chain atomic swaps (limited scope)
- Integration with 2+ alternative platforms

**Deliverables:**

- Interoperability compliance certification program
- Platform migration playbook
- Cross-platform transaction testing results

**Phase 3: Institutionalization (Months 37+, if successful)**

**Interoperability Focus:**

- Submit standards to ISO/TC 307 for formal standardization
- Establish permanent governance structure
- Achieve interoperability with international frameworks (EU MiCA, Singapore MAS)

**Deliverables:**

- ISO/AWI proposal for tokenized municipal securities
- International regulatory mapping guide

- Global interoperability demonstration (US-EU-Asia)

---

**CONCLUSION**

This appendix addresses three critical operational dimensions that ensure the Tokenized Municipal Instruments framework operates with institutional-grade reliability, liquidity, and future-proofing:

1. **Cybersecurity Incident Response:** Defined RTOs/RPOs and structured protocols ensure rapid recovery from incidents while maintaining investor protection and regulatory transparency.
2. **Secondary Market Liquidity:** Market-making obligations, ATS integration, and fractional ownership pathways create viable secondary markets essential for investor confidence and price discovery.
3. **Interoperability Standards:** Data portability, cross-platform protocols, and governance mechanisms prevent vendor lock-in and position the framework for long-term sustainability as the tokenization ecosystem evolves.

These enhancements demonstrate the pilot program's commitment to operational excellence and risk management aligned with SEC expectations for innovative market infrastructure.

---

# APPENDIX G: STRATEGIC ENHANCEMENTS FOR REGULATORY ROBUSTNESS

To address specific regulatory priorities regarding civil liability, environmental data integrity, and market continuity, the Pilot Program incorporates three additional strategic frameworks derived from advanced RegTech principles.

### G.1 Technology Liability and Insurance Framework

To mitigate the specific risks associated with smart contract operations and potential technological failures, participating entities are required to maintain a tiered insurance structure that goes beyond standard errors and omissions (E&O) coverage. This framework ensures that investors have clear financial recourse in the event of code-based failures that are not covered by the underlying municipal obligation.

**Minimum Coverage Requirements by Role:**

- **Custodians:** Must maintain Professional Liability coverage of at least $10M plus 2% of Assets Under Custody (AUC), alongside a Crime/Fidelity bond minimum of $5M.
- **Validators & Oracle Operators:** Required to hold E&O insurance of $2M plus a "Technology Performance Bond" or equivalent coverage of at least $3M to cover potential liability resulting from inaccurate data feeds or consensus failures.
- **Smart Contract Guarantee Fund:** A pooled reserve fund contributed to by participating technology providers, capped at 2% of total issuance volume, to serve as a first-loss tranche

for purely technical failures (e.g., gas fee anomalies, unintended execution loops) that do not trigger major insurance claims.

### G.2 Anti-Greenwashing & Impact Verification Oracles

For issuances designated as "Green Bonds" or "Sustainability Notes" (such as the City of Lakeview water treatment example), the Pilot implements a "Proof-of-Impact" layer to prevent greenwashing and ensure programmable compliance with environmental objectives.

**Operational Mechanism:**

- **IoT Integration:** Funds designated for specific infrastructure projects are linked to "Impact Oracles" that ingest data from certified smart meters and IoT devices (e.g., water flow meters, energy consumption monitors).
- **Programmable Release of Funds:** The smart contract can be configured to release tranches of funding or adjust interest rate spreads only upon receipt of cryptographically signed data verifying that specific physical milestones have been met (e.g., installation of equipment, verified reduction in energy usage).
- **Third-Party Validation:** All impact data must be attested to by an accredited third-party validator before being accepted by the smart contract, ensuring an independent chain of custody for environmental claims.

### G.3 Universal Legacy Compatibility (CUSIP Mirroring)

To strictly eliminate "vendor lock-in" risks and ensure absolute market continuity, the Pilot adopts a "Shadow CUSIP" standard for all tokenized instruments.

