PACT Protocol: Technical Compliance Architecture for Securities Regulation

A Deterministic, AI-Attested Compliance Framework Aligned with SEC Rule 17a-4, FINRA Rule 4511, and OCC Heightened Standards

Document Type: IEEE-Style Technical Whitepaper
Prepared by: ARKA Systems LLC
Version: 1.0
Date: December 2024
Classification: Regulator Staff Reference

Abstract

This whitepaper presents the technical architecture of the PACT Protocol, a compliance operating system designed to address the regulatory requirements of modern financial institutions. PACT implements deterministic rule execution through a formally-specified virtual machine, AI-assisted analysis with cryptographic attestation, and a permissioned blockchain for immutable audit trail preservation. This document examines how PACT's architecture aligns with SEC Rule 17a-4 (records preservation), FINRA Rule 4511 (books and records), and OCC Heightened Standards for large financial institutions. The system provides mathematical guarantees of execution consistency while leveraging large language models for risk assessment and narrative generation—always under human supervision and with complete audit provenance.

Keywords: Regulatory Technology, Deterministic Execution, Blockchain Attestation, AI Compliance, SEC 17a-4, FINRA 4511, Record Retention

1. Introduction

1.1 Regulatory Context

Financial institutions operate under a complex web of recordkeeping and compliance requirements. SEC Rule 17a-4 mandates that broker-dealers preserve records in a non-rewriteable, non-erasable format (WORM compliance). FINRA Rule 4511 requires members to make and preserve books and records as prescribed by FINRA rules and the Exchange Act. The OCC's Heightened Standards establish expectations for risk governance at large insured national banks.

Current compliance systems face fundamental limitations:

- **Non-determinism:** Rules encoded in procedural code produce variable outputs
- **Mutable Audit Trails:** Database-backed logs can be altered post-facto
- **Unverified AI:** Machine learning models operate as black boxes without attestation
- **Fragmented Architecture:** Compliance functions siloed across incompatible systems

1.2 PACT Protocol Overview

PACT (Programmable Automated Compliance Technology) addresses these limitations through a four-layer architecture:

1. **PACT Engine:** Deterministic rules execution with bit-exact reproducibility
2. **PACT Cloud:** Multi-tenant compliance workflow orchestration
3. **PACT AI:** Supervised artificial intelligence with cryptographic attestation
4. **PACT Blockchain:** Permissioned Proof-of-Authority ledger for audit anchoring

This paper details each layer's technical implementation and regulatory alignment.

2. Deterministic Execution: The Rule-Time Virtual Machine

2.1 The Non-Determinism Problem

Traditional compliance systems implement rules in general-purpose programming languages (Java, Python, C#). These implementations suffer from inherent non-determinism:

- Floating-point arithmetic varies across hardware architectures
- Hash table iteration order is undefined
- Timestamp generation depends on system clock
- Random number generation introduces variability
- Thread scheduling affects execution order

Such non-determinism means the same transaction, evaluated twice, may produce different compliance outcomes—an unacceptable condition for regulatory enforcement.

2.2 PACT Engine Architecture

PACT Engine implements a deterministic virtual machine with the following guarantees:

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ PACT RULE EXECUTION ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ Input: Event E, RuleSet R, Context C ■
■ Output: Decision D, Audit Trail A ■
■ ■
■ Guarantee: ∀ nodes N■, N■: ■
■ Execute(E, R, C) on N■ = Execute(E, R, C) on N■ ■
■ ■
■ Properties: ■
■ • Bit-exact reproducibility ■
■ • Total ordering of operations ■
■ • Deterministic timestamp assignment ■
■ • Canonical serialization ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

