Mitigating Wash Trading in Incentive-Oriented Semiconductor Blockchain Frameworks

Aritri Saha*, Ujjwal Guin*, and Vivek Menon†
*Dept. of Electrical and Computer Engineering, Auburn University
†National Reconnaissance Office
Emails: {aritri.saha, ujjwal.guin}@auburn.edu, and vivekv@vt.edu

***Abstract*—As globalization deepens in the semiconductor supply chain, organizations increasingly rely on untrusted third parties for sourcing chiplets and integrated circuits. To secure these complex networks, incentive-based blockchain frameworks have been proposed to align the behavior of each participant through the use of rewards and punishments. However, such systems are vulnerable to collusive behaviors, such as wash trading, where malicious entities repeatedly transact among themselves to inflate sales activity and trust metrics without adding real value. This work systematically analyzes the impact of wash trading in a simulated semiconductor supply chain secured by an incentive mechanism that employs an additive increase, multiplicative decrease (AIMD) strategy to reward or penalize participants based on transaction outcomes. We first identify the conditions under which such an attack emerges and the exploitative gains that attackers earn. We then introduce an anomaly-based detection scheme that flags suspicious transaction paths indicative of wash trading and propose corresponding prevention strategies. We discuss a dynamic reputation reduction mechanism that penalizes wash traders more than the rewards they unfairly accrue, ensuring that they gain no net benefit from wash trading. By combining detection and penalty mechanisms, our approach effectively discourages wash trading and can support fairness and trust in blockchain-based semiconductor supply chains.**

***Index Terms*—Blockchain, wash trading, reputation, trust, 3D IC, heterogeneous integration, chiplets, and semiconductor supply chain.**

I. Introduction

The modern semiconductor supply chain is often plagued by deceptive practices and market manipulation tactics. Wash trading, a collusive practice, is one such attack in which a group of malicious entities repeatedly conducts transactions among themselves to artificially inflate transaction volume, with the intent of manipulating the system to achieve exploitative gains. In recommendation-based systems, this manifests as fraudulent reviews from colluding malicious traders or customers, thereby promoting or asserting higher ratings to products of lesser quality. In traditional financial systems, this practice can result in artificially inflated asset prices, a misleading perception of increased demand or interest, and distorted trading volumes. For instance, in 2021, the U.S. Securities and Exchange Commission (SEC) charged two individuals with executing a meme-stock wash trading scheme that netted over half a million dollars in illicit profits [1]. Similarly, in NFT markets, wash trading is often used to fabricate demand and inflate token prices, creating a pretense of higher value that does not reflect genuine buyer interest [2].

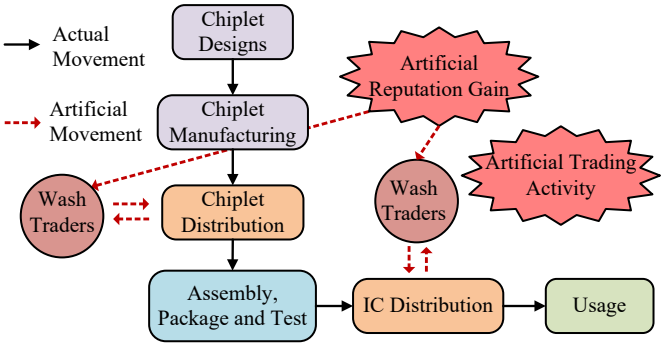

Fig. 1. Wash trading exploitation in incentivized blockchain infrastructure.

While these incidents have been widely studied in financial and digital asset markets, similar forms of manipulation can emerge in other high-stakes domains where reputation or incentives drive decision-making. One such domain is the semiconductor supply chain, which forms the backbone of modern computing and communication infrastructure. The onset of heterogeneous integration (HI), coupled with increasing globalization and the rise of fabless models, has significantly increased the complexity of semiconductor manufacturing and distribution. As a result, the supply chain is now more vulnerable to disruptions, such as the global chip shortage [3], and security threats, including the insertion of hardware Trojans [4], [5], the introduction of counterfeit and recycled ICs [6], [7], and intellectual property piracy [8], [9]. To mitigate these risks, researchers have proposed incorporating all supply chain participants into unified digital infrastructures, including permissioned blockchain frameworks [10]–[13], which ensure the immutability and transparency of provenance records. Although these frameworks offer the promise of secure and verifiable data sharing, their real-world adoption remains limited. Many organizations may perceive that the cost of implementing a blockchain framework outweighs its potential benefits. To address this challenge and incentivize participation, Valapu et al. [14] proposed a reputation-based reward and penalty mechanism. In this framework, the performance of supply chain members is continuously assessed based on their transaction behavior. Members who maintain high reputation scores can gain tangible benefits, such as access to more