**Wind-Down and Continuity Protocol:**

- **1:1 CUSIP Mapping:** Every Tokenized Municipal Security issued in the Pilot is inextricably linked to a standard CUSIP number reserved at issuance. The Token serves as the primary settlement record during the Pilot.
- **Fail-Safe Reversion:** In the event of Pilot termination, platform discontinuation, or regulatory directive, the "Digital Twin" relationship is dissolved, and the ownership registry is automatically exported to the Depository Trust & Clearing Corporation (DTCC) format. The "Shadow CUSIP" becomes the primary record, and the securities convert instantly to traditional book-entry form without legal friction or asset repricing.
- **No Stranded Assets:** This mechanism guarantees that no investor can be left with a "stranded" digital asset, as the legal and operational existence of the security is fully portable to legacy infrastructure at any moment.

---

# CONCLUSION

This Concept Paper presents a comprehensive framework for a time-limited regulatory pilot program enabling the issuance and settlement of tokenized municipal securities within a fully

regulated environment designed to preserve investor protection while evaluating the operational, economic, and legal implications of distributed ledger technology in municipal debt markets.

The proposal is grounded in three fundamental commitments:

**First**, that all tokenized securities remain subject to the full scope of federal securities laws, Municipal Securities Rulemaking Board rules, and established investor protection standards, with no exemptions, forbearance, or novel legal classifications sought.

**Second**, that traditional legal instruments govern the substantive rights and obligations of all parties, with distributed ledger technology serving purely as operational infrastructure that enhances rather than replaces established legal frameworks.

**Third**, that incumbent financial intermediaries are preserved and enhanced rather than disintermediated, ensuring that innovation builds upon rather than disrupts existing regulatory relationships and market structures.

The pilot offers significant potential benefits to municipal issuers, investors, intermediaries, and regulatory authorities. For issuers, particularly mid-sized jurisdictions facing disproportionate costs under traditional underwriting models, tokenized securities may reduce issuance expenses, enhance transparency, and broaden access to capital markets. For investors, tokenized securities offer enhanced liquidity potential, automated compliance, and real-time visibility into use-of-proceeds deployment. For intermediaries, the pilot demonstrates pathways for technological modernization that leverage existing capabilities and regulatory relationships. For regulators, the pilot generates empirical data informing future policy deliberations regarding market structure evolution and the integration of distributed ledger technology with traditional legal and operational frameworks.

**Building on Proven Success:** This proposal is strengthened significantly by the successful real-world precedent established by the City of Quincy, Massachusetts, in collaboration with JPMorgan Chase. The Quincy transaction demonstrated that tokenized municipal securities can:

- Operate in full compliance with existing securities laws and MSRB regulations
- Attract institutional investment from major asset managers such as BlackRock
- Deliver measurable operational benefits including T+0 settlement, reduced intermediation costs, and enhanced transparency
- Function within established legal frameworks without requiring novel exemptions or regulatory forbearance

The proposal incorporates comprehensive safeguards designed to ensure that experimentation occurs within carefully controlled parameters that prioritize investor protection. Limited scale and duration ensure that the pilot remains a modest experiment generating valuable data without introducing systemic risks. Comprehensive reporting and oversight mechanisms ensure that the Commission maintains visibility into pilot operations and can intervene if concerns arise. Emergency Override Protocols ensure that human judgment and political accountability retain ultimate authority over automated systems.

**Technical Innovation and Long-Term Security:** The framework incorporates cutting-edge technical elements that demonstrate institutional sophistication and address legitimate long-term concerns:

- Post-quantum cryptography (NIST FIPS 203/204/205) ensures that securities issued during the pilot maintain robust cryptographic security throughout their entire lifecycle, even in the face of future quantum computing advances
- Enterprise-grade permissioned blockchain infrastructure (based on proven platforms such as JPMorgan Onyx) provides institutional-quality operational reliability and regulatory compliance capability
- Comprehensive oracle architecture enables secure integration with traditional market data providers and credit rating agencies
- Dual-mode settlement accommodates both instantaneous atomic settlement and compatibility with traditional clearing infrastructure

We respectfully submit this proposal for the Commission's consideration and welcome the opportunity to engage with FinHub staff to refine the framework, address questions, and demonstrate our commitment to responsible innovation within the boundaries of existing regulatory frameworks. We stand ready to provide additional information, participate in consultations with Commission staff and stakeholders, and work collaboratively to design a pilot program that advances the public interest while maintaining the investor protection principles that have long guided securities regulation.

