BNB-Shield (web3 AML Solution)

Creators: Rob JB, Anthony Nixon (alch3mist), Eric McEvoy

This document outlines the design and architecture of a decentralized PEP detection system for real-time AML compliance. The system seamlessly integrates public blockchain auditability via OpBNB with secure, privacy-preserving off-chain data management and computation—leveraging advanced technologies such as Trusted Execution Environments (TEE), Zero-Knowledge proofs (ZK), and Fully Homomorphic Encryption (FHE). By combining an off-chain issuer process, a BNB-Greenfield data storage layer, and an encrypted agent substrate that supports collateral-based attestation ordering and automated dispute resolution, the solution is engineered to drastically reduce settlement times for high-confidence proofs while ensuring rigorous validation and accountability for lower-collateral submissions. This architecture not only fosters a trustless and transparent environment but also empowers network participants to collaboratively secure and maintain the integrity of AML processes.

Stage 1: Workflow (Data enrichment / PEP Challenge)

On Generality

Note: We chose to illustrate a Politically Exposed Persons check, but the solution horizontally abstracts to each requirement of full AML solutions. On prior or subsequent stages, agent strategies would submit a, <Stage> Challenge, via protocol.

1. **PEP Checks ← (example)**
2. Sanctions Screening
3. Watchlist Screening (Adverse Media & Criminal Records)
4. Transaction Monitoring & Behavioral Anomaly Detection
5. Geographical Risk Screening
6. Beneficial Ownership Screening (UBO)
7. Counter-Terrorist Financing (CTF) Screening
8. AML Risk Scoring & Customer Risk Rating
9. KYC & KYB Verification
10. Crypto-Specific AML Screening

Description

The protocol holds an Attestation Object [PEP: Politically Exposed Person(s)].

1. **Volume/Velocity/Variety -** Standard web2 AML tools will rely on whitelists, vendor data stores and heuristics, and often AI insights, however scalable agent swarms are able to tap into correlations and meta-data analysis to drive higher certainty.
2. **Financial Incentives and Guarantees** - Current AML tools tend to be only information aggregators and providers. The usefulness of the assertion or result has low effect on all parties but the final consumer (who in turn may provide a subscription model). Swarm enrichment creates strong collateral incentives for accuracy for every party involved in the analysis and process.
3. **Unification of Behavioral Analytics -** Solutions are primarily divided into two domains, off-chain (white/black-lists, media, investigative) and on-chain (TX analysis). Decentralized proposals from agents unify approaches where agent tooling may leverage data from all entities interactions : TX analysis, social media, oracles, white/black-lists, or sub-assertions, etc. maximizing coverage and creating a unified view.

Process

Overview

The system combines on-chain records, off-chain data uploads, and secure off-chain (or cross-chain) processing to validate PEP (Politically Exposed Person) records. It uses a staking/reward mechanism to encourage correct decisions while reducing false positives. In essence, data is enriched and checked by decentralized “swarm agents” operating in secure compute environments, and the outcome is confirmed either automatically or through manual review/dispute resolution.

Steps

1. **Record Creation & Data Upload**
   - **Minting on Public Chain:**
     A new PEP record (with a unique ID and pointer) is created on the public blockchain (OpBNB).
   - **Triggering Data Upload:**
     The off-chain issuer detects the new record and uploads a corresponding data payload to the BNB Greenfield Data Layer.
2. **Work Item Initiation**
   - **Polling & Event Trigger:**
     A polling service monitors the public chain for new PEP records.
   - **Work Item Publication:**
     The system fetches the record’s pointer via a confidential container, which then posts a work item to the secure compute layer (TEN).
3. **Secure Data Processing**

