

Sovereign Game Theory and Confidential Restructuring: Implementing Shapley Cost Allocations and Blind M&A Debt-Equity Swaps on the Zama FHEVM

1. THE BECH-GARRATT DEFIANCE: CONFIDENTIAL SHAPLEY VALUE ENGINES

1.1. Strategic Context: Cooperative Game Theory in Clearing

The integration of cooperative game theory into confidential clearing cycles fundamentally alters market participant incentives, transitioning the landscape from defensive liquidity hoarding to proactive systemic solvency. By leveraging Fully Homomorphic Encryption (FHE), the protocol enables firms to resolve mutual debts within an environment of "Computational Blindness." This shift ensures that the pursuit of individual liquidity no longer chokes the network's total health, creating a self-healing grid where clearing is a collective optimization of capital rather than a zero-sum struggle for survival.

1.2. The Liquidity Hoarding Game

The Bech-Garratt strategic delay Nash equilibrium—where participants withhold payments to preserve their own liquidity—leads to systemic gridlock. The Zama fhEVM resolves this by enforcing state isolation through 32-byte encrypted ciphertext handles (uint64). Confidentiality is the prerequisite for cooperative stability; because no participant can probe the liquidity positions of others, predatory delay is neutralized. Secure client-side enforcement is achieved via the W3C Web Cryptography API, utilizing non-extractable keys (extractable=false) within the browser's volatile memory. This hardware-level isolation, combined with polynomial rings of dimension $N=32,768$, ensures that private signing material never leaves the user's firewall, shifting the dominant strategy toward early submission.

1.3. Shapley Value Cost Allocation (ϕ_i)

The Ecompensa Compensation Agent calculates the marginal contribution (ϕ_i) of firms within the cleared debt pool. To prevent double-financing fraud, the system utilizes SHA-256 hashes of ATCUD invoice codes as ZK-Nullifiers. The "take-it-or-leave-it" liquidity offer workflow follows a rigorous sequence:

- **Inversion Phase** : Local SAF-T PT XML faturamento data is ingested and converted into homomorphic ciphertexts at the edge.
- **Marginal Contribution Analysis** : The agent computes the delta in system netting efficiency created by adding firm i to every possible coalition.
- **ZK-Nullifier Verification** : SHA-256 ATCUD hashes are checked against the ledger to ensure invoice uniqueness without revealing underlying commercial data.
- **Final Settlement** : Participants receive an optimized net position (ϕ_i); acceptance leads to atomic financial extinction, while rejection returns the firm to its original, un-netted debt state.

1.4. The Vital Links Commission Engine

To incentivize volume, the Vital Links engine utilizes the ERC-7984 standard to award transaction fee rebates. This model bypasses the $O(N^2)$ computational wall by shifting

heavy math to off-chain coprocessors while maintaining on-chain integrity. | Computational Complexity | Shapley Discount Stamp | Rebate Incentive (ERC-7984) || ----- | ----- | ----- || Low (Linear Netting) | Tier 1: Bronze | 5% Transaction Fee Credit || Medium (Multi-node Cycle) | Tier 2: Silver | 12% Transaction Fee Credit || High (Cross-Sectoral Path) | Tier 3: Gold | 25% Transaction Fee Credit || Critical (Systemic Bridge) | Tier 4: Sovereign | 40% Transaction Fee Credit |

1.5. Section Conclusion

The mathematical optimization of liquidity through Shapley engines provides the financial bedrock for the structural re-engineering of distressed corporate balance sheets.

2. CORPORATE ENGINEERING ON-CHAIN: THE CONFIDENTIAL M&A SWAP

2.1. Strategic Context: On-Chain Restructuring

On-chain restructuring is a tool for systemic resilience, moving beyond simple transfers to complex equity-debt transformations. By executing these swaps within Trusted Execution Environments (TEEs), specifically AWS Nitro Enclaves, the system rehabilitates strategically important nodes without triggering credit contagion or market-wide panic.

2.2. Homomorphic Valuation via Leontief Matrices

The Fusion Agent (Agent 10) utilizes a 100-sector Leontief input-output matrix to intercept default spirals. Optimal Dilution and Equity Swap Ratios (R_{swap}) are computed homomorphically, identifying interdependencies without leaking balance-sheet data. Performance is monitored via a D3.js Cartesian Visualizer on a normalized cube scale of -100, 100, where the X-axis represents Target Valuation (EUR), the Y-axis represents the Swap Ratio (%), and the Z-axis specifically tracks Residual Debt (EUR).