The evolution of market infrastructure to incorporate emerging technologies represents both opportunity and responsibility. We believe this pilot program strikes an appropriate balance between innovation and caution, between operational efficiency and investor protection, between technological modernization and preservation of essential regulatory safeguards. We look forward to the Commission's evaluation of this proposal and to the possibility of contributing to the thoughtful, data-driven evolution of capital formation mechanisms in the digital era.

---

# REFERENCES AND FUNDAMENTAL STANDARDS

## Tokenized Municipal Instruments Under Distributed Ledger Technology

### Regulatory Sandbox Framework for Market Modernization

**Document Version:** November 2025
**Prepared for:** U.S. Securities and Exchange Commission Strategic Hub for Innovation and Financial Technology (FinHub)

---

# I. PRIMARY REGULATORY AUTHORITIES

## A. Securities and Exchange Commission

**Federal Securities Laws:**

- Securities Act of 1933, Section 3(a)(2) – Municipal Securities Exemption
- Securities Exchange Act of 1934, Rule 15c3-3 – Customer Protection (Custody Requirements)
- Securities Exchange Act of 1934, Rule 17Ad-9 – Transfer Agent Recordkeeping

**SEC Division of Corporation Finance Guidance:**

- "Offerings and Registrations of Securities in the Crypto Asset Markets" (April 10, 2025)
- Statement on Certain Proof-of-Work Mining Activities (March 20, 2025)
- Statement on Certain Liquid Staking Activities (August 5, 2025)

**Project Crypto Initiative:**

- Chairman Paul S. Atkins, "Remarks on Digital Asset Taxonomy Framework" (November 12, 2025)
- SEC Crypto Task Force, Digital Asset Regulatory Clarity Initiative (2025)

## B. Municipal Securities Rulemaking Board

**Core Rules:**

- MSRB Rule G-17: Conduct of Municipal Securities and Municipal Advisory Activities
- MSRB Rule G-32: Disclosures in Connection with Primary Offerings
- MSRB Rule G-34: CUSIP Numbers, New Issue, and Market Information Requirements

**Electronic Municipal Market Access (EMMA) System:**

- Continuing Disclosure Filing Requirements
- Material Event Notice Standards
- Real-Time Transaction Reporting

# II. TECHNICAL STANDARDS AND SPECIFICATIONS

## A. Post-Quantum Cryptography (NIST Standards)

**Federal Information Processing Standards (FIPS):**

- **FIPS 203** – Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), derived from CRYSTALS-Kyber. Published August 13, 2024.
- **FIPS 204** – Module-Lattice-Based Digital Signature Algorithm (ML-DSA), derived from CRYSTALS-Dilithium. Published August 13, 2024.
- **FIPS 205** – Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), derived from SPHINCS+. Published August 13, 2024.

**Additional Selected Algorithms:**

- **HQC (Hamming Quasi-Cyclic)** – Backup key encapsulation mechanism selected for standardization March 11, 2025. Expected finalization 2027.

**NIST Reports:**

- NIST IR 8545: Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process (2025)
- NIST IR 8547: Transition to Post-Quantum Cryptography Standards (November 2024)
- NIST SP 800-227: Recommendations for Key Encapsulation Mechanisms (Draft, January 2025)

**Migration Guidance:**

- White House National Security Memorandum 10 (NSM-10) – Target completion 2035 for federal systems
- Quantum Computing Cybersecurity Preparedness Act

## B. Cryptographic Security Standards

**Hardware Security Modules:**

- Federal Information Processing Standards Publication 140-3 (FIPS 140-3) – Security Requirements for Cryptographic Modules, Level 3 or higher

**Key Management:**

- NIST SP 800-57: Recommendation for Key Management
- Multi-Party Computation and Threshold Signature Schemes (Shamir's Secret Sharing)

## C. Enterprise Blockchain Platforms

**Reference Implementation:**

- JPMorgan Chase Onyx Digital Assets (Kinexys) – First live municipal blockchain bond (Quincy, MA, April 2024)