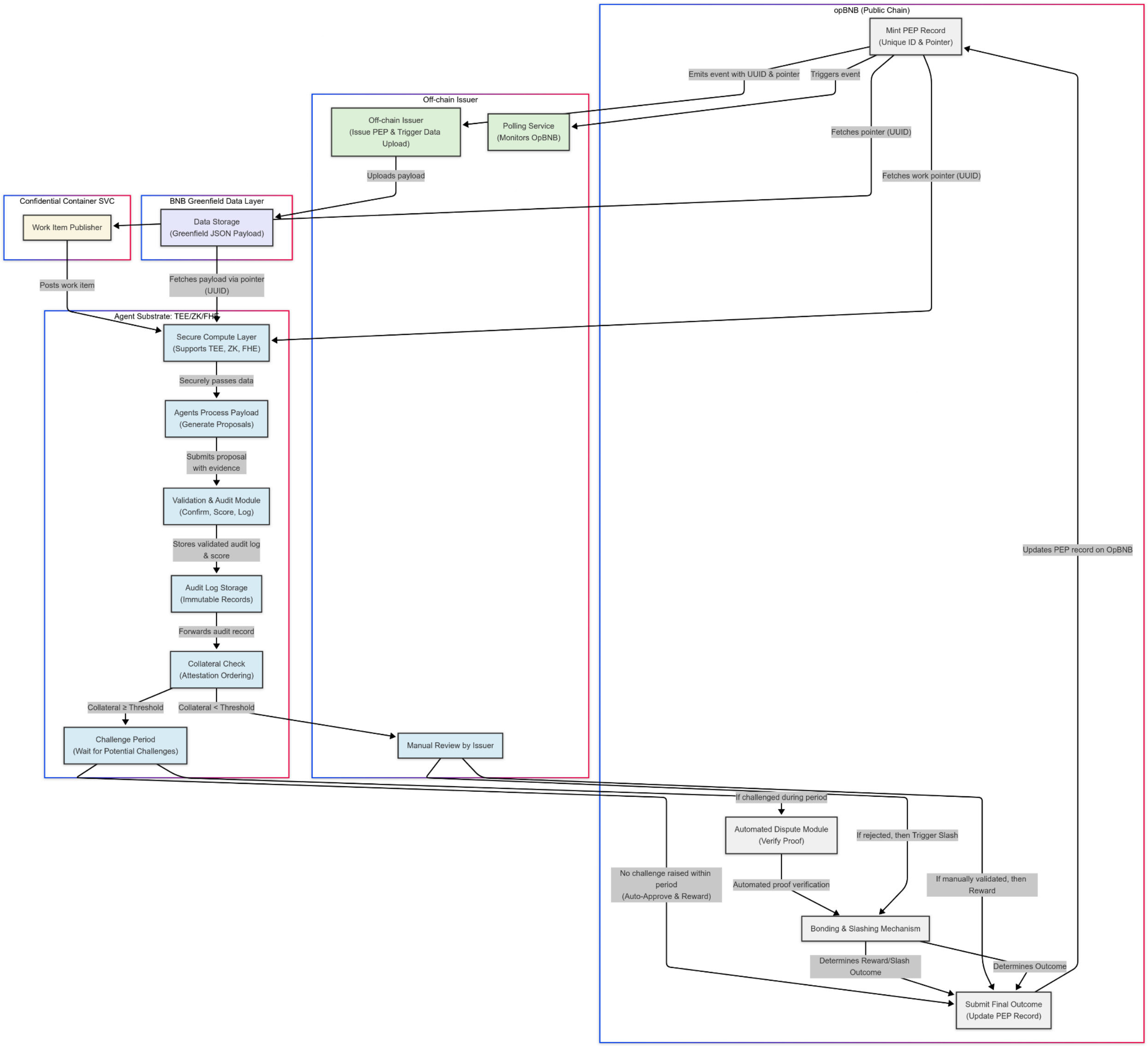
    - **Retrieving Data:**
      The secure compute layer retrieves the work pointer and corresponding payload from storage.
    - **Agent Processing:**
      Within a secure environment (using TEE, ZK, or FHE), swarm agents process the payload and generate proposals, including supporting evidence.
    - **Validation & Logging:**
      A validation module checks and scores the proposals, storing the results in an immutable audit log.
4. **Collateral Check & Decision Branching**
    - **Collateral Verification:**
      The audit log is sent to a collateral check module:
        - **High Collateral:**
          If the collateral meets a set threshold, the process enters a **Challenge Period**:
            - **No Challenge:** The proposal is auto-approved, and rewards are issued.
            - **Challenge Raised:** An automated dispute module verifies the evidence; the bonding/slashing mechanism then determines the reward or penalty.
        - **Low Collateral:**
          If collateral is insufficient, the issuer performs a **Manual Review**:
            - **Validated:** The proposal is approved, and rewards are issued.
            - **Rejected:** The bonding/slashing mechanism is triggered to impose penalties.
5. **Final Outcome Submission**
    - **Updating the Record:**
      The final outcome (whether through auto-approval, dispute resolution, or manual review) is submitted back to the public chain to update the original PEP record.