efficient sales processes and increased trust within the network. Despite the growing interest in blockchain-based supply chain frameworks, the risk of adversarial behaviors such as wash trading within these environments remains largely unexplored. Figure 1 presents a simplified semiconductor supply chain model, highlighting how wash traders can infiltrate the chiplet lifecycle by colluding with malicious chiplet distributors. A similar infiltration pattern may also occur within the IC lifecycle. This is particularly detrimental as in decentralized supply chain systems, reputation acts as a proxy for trust, influencing trading decisions. Therefore, maintaining the integrity of reputation scores is essential to ensure system-wide fairness and reliability. The lack of robust detection and prevention mechanisms against wash trading poses a significant threat to the credibility of the trust score.

The paper investigates how wash trading among semiconductor supply chain participants can manipulate tangible indicators of trust, i.e., reputation scores, in a blockchain-based network. We introduce several attack simulations that model wash trading behavior, where entities repeatedly transact among themselves to inflate their reputation without participating in the supply chain transactions.

We demonstrate that, within a traditional reward-and-punishment framework, such behavior yields disproportionate gains in reputation and transaction value, enabling malicious entities to exploit the incentive mechanism. To address this threat, we propose both preventive and reactive mechanisms. First, we define smart contract-level restrictions that limit repeated transactions between the same entities, aiming to suppress direct forms of wash trading at the protocol level. However, recognizing that some sophisticated actors may bypass these restrictions through indirect loops or bridge nodes, we develop a detection framework that monitors transaction history for suspicious behavioral markers. Upon detection, our system invokes a reputation slashing mechanism that irreversibly "burns" the inflated reputation scores of identified wash traders, significantly reducing their standing in the network.

Contributions.

- *Modeling Wash Trading in the Semiconductor Supply Chain:* We demonstrate how wash trading, typically existing in NFT, financial, or digital marketplaces, can infiltrate the reward and punishment scheme for the semiconductor supply chain. We demonstrate how reputation systems, when tied to transaction volume or peer interactions, can be manipulated by repeated transactions among wash traders, resulting in inflated reputation scores and distorted incentives.
- *Techniques for Identifying Wash Trading:* To proactively mitigate wash trading, we introduce smart contract-level constraints aimed at limiting wash trading behavior. Recognizing that such restrictions may be bypassed, we further propose a set of detection heuristics tailored to capture more covert wash trading patterns.
- *Mitigating the Effects of Wash Trading:* Finally, we present a penalty mechanism that irreversibly "burns" reputation scores of identified wash traders, demonstrating how regaining trust becomes significantly harder once the wash trading attack is detected.

The rest of the paper is organized as follows. Section II reviews related work on wash trading and introduces the reward and punishment-based blockchain framework that serves as the foundation of this paper. In Section III, we present different types of wash trading attacks applicable to the reputation scheme mentioned earlier. In Section IV, we describe our proposed wash trading detection methodology for detecting and mitigating these malicious behaviors. In Section V, we present the simulation results and discuss the evaluation methods. Finally, in Section VI we conclude the paper.

II. Prior Work

Blockchain-based incentive schemes have been widely explored across diverse domains, including healthcare [15], [16] and vehicular ad hoc networks [17], [18]. More common blockchain platforms where sales volume and reputation scores are central include decentralized cryptocurrency exchanges [19] and NFT marketplaces [20]. Imisiker et al. identify wash trades in stock markets as instances where the buyer and seller are the same entity [21]. Victor et al. [19] detect wash trading in decentralized exchanges through groups of different actors who trade among themselves while maintaining constant net market positions or token exchanges. Although wash trading has been extensively analyzed in decentralized financial markets and NFT platforms, these markets operate under fundamentally different dynamics compared to the semiconductor supply chain.