2.3 Rule Domain-Specific Language

PACT rules are expressed in a declarative JSON-based DSL with formal semantics:

```
{
"id": "AML-001",
"version": "2024.1.0",
"name": "Large Cash Transaction Report",
"conditions": {
"and": [
{ "field": "transaction.type", "operator": "equals", "value": "CASH" },
{ "field": "transaction.amount", "operator": "greaterThan", "value": 10000 },
{ "field": "entity.type", "operator": "in", "value": ["INDIVIDUAL", "BUSINESS"] }
]
},
"actions": [
{ "type": "FLAG", "severity": "HIGH", "code": "CTR_REQUIRED" },
{ "type": "NOTIFY", "channel": "COMPLIANCE_QUEUE" }
],
"metadata": {
"regulation": "31 CFR 1010.311",
"effectiveDate": "2024-01-01",
"jurisdiction": "US"
}
}
```

2.4 Execution Guarantees

Property	Implementation	Verification
Determinism	Fixed-point arithmetic, canonical ordering	Formal proof via property-based testing
Completeness	All rules evaluated for every event	Rule coverage analysis

Termination	No recursion, bounded iteration	Static analysis
Auditability	Full execution trace captured	Hash-chain verification

2.5 Alignment with SEC 17a-4

SEC Rule 17a-4(f) requires records to be preserved in a manner that:

- Preserves the records exclusively in a non-rewriteable, non-erasable format
- Verifies automatically the quality and accuracy of the storage media recording process
- Serializes the original and duplicate units of storage media
- Has the capacity to download indexes and records preserved

PACT Engine compliance:

- **Non-rewriteable:** All decisions are cryptographically hashed and anchored to blockchain
- **Quality Verification:** Merkle tree construction verifies data integrity
- **Serialization:** Canonical JSON serialization with deterministic ordering
- **Download Capability:** Full audit export via standardized API

---

3. AI-Attestation Model: Intelligence with Accountability

3.1 The AI Accountability Challenge

Large language models provide valuable capabilities for compliance:

- Natural language understanding of regulatory text
- Pattern recognition in transaction flows
- Narrative generation for examination responses
- Risk scoring based on entity behavior

However, AI systems pose regulatory challenges:

- **Non-determinism:** Same prompt may produce different outputs
- **Opacity:** Model reasoning is not directly auditable
- **Hallucination:** Models may generate plausible but incorrect outputs
- **Version Drift:** Model updates change behavior unpredictably

3.2 PACT AI Architecture

PACT implements a supervised AI model with cryptographic attestation:

3.3 AWS Bedrock Integration

PACT AI utilizes AWS Bedrock for foundation model access:

Capability	Model	Use Case
Risk Analysis	Claude 3.5 Sonnet	Entity risk scoring with narrative justification
Policy Analysis	Claude 3.5 Sonnet	Rule conflict detection, gap analysis
Embeddings	Titan Embed v2	Similarity search, entity resolution
Summarization	Claude 3 Haiku	Alert triage, report generation

3.4 Human-in-the-Loop Supervision

PACT AI operates under mandatory human supervision:

1. **Proposal Generation:** AI generates recommendations, never executes autonomously
2. **Confidence Thresholds:** Low-confidence outputs require human review
3. **Approval Workflow:** All AI-suggested actions require explicit human approval
4. **Override Capability:** Human operators can override any AI recommendation
5. **Audit Trail:** All human decisions recorded with attestation

3.5 Alignment with FINRA Rule 4511

FINRA Rule 4511 requires members to preserve records related to their business. AI-generated analysis constitutes business records. PACT ensures:

- **Preservation:** All AI inputs, outputs, and attestations preserved
- **Accessibility:** Records retrievable via standardized query interface
- **Integrity:** Cryptographic hashes prevent post-hoc modification
- **Attribution:** Model version, timestamp, and reviewer recorded

---

4. Permissioned Blockchain: Trust Governance and PoA Rotation

4.1 Why Blockchain for Compliance

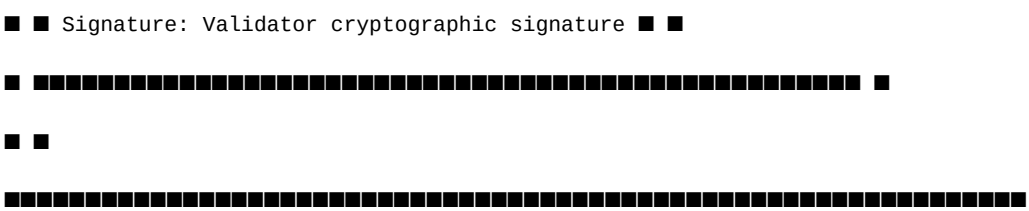
Traditional databases, even append-only logs, have inherent limitations:

- Database administrators can modify records
- Backup restoration can revert audit trails
- Single points of failure enable systemic compromise

Blockchain provides cryptographic guarantees that no single party—including system operators—can unilaterally modify historical records.

4.2 PACT Blockchain Architecture

PACT implements a permissioned Proof-of-Authority (PoA) blockchain:



4.3 Proof-of-Authority Consensus

Unlike public blockchains (Bitcoin, Ethereum), PACT uses Proof-of-Authority:

Characteristic	Public Blockchain	PACT PoA
Validators	Anonymous miners	Known, regulated entities
Consensus	Proof-of-Work/Stake	Round-robin with rotation
Finality	Probabilistic	Immediate
Throughput	~15-30 TPS	10,000+ TPS
Energy	High consumption	Minimal
Privacy	Public ledger	Permissioned access

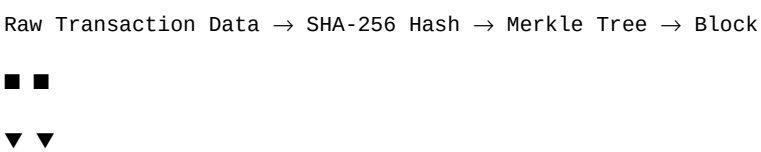
4.4 Validator Rotation Protocol

To prevent single-validator compromise, PACT implements rotation:

1. **Epoch Definition:** 24-hour rotation periods
2. **Validator Selection:** Deterministic round-robin among authorized nodes
3. **Signature Requirement:** Each block signed by designated validator
4. **Challenge Period:** 6-hour window for validator challenges
5. **Slashing Conditions:** Misbehaving validators removed from rotation

4.5 Data Privacy Architecture

PACT anchors hashes, not raw data:




```
Stored Off-Chain Stored On-Chain

(Encrypted, Access-Controlled) (Hash Only, Immutable)
```

This design ensures:

- **Regulatory Compliance:** Sensitive data remains in controlled environments
- **Audit Integrity:** Hash anchoring proves data existed at specific time
- **Privacy:** No PII or transaction details on shared ledger

4.6 Alignment with OCC Heightened Standards

OCC Heightened Standards (12 CFR Part 30, Appendix D) require:

Standard	PACT Implementation
Risk Governance	Deterministic rules with version control
Risk Appetite	Configurable thresholds with audit trail
Audit Function	Immutable blockchain attestation
Data Quality	Schema validation, canonical serialization
Model Risk	AI attestation with human oversight

5. Zero-Knowledge Audit Hashing: Future Upgrade Roadmap

5.1 Current Limitations

Present PACT architecture relies on SHA-256 hashing for audit anchoring. While cryptographically secure, this approach has limitations:

- Verifiers must access raw data to validate hashes
- Privacy-preserving verification requires trusted intermediaries
- Cross-institution verification requires data sharing

5.2 Zero-Knowledge Proof Integration

PACT's roadmap includes zero-knowledge proof (ZKP) integration:

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ZERO-KNOWLEDGE AUDIT VERIFICATION ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ Prover (Institution): ■
■ • Holds raw compliance data ■
■ • Generates ZK proof of compliance ■
■ • Publishes proof to blockchain ■
■ ■
■ Verifier (Regulator): ■
■ • Receives ZK proof ■
■ • Verifies compliance without accessing raw data ■
■ • Mathematical certainty of compliance ■
■ ■
■ Properties: ■
■ • Completeness: Valid proofs always verify ■
■ • Soundness: Invalid proofs always rejected ■
■ • Zero-Knowledge: No information leaked beyond validity ■
■ ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