Diagram

Key Components

- **opBNB (Public Chain):**
    - *Mint PEP Record*: Creates the initial record.
    - *Submit Final Outcome*: Updates the record with the decision.
    - *Dispute Module & Bonding/Slashing*: Handle proof challenges and enforce economic incentives.
- **Off-chain Issuer:**
    - *Issue PEP & Trigger Data Upload*: Initiates data storage.

    - *Polling Service*: Monitors on-chain events.
    - *Manual Review*: Intervenes when collateral is low.
- **BNB Greenfield Data Layer:**
    - *Data Storage*: Holds the JSON payloads corresponding to PEP records.
- **Confidential Container:**
    - *Work Item Publisher*: Securely publishes work items for processing.
- **(Encrypted Compute Layer):**
    - *Secure Compute*: Retrieves and processes data securely.
    - *Agent Processing*: Swarm agents generate proposals with evidence.
    - *Validation & Audit*: Confirms the proposals, scores them, and logs the results.
    - *Collateral Check & Challenge Period*: Determines if the proposal is trusted enough for auto-approval or needs further dispute handling.



The workflow begins with minting a record on the public chain, followed by data upload and secure off-chain processing. Proposals are generated and validated by secure agents, with a collateral check determining the next step:

- **High collateral:** Enters a challenge period, possibly leading to automatic approval if unchallenged, or dispute resolution if challenged.
- **Low collateral:** Triggers manual review by the issuer.

In the end, the verified outcome is updated back on-chain, ensuring a trustless and economically incentivized process for reducing false positives and confirming high-confidence hits.

Stage 2: Collaborative Risk Sharing & Automated Reaffirmation

Counter-Parties

In a typical PEP event such as an insurance claim the following counter-parties are likely to run distinct duplicate checks and flag-remediations. These par:

Broker: As the initial intermediary responsible for gathering and preliminarily verifying information, the broker can use the agent-generated PEP assertion as a trusted source. This streamlines their due diligence and reduces the need for a separate internal PEP check.

Legal Entity / Underwriting Team: This group, which often performs a detailed risk and compliance review, can incorporate the agent-based result into their decision-making process. Relying on the trustless, collateral-backed assertion helps avoid duplicative efforts and maintains consistency across the review process.