The complex, globalized nature of semiconductor supply chains underscores the need for a uniform and transparent method to evaluate the performance of participants. Incentive mechanisms remain largely unexplored in the context of the semiconductor supply chain and blockchain initiatives. Therefore, to evaluate the impact of wash trading in a semiconductor supply chain, we adopt the reward and punishment framework proposed by Valapu et al., which incentivizes participation in blockchain-based supply chains through a reputation-based mechanism [14]. To the best of our knowledge, this is the only blockchain framework that utilizes an incentive-oriented mechanism specifically catered towards the semiconductor supply chain. Therefore, our evaluation of reputation, presented in [14], is based on two key factors:

- *Stake-weighted reputation accumulation:* The framework in [14] employs an additive increase strategy to conservatively reward entities for successful participation in the supply chain. Each transaction is interpreted as an implicit endorsement, whereby a sale from entity A to entity B for d dollars signifies B's trust in A, and results in A gaining reputation proportionate to the sale amount, provided that no defect is detected in the downstream lifecycle. To make our scheme more robust against wash trading, we propose normalizing the reward over the total number of entities present across the full

part (i.e., chiplet or IC) provenance path before it is assimilated into the system.

• *Trust-calibrated reputation penalization:* When a defect is identified in a part, all entities within its traceability path are penalized using a multiplicative decrease strategy [14]. The penalty is determined by a base penalty factor m and a discount factor d. The discount factor d is selectively applied to entities belonging to consortiums deemed trusted by end users *EU*. Furthermore, within trusted consortiums, the penalty discount factor is higher for entities closer to the *EU* and therefore incur a lesser penalty reduction than entities closer to the untrusted consortiums.

While the framework effectively penalizes entities that introduce defective parts, it does not explicitly address scenarios where participants can gain an unfair advantage by repeatedly transacting among themselves without participating in the supply chain transactions. Thus, wash trading can artificially inflate reputation scores and distort incentives. Therefore, *EUs* may be misled into believing that certain organizations are trustworthy, and these entities could then unfairly dominate the market and reap undue advantages based on perceived over actual reliability. The authors of [14] also acknowledged this vulnerability, but do not propose concrete mechanisms to detect or mitigate such manipulations.

III. Proposed Wash Trading Attack

Wash trading in reputation-based semiconductor supply chains is primarily motivated by the desire to artificially inflate reputation scores through non-legitimate transactions, thereby gaining trust. Since the reward-and-punishment mechanism used in this framework is dependent on the final testing issued by *EUs* and trusted authorities, any reputation gains do not materialize immediately when wash trading occurs.

A. Threat Model

Wash traders within the supply chain can exhibit several behavioral characteristics. Opportunistic wash traders are entities that initially engage in legitimate transactions to establish trust within the blockchain ecosystem. Over time, however, they exploit this trust by manipulating the system through artificial asset transfers, often leveraging their previously established reputation for deceptive purposes. In contrast, foundational wash traders are entities that engage in fraudulent behavior from the outset. These traders consistently manipulate the system with no intention of conducting legitimate transactions, and their activities are inherently designed to deceive for personal gain from the very beginning.

This paper adopts the same trust model presented in [14]. The manufacturers (i.e., chiplet and IC) and system integrators are trusted entities, whereas the distribution layer, comprising chiplet and IC distributors, may include both trusted and untrusted actors. Our threat model is centered on:

- One or more colluding distributors engaging in coordinated wash trading behavior.
- An incentive-based trust metric primarily relying on transactional volume.

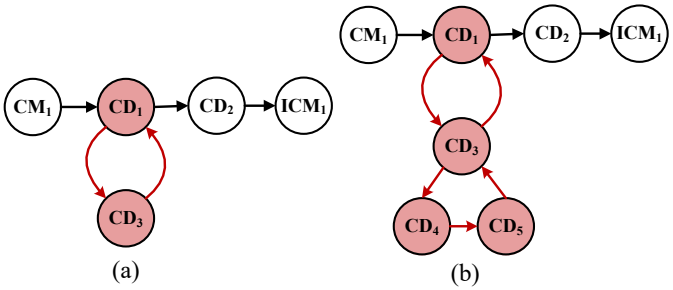

Fig. 2. Supply chain entities engaging in wash trading. Fig.(a) shows a simple cyclic behavior between two wash trading members. Fig.(b) shows members forming cycles with more complex loops.