**Alternative Platforms:**

- Hyperledger Fabric 2.5+ (Linux Foundation)
- R3 Corda 5.x Enterprise (R3 Holdings)
- ConsenSys Quorum (Enterprise Ethereum variant)

**Consensus Mechanisms:**

- Istanbul Byzantine Fault Tolerant (IBFT)
- QBFT (Quorum Byzantine Fault Tolerant)
- Practical Byzantine Fault Tolerance (PBFT) variants

---

# III. MARKET PRECEDENTS AND CASE STUDIES

## A. City of Quincy, Massachusetts (2024)

**Transaction Details:**

- **Issuance Date:** April 2024
- **Principal Amount:** $10 million (tax-exempt, seven-year general obligation bonds)
- **Platform:** JPMorgan Onyx (Kinexys Digital Assets)
- **Underwriter:** JPMorgan Chase & Co. (sole underwriter)
- **Institutional Validation:** BlackRock iShares Short Maturity Municipal Bond Active ETF (MEAR) purchased $6.5 million (65% of issuance) in December 2024

**Technical Implementation:**

- Digital Debt Service on permissioned blockchain
- Delivery-versus-payment settlement in near real-time
- Elimination of traditional Issuing and Paying Agent
- Blockchain-based deposit accounts for proceeds receipt

**Operational Benefits Documented:**

- T+0 settlement capability
- Reduced settlement risk through simultaneous asset/cash exchange
- Enhanced transparency via permanent on-chain records
- Decreased reliance on intermediaries and third parties
- Potential for programmable settlement and precise timing specification

**Sources:**

- JPMorgan Chase Press Release: "JPMorganChase launches the Digital Debt Service with the first live municipal blockchain-based bond issuance in the U.S." (November 12, 2024)
- CFO.com Interview with Eric Mason, CFO City of Quincy (January 31, 2025)
- BlackRock Holdings Disclosure, iShares MEAR ETF (December 2024)

## B. Alphaledger Municipal Bond Platform (2022)

**Implementation:**

- Recorded three U.S. municipal bond issuances on permissioned blockchain
- Parallel recordkeeping alongside traditional systems
- Transfer agent subsidiary and FINRA-registered broker-dealer (Iris Technology)

**Source:**

- Ledger Insights: "Alphaledger originates 3 municipal bonds on blockchain" (December 19, 2022)

### C. Moody's Ratings On-Chain Integration (2025)

**Proof-of-Concept:**

- Credit rating data embedded into tokenized municipal securities
- Solana blockchain implementation with Alphaledger
- API-based data transfer from off-chain systems to on-chain tokens

**Significance:**

- Demonstrates oracle architecture for trusted third-party data integration
- Validates real-time credit assessment availability for tokenized assets

**Source:**

- CoinDesk: "Moody's Ratings Brings Credit Rating to Solana in Real World Asset Tokenization Trial" (June 11, 2025)

### D. Other Relevant Precedents

**Goldman Sachs Digital Asset Platform:**

- Michigan State University consideration of $38 million municipal bond issuance (2024)
- Demonstrates institutional interest from multiple major financial institutions

**New Hampshire Business Finance Authority:**

- $100 million Bitcoin-backed municipal bond (November 2025)
- First digital-asset-collateralized municipal security

---

## IV. INDUSTRY STANDARDS AND BEST PRACTICES

### A. Securities Industry and Financial Markets Association (SIFMA)

**Digital Asset Framework Submissions:**

- "SEC Crypto RFI Initial Response" (May 2025)
- Distinction between "tokenized securities" and "security tokens"
- Custody requirements for digital assets by broker-dealers and investment advisers

## B. International Organization for Standardization (ISO)

**Blockchain and Distributed Ledger Technologies:**

- ISO/TC 307 Technical Committee Standards
- Focus on terminology, reference architecture, and security

## C. Financial Stability Board (FSB)

**Global Regulatory Framework:**

- "Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets" (July 2023)
- High-level recommendations for activities and markets

---

# V. LEGAL AND COMPLIANCE FRAMEWORKS

## A. Bank Secrecy Act and Anti-Money Laundering

**Customer Identification Program (CIP):**

- 31 CFR § 1020.220 – Customer identification requirements for banks
- 31 CFR § 1023.220 – Customer identification requirements for broker-dealers