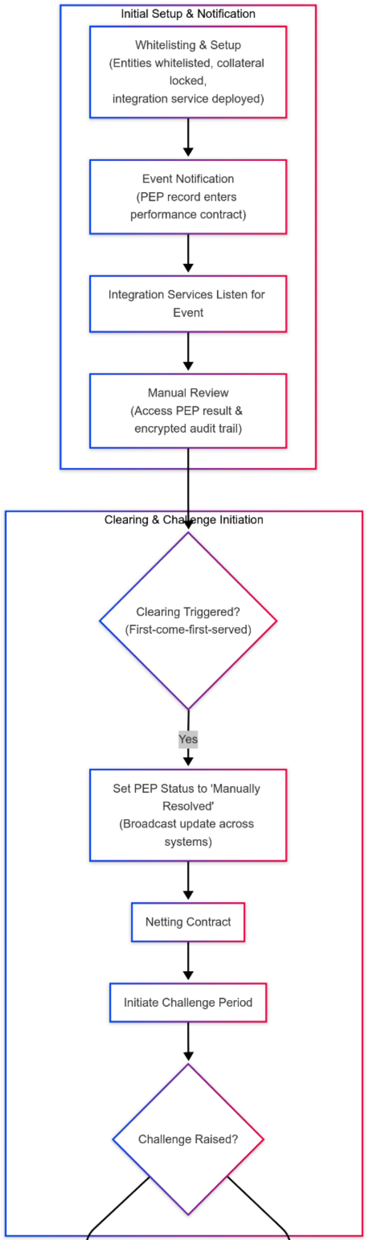
Insurance Company (Carrier): As the final risk bearer and decision maker, the insurance company can confidently use the validated PEP result for regulatory compliance and risk management purposes. This reliance ensures that the final underwriting decision is based on a robust, economically incentivized verification process.

Payment Processor (Conditional): While the payment disbursement entity is typically more focused on financial transaction compliance, if they are integrated into a broader AML/KYC workflow, they could also use the provided PEP assertion to satisfy their checks—**Conditional on the regulatory framework operating within**

Process

Steps

1. **Whitelisting & Setup:**
    a. Relevant entities (counterparties) are whitelisted via their public keys, granting access to specific PEP UUIDs' results and encrypted audit trails.
    b. Each counterparty locks collateral into a performance contract.
    c. Every counterparty deploys an integration service that links their sovereign EOA with their chosen AML SaaS/solution.
2. **Event Notification:**
    a. The integration service listens for blockchain events.
    b. When a PEP record is added to the performance contract (i.e., queued for review), an event is triggered for all whitelisted parties
3. **Manual Review:**
    a. Any whitelisted counterparty can, at any time, review the flagged PEP using their standard internal workflow.
    b. The review accesses both the PEP result and the encrypted audit trail for full context.
4. **Clearing & Status Update:**
    a. The first party to clear (resolve) the PEP triggers an update that marks the PEP record as "manually resolved."
    b. This change is propagated across all systems on a first-come-first-served basis.
    c. The clearing party is automatically credited for the resolution.
5. **Initiation of the Challenge Period:**
    a. Upon clearance, the PEP record enters a predefined challenge period.
    b. During this period, any counterparty may raise a dispute if discrepancies are found.
6. **Challenge Resolution & Remediation:**
    a. If a challenge is raised, an automated dispute resolution process examines the evidence in the audit trail.
    b. If the challenge is validated:
        - ■ The collateral of the clearing party is automatically slashed.
        - ■ Remediation fees are distributed to the challenging counterparties.


Initial Setup & Notification
Whitelisting & Setup (Entities whitelisted, collateral locked, integration service deployed)
Event Notification (PEP record enters performance contract)
Integration Services Listen for Event
Manual Review (Access PEP result & encrypted audit trail)
Clearing & Challenge Initiation
Clearing Triggered? (First-come-first-served)
Yes
Set PEP Status to 'Manually Resolved' (Broadcast update across systems)
Netting Contract
Initiate Challenge Period
Challenge Raised?

    c. If no challenge is raised within the challenge period, the clearance stands.

7. **Final Outcome:**
    a. The final, verified outcome is recorded on-chain and disseminated to all connected systems.
    b. This shared outcome removes the need for duplicate manual PEP checks within each counterparty’s internal processes.
8. **Continuous Monitoring:**
    a. Integration services continue to monitor for new PEP records and events, repeating the process as needed.

Economic Impact, Friction Reduction & Emergent Value

Overview:

Our decentralized AML enrichment and collaboration protocol revolutionizes the traditional compliance process by eliminating redundant manual checks and reducing false positives. The result is not only substantial direct cost savings but also a range of emergent benefits—such as improved capital efficiency, reduced risk, and enhanced agility—that drive long-term profitability and market differentiation.