2.3. Restructuring Mechanics: Comparison Table

Feature	Traditional Public Equity Swap	Ecompensa Confidential Swap
Data Privacy	Full exposure of valuation/debt	Total state isolation (bytes32 handles)
Execution Certainty	Subject to front-running/reorgs	Atomic settlement via FHE.select
Valuation Model	Speculative/Publicly debated	Algorithmic 100-sector Leontief
Signaling Risk	High; signals financial distress	"Zero; occurs inside the ""Blind"" enclave"

2.4. SPV Joint Venture Capitalization

The 3-Year SPV capitalization schedule transitions liabilities into productive capital. This model reconciles partner incentives through a structured equity vehicle:

- **Equity Allocation** : 55% of the entity is retained by the parent; 45% is issued as Class B shares.
- **Value-Share Commission** : The 45% Class B shares act as the primary vehicle for the 40% partner value-share commission.
- **Fee Reversion** : A 20% reversion of the 0.05% operational fee is directed to ERP integrators.
- **Debt Extinction** : Direct conversion of B2B liabilities into equity, lowering the Weighted Average Cost of Capital (WACC) and expanding EBITDA multiples.

2.5. Section Conclusion

The financial logic of M&A swaps is secured by hardened code patterns, ensuring that the transition from debt to equity is immutable and confidential.

3. HARDENED SOLIDITY PATTERNS: FheClearingMerger.sol & ClearingHouse.sol

3.1. Strategic Context: FHEVM Specific Paradigms

Developers must abandon standard Solidity branching logic to prevent timing side-channel leaks. The @fhevm/solidity v0.11.x migration is mandatory, shifting all operations to the FHE namespace to maintain compatibility with the Zama coprocessor architecture.

3.2. Cryptographic Invariants and Developer Checklist

To maintain integrity in FheClearingMerger.sol, the following hardening measures are required:

- **Multiplexer Logic** : Use FHE.select exclusively for conditional state updates to ensure gas-cost consistency regardless of encrypted values.
- **Overflow Protection** : Implement FHESafeMath to prevent silent wrap-around risks. Developers must explicitly guard against **CVE-2026-73645** , where the silent failure of the _mint operation in ERC7984ERC20Wrapper.sol during total supply overflow can lead to unrecoverable loss of user funds.
- **Noise Management** : Monitor multiplicative depth; results approaching 2^{80} must trigger the matchZamaError utility to prevent decryption failure.
- **Authorization Verification** : Verify permissions using FHE.isSenderAllowed at every point of handle consumption.

3.3. Atomic Settlement and CCN-ERR-901

The clearing process utilizes a "Silent Failure" loop. If a node has insufficient ERC-7984 credits for a netting round, the entire operation rolls back in-memory. This prevents leaking the identity of the defaulting node on-chain. The system emits error code CCN-ERR-901, signaling a settlement failure while preserving the commercial secrecy of the participants.

3.4. Account Abstraction and Transient Storage

In Account Abstraction (AA) contexts, multiple user operations bundled into a single transaction create a data-leakage channel if transient permissions persist. **Requirement for Deployment** : AA wallets must detect FHEVM contracts by querying confidentialProtocolId(). Upon detection, the wallet must automate the execution of FHE.cleanTransientStorage() immediately following each FHE-sensitive operation to ensure state isolation between bundled operations.

3.5. Section Conclusion

Technical implementation is anchored in the legal finality provided by the Portuguese jurisdiction, mapping code to statute.

4. REGULATORY ALIGNMENT & THE POST-FIAT TRANSITION

4.1. Strategic Context: Legislative Irrevocability

Aligning cryptographic systems with national law is essential to transform digital "set-off orders" into legal "financial extinction." This alignment ensures that on-chain settlement is irrevocable and recognized by central authorities.

4.2. Portuguese Legislative Framework

The FluidCluster stack operates under **Decree-Law no. 150/2019 (Article 12)** and **Portuguese Ley 69/2019**. These statutes support the finality of set-off orders executed within the **ZLT#13 Sandbox**. By mapping homomorphic netting results to these legal standards, the system ensures that once a debt is extinguished on-chain, it is legally void across the jurisdiction.

4.3. The Era Pós-Moeda (E-Barter)

The transition to a sovereign liquidity grid is realized through the transformation of B2B liabilities into ERC-7984 credits. This "E-Barter" system, powered by the "Modelo 5" netting solver, achieves a **72% gross extinction rate** and an **85% reduction in energy consumption** by utilizing photonic hardware. This bypasses traditional central bank credit lines, enabling a direct, sovereign exchange of value.

4.4. SRE Monitoring and Automated Slashing

SRE guidelines for the 9-of-13 threshold KMS partitions mandate rigorous performance monitoring:

- **LATENCY_SLA_VIOLATION** : A strict **\$\le 10.0\$ ms** local latency SLA is required for high-performance sovereign grid operations (80ms is the legacy outer-bound threshold).
- **FHE_NOISE_CRITICAL** : Ciphertext depth reaching **$L \geq 8$** triggers an automated noise-reset using the matchZamaError handler.
- **Automated Slashing** : Persistent performance degradation or bad-acting triggers a **50% collateral penalty** to maintain the health of the self-healing grid.

4.5. Final Concluding Statement

FluidCluster 3.0 represents the ultimate convergence of cryptographic "Blindness" and agentic intelligence, creating an autonomic, self-healing liquidity grid that returns sovereign financial control to the enterprise.