**Suspicious Activity Reporting:**

- FinCEN SAR requirements for financial institutions
- Digital asset-specific guidance

## B. Office of Foreign Assets Control (OFAC)

**Sanctions Screening:**

- OFAC Specially Designated Nationals (SDN) List
- Sectoral Sanctions Identifications List
- Digital currency address screening protocols

## C. State Municipal Finance Laws

**Uniform Municipal Bond Act (Model Legislation):**

- Issuance authorization procedures
- Debt service requirements
- Use-of-proceeds restrictions

**State-Specific Provisions:**

- Authorization for electronic securities (various state statutes)
- Municipal charter requirements for debt issuance

---

# VI. ACADEMIC AND RESEARCH FOUNDATIONS

## A. Distributed Ledger Technology

**Consensus Mechanisms:**

- Castro, M., & Liskov, B. (1999). "Practical Byzantine Fault Tolerance." *Proceedings of the Third Symposium on Operating Systems Design and Implementation.*
- Buchman, E. (2016). "Tendermint: Byzantine Fault Tolerance in the Age of Blockchains." (Foundation for modern BFT implementations)

**Smart Contract Security:**

- Atzei, N., Bartoletti, M., & Cimoli, T. (2017). "A Survey of Attacks on Ethereum Smart Contracts (SoK)." *International Conference on Principles of Security and Trust.*

## B. Municipal Finance

**Market Structure:**

- Securities Industry and Financial Markets Association (SIFMA) Research: U.S. Municipal Bond Market Statistics (2025)
- Approximately $4 trillion market with 13,000+ annual issuances (2021 data)
- Majority of issuances under $50 million principal amount

**Tokenization Benefits Analysis:**

- Clifton, J., et al. (2023). "Blockchain Technology in Public Finance: The Berkeley Municipal Bond Case Study." (Referenced in academic literature)

---

# VII. GOVERNMENTAL POLICY DOCUMENTS

## A. Executive Branch

**White House Initiatives:**

- Executive Order 14067: "Ensuring Responsible Development of Digital Assets" (March 9, 2022)
- National Security Memorandum 10 (NSM-10): Post-Quantum Cryptography Migration Timeline

## B. Congressional Legislation

**Digital Asset Market Clarity (CLARITY) Act of 2025:**

- Title V, Section 503: Strategic Hub for Innovation and Financial Technology (FinHub) establishment
- Section 508: Study on tokenized securities and derivatives products

**GENIUS Act:**

- Public Law No. 119-27 (Signed July 18, 2025)

- Stablecoin regulatory framework with relevance to fiat-referenced digital currencies

---

# VIII. TECHNICAL DOCUMENTATION REFERENCES

## A. Blockchain Platform Documentation

**JPMorgan Onyx (Kinexys):**

- Technical Architecture Whitepaper (available through JPMorgan institutional channels)
- Digital Debt Service Product Specifications

**Hyperledger Fabric:**

- "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains" (2018)
- Version 2.5+ Release Documentation (Linux Foundation)

**R3 Corda:**

- "Corda: An Introduction" – R3 Technical Whitepaper
- Enterprise Edition 5.x Documentation

## B. Oracle Network Standards

**Chainlink Oracle Networks:**

- Decentralized oracle architecture for off-chain data integration
- Multiple independent data providers with cryptographic attestation

**API3 Data Feeds:**

- First-party oracle solutions for financial market data

---

# IX. REGULATORY EXAMINATION AND SUPERVISION

## A. Federal Banking Agencies

**Office of the Comptroller of the Currency (OCC):**

- Interpretive Letter #1179: National Bank and Federal Savings Association Authority to Use New Technologies (January 2022)
- "Digital Asset Custody by Banks" guidance

**Federal Reserve:**

- Supervision and Regulation Letters on digital asset activities
- Payment system modernization initiatives

**Federal Deposit Insurance Corporation (FDIC):**

- Digital asset risk management guidance for insured depository institutions

### B. Self-Regulatory Organizations

**Financial Industry Regulatory Authority (FINRA):**

- Regulatory Notice 22-08: FINRA Reminds Firms of Their Regulatory Obligations Relating to Recommendations of Crypto Assets
- Broker-dealer supervision requirements for digital securities