5.3 Planned ZKP Capabilities

Capability	Timeline	Application
ZK-SNARK Anchoring	2025 Q2	Batch compliance proofs
Private Set Intersection	2025 Q4	Cross-institution verification
Recursive Proofs	2026 Q2	Aggregated regulatory reporting

6. Regulatory Alignment Summary

6.1 SEC Rule 17a-4 Compliance Matrix

Requirement	Section	PACT Implementation
Non-rewriteable storage	17a-4(f)(2)(i)	Blockchain immutability
Non-erasable format	17a-4(f)(2)(i)	Append-only ledger
Quality verification	17a-4(f)(2)(ii)(A)	Merkle tree validation
Serialization	17a-4(f)(2)(ii)(B)	Canonical JSON with hashing
Time-dating	17a-4(f)(2)(ii)(C)	Deterministic timestamps
Download capability	17a-4(f)(2)(ii)(D)	API-based export
Audit system	17a-4(f)(3)(v)	Blockchain explorer

6.2 FINRA Rule 4511 Compliance Matrix

Requirement	PACT Implementation
Make and preserve books and records	Automatic capture of all decisions
Readily accessible	Real-time query API
Prescribed format	Standardized JSON schema
Required retention periods	Configurable retention policies
Examination access	Regulator dashboard with full access

6.3 OCC Heightened Standards Compliance Matrix

Standard	PACT Implementation
Board-level risk governance	Configurable approval workflows
Independent risk management	Separation of rules engine and AI
Internal audit	Immutable audit trail
Talent management	Training and certification tracking
Compensation oversight	Not applicable (technical system)

7. Conclusion

The PACT Protocol provides a technical architecture that addresses fundamental limitations in current compliance systems. By combining deterministic rule execution, AI-attested analysis, and blockchain-anchored audit trails, PACT delivers:

1. **Certainty:** Mathematical guarantees of consistent rule application
2. **Accountability:** Complete provenance for every decision and AI output
3. **Immutability:** Cryptographic proof of record integrity
4. **Interoperability:** Standardized interfaces for regulatory examination

This architecture aligns with existing regulatory requirements while providing a foundation for future enhancements, including zero-knowledge proofs for privacy-preserving verification.

PACT represents a new paradigm in regulatory technology: compliance infrastructure that is verifiable by design, not merely by policy.

References

[1] Securities and Exchange Commission, "Electronic Storage of Broker-Dealer Records," 17 CFR 240.17a-4, 2003.

[2] Financial Industry Regulatory Authority, "Books and Records Requirements," FINRA Rule 4511, 2011.

[3] Office of the Comptroller of the Currency, "Guidelines Establishing Heightened Standards for Certain Large Insured National Banks," 12 CFR Part 30, Appendix D, 2014.

[4] National Institute of Standards and Technology, "Secure Hash Standard (SHS)," FIPS PUB 180-4, 2015.

[5] Amazon Web Services, "AWS Bedrock Security Whitepaper," 2024.

[6] Ben-Sasson, E., et al., "Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture," USENIX Security, 2014.

Appendix A: Technical Specifications

A.1 Cryptographic Primitives

Primitive	Algorithm	Key Size
Hashing	SHA-256	256-bit
Digital Signatures	Ed25519	256-bit
Encryption (at rest)	AES-256-GCM	256-bit
Encryption (in transit)	TLS 1.3	256-bit
Key Derivation	HKDF-SHA256	Variable

A.2 Performance Characteristics

Metric	Specification
Rule Evaluation	<10ms per event
AI Analysis	<5s per request
Block Time	1 second
Transaction Throughput	10,000 TPS
Storage Efficiency	~500 bytes per attestation

A.3 Availability Requirements

Tier	Uptime	Recovery Time
Production	99.99%	<15 minutes
Blockchain Network	99.999%	<1 minute
AI Services	99.9%	<1 hour

Document prepared for regulatory staff evaluation. Technical specifications subject to implementation updates. Contact ARKA Systems LLC for current documentation.