Our model assumes that the physical movement of chiplets without a valid operational reason is inherently costly. Therefore, it is reasonable to expect that many wash traders will avoid real transfers and instead rely on falsified ledger entries to simulate transactions.

B. Wash Trading Driven by Cyclic Transactions

Cyclic transactions occur when entities repeatedly engage in back-and-forth trades within a closed loop. These can range from simple bilateral exchanges between two wash traders, as illustrated in Figure 2(a), to more complex cycles involving larger groups of entities, as shown in Figure 2(b). In such cases, a part circulates through a series of transactions and is eventually repurchased by the originating entity, creating the illusion of legitimate trade activity. These cycles may occur multiple times or be executed intermittently to evade detection.

While occasional repurchasing of parts may be legitimate, persistent cyclic transactions, particularly those involving colluding parties, can indicate wash trading. In Figure 2, the original trace of a chiplet is indicated by the black arrows. However, cyclic behavior can emerge when a single wash trader is present in the system. For instance, the manufacturer, CM_1, may sell to an initial distributor, CD_1, who then transfers the part through wash trading intermediaries before eventually repurchasing it, creating a loop. This is difficult to detect using conventional chiplet/IC tracking, as from an organization level, CM_1 is still selling the part to CD_1 and CD_2 is purchasing from CD_1 despite the additional rerouting. If defects are not found, these wash traders accumulate reputation unfairly, as the framework interprets each transaction as a valid endorsement. As a result, the intermediate wash trading entities gain disproportionate reputation without any meaningful contributions to the network.

One way to mitigate cyclic wash trading is to restrict a chiplet or IC from being owned by the same entity more than a certain times within its lifecycle. Such constraints can be enforced on-chain via smart contracts, limiting cases where parts circulate back to previous owners.

C. Wash Trading Driven by Cluster-based Transactions

Cluster-based transactions refer to a collusive strategy in which a group of entities forms a transactional network without forming a closed loop while collectively manipulating the sales path of chiplets or ICs among them. In this mechanism,

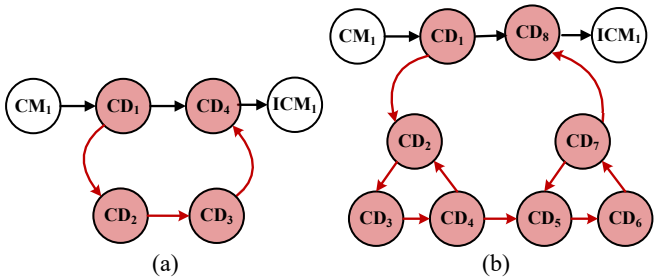

Fig. 3. Supply chain entities engaging in wash trading. Fig.(a) shows a simple cluster wash trading. Fig.(b) shows members forming a hybrid wash trading, including cyclic and cluster ones.

at least two members of the wash trading cluster appear in the chiplet or IC's normal sales path adjacent to each other, as a buyer and a seller. Rather than engaging in direct transactions, these entities reroute the part through other members of the cluster before delivering it to the intended non-malicious buyer down the supply chain. For example, in Figure 3(a), entities CD_{1-4} form a wash trading cluster. The traditional path for the chiplet is shown by the black arrows. However, because both CD_1 and CD_4 are members of the same cluster, they can artificially route the part through the other wash trading intermediaries before finally transferring to ICM_1. The same logic applies when any two of the other wash trading entities appear in a traditional chiplet lifecycle. This scheme avoids repeated ownership to avoid standard detection mechanisms.

While the two methods discussed in this paper represent distinct strategies that may be employed by malicious actors, we acknowledge the existence of hybrid approaches, as shown in Figure 3(b). Attackers may exhibit characteristics of both these attacks within a single wash trading pattern, which could be more prevalent in real-world scenarios.

IV. Proposed Wash Trading Identification and Mitigation