---

# X. CONTINUING PROFESSIONAL EDUCATION

## A. Industry Associations

**Government Finance Officers Association (GFOA):**

- Best practices for municipal debt management
- Technology adoption guidelines for local governments

**National Association of Bond Lawyers (NABL):**

- Legal framework for digital securities representation
- Master Indenture modernization for blockchain integration

## B. Academic Institutions

**MIT Digital Currency Initiative:**

- Research on central bank digital currencies and tokenized assets
- Technical standards development

**Stanford Center for Blockchain Research:**

- Cryptographic protocols for financial applications
- Smart contract formal verification methodologies

---

# XI. SUPPLEMENTARY INDUSTRY REPORTS

## A. Financial Market Infrastructure

**Depository Trust & Clearing Corporation (DTCC):**

- "Digital Asset and Distributed Ledger Technology" research reports
- Settlement infrastructure modernization studies

**Securities Industry and Financial Markets Association (SIFMA):**

- Municipal bond market liquidity studies
- Technology adoption in fixed income markets

## B. Consulting and Professional Services

**Deloitte Blockchain and Digital Assets:**

- "Blockchain in Capital Markets" industry analysis
- Regulatory compliance frameworks for tokenized securities

**PwC Digital Assets:**

- "Global Crypto Regulation Report 2025"
- Institutional adoption studies

---

# XII. INTERNATIONAL REGULATORY FRAMEWORKS

## A. European Union

**Markets in Crypto-Assets Regulation (MiCA):**

- Comprehensive digital asset regulatory framework (effective 2024-2025)
- Tokenized securities classification and supervision

## B. United Kingdom

**Financial Conduct Authority (FCA):**

- Cryptoasset regulatory framework
- Distributed ledger technology guidance for financial institutions

## C. Switzerland

**Swiss Financial Market Supervisory Authority (FINMA):**

- Guidelines for ICOs and token classifications
- DLT trading facility licensing

---

# XIII. IMPLEMENTATION RESOURCES

## A. Open-Source Tools

**Smart Contract Development:**

- OpenZeppelin Contracts (audited smart contract libraries)
- Truffle Suite (development framework)
- Hardhat (Ethereum development environment)

**Formal Verification:**

- Certora Prover (smart contract verification)
- Runtime Verification (K Framework)

## B. Auditing Services

**Smart Contract Security Auditors:**

- Trail of Bits
- ConsenSys Diligence

- OpenZeppelin Security Audits

---

# CONCLUSION

This reference framework provides the foundational regulatory, technical, and industry standards underpinning the proposed pilot program for tokenized municipal instruments. The integration of established precedents (particularly the Quincy-JPMorgan case), current SEC policy frameworks (Project Crypto), and cutting-edge technical standards (NIST post-quantum cryptography) demonstrates that the proposal operates at the intersection of proven market practices and forward-looking innovation.

The comprehensive citation of regulatory authorities, technical specifications, and industry best practices ensures that the pilot program maintains full compliance with existing legal frameworks while demonstrating institutional sophistication appropriate for consideration by the Securities and Exchange Commission's Strategic Hub for Innovation and Financial Technology.

---

**Document Prepared:** November 2025
**For Official Use:** SEC FinHub Pilot Program Application
**Classification:** Public Regulatory Submission

---

# APPENDIX: KEY CONTACTS AND RESOURCES

## Regulatory Authorities

- **SEC FinHub:** finhub@sec.gov
- **MSRB:** www.msrb.org
- **FINRA:** www.finra.org

## Technical Standards Organizations

- **NIST Post-Quantum Cryptography:** csrc.nist.gov/projects/post-quantum-cryptography
- **Linux Foundation (Hyperledger):** www.hyperledger.org
- **R3:** www.r3.com

## Industry Associations

- **SIFMA:** www.sifma.org
- **GFOA:** www.gfoa.org
- **NABL:** www.nabl.org

## Market Infrastructure

- **EMMA (MSRB):** emma.msrb.org
- **DTCC:** www.dtcc.com

---

*End of References and Fundamental Standards Document*