Traditional AML Workflow: High Friction, High Cost & Hidden Inefficiencies

- **Multiple Checks & Redundant Processes:** Legacy systems involve up to four independent teams (brokers, legal/underwriting, insurance carriers, external vendors) performing duplicate manual reviews.
- Direct Costs:
    - Manual Review Assumptions:
        - **Time per review:** ~45 minutes
        - **Labor rate:** ~$80/hour
        - **Cost per review:** 0.75 hours × $80 = **$60**
    - **Aggregate Cost:**
      4 reviews × $60 = **$240 per event**
- Hidden Costs:
    - **Capital Locking Delays:** Lengthy AML checks can delay customer onboarding and transaction processing, tying up capital that could otherwise be deployed productively.
    - **Regulatory & Reputational Risk:** Higher false positives, missed flags and slower dispute resolutions increase the risk of regulatory fines, legal expenses, and reputational harm, which can indirectly erode profits.

Our Protocol: Streamlined, Secure, Scalable & Multi-Dimensionally Valuable

Unified, Automated Process: Leveraging smart contracts for automated minting and event triggering (with minimal gas fees) combined with secure off-chain computation and decentralized “swarm” agent validations, our protocol reduces the need for duplicate reviews.

Per-Event Cost Breakdown:

- **On-Chain & Integration Efficiency:** Automated minting and integration occur at low gas costs.
- **Secure Off-Chain/Cross-Chain Processing:** Efficient data enrichment via secure compute layers incurs minor fees.
- **Buffer for Occasional Manual Reviews:** While most events are automated, a small percentage require manual PEP confirmations or dispute resolution.
- **Conservative Average Cost Estimate: ~$50 per event**

Direct Savings:

- **Per-Event Savings:** Traditional cost of $240 minus $50 for our protocol = **$190 saved per event**
- **Additional Efficiency Gains:** Enhanced data accuracy and fewer false positives yield an extra **$20 saving per event**
- **Total Savings per Event:** Approximately **$210**

Emergent Value Drivers: Unlocking Higher-Dimensional Benefits

Improved Capital Efficiency:

- **Reduced Processing Delays:** Faster AML checks mean quicker customer onboarding and transaction clearance, liberating capital that might otherwise be locked up during lengthy reviews.
- **Accelerated Revenue Recognition:** Streamlined processes enable quicker service delivery, shortening the sales cycle and boosting cash flow.

Enhanced Risk Management:

- **Lower Regulatory Risk:** With fewer false positives and a unified, collateral-backed process, our protocol mitigates the risk of non-compliance, reducing potential fines, legal costs, and reputational damage.
- **Operational Resilience:** More reliable processes build stronger internal controls, further decreasing overall risk exposure.

Competitive Differentiation & Strategic Agility:

- **Customer Trust & Market Reputation:** A faster, more reliable AML process improves customer satisfaction and builds trust—critical in highly regulated sectors.
- **Agile Response to Regulatory Changes:** Our scalable, modular approach allows for rapid adjustments to evolving compliance requirements, preserving market competitiveness.

Scaling the Savings: A Clear Path to Profitability

Conservative Annual Projections:

- **At 2,000 Events/Year:**
  - 2,000 × $210 = **$420,000** in direct cost savings
- **At 5,000 Events/Year:**
  - 5,000 × $210 = **Over $1M** in annual savings
- **Compounded Emergent Benefits:** Beyond direct savings, reduced capital lock-up, lower risk, and enhanced operational agility contribute additional value that can improve margins and accelerate growth.

Conclusion

BNB Shield, the decentralized AML protocol redefines compliance by transforming it from a high-cost, fragmented process into a unified, automated, and scalable system. With an average cost of **~$50 per event**, we realize direct savings of around **$210 per event** compared to traditional methods—translating into annual savings from **$420,000 to over $1M** at varying scales. Moreover, by reducing capital locking delays, mitigating risk, and enhancing operational agility, our solution unlocks significant emergent value that further amplifies profitability and strategic positioning. We invite you to join us in revolutionizing AML compliance and capturing this multifaceted economic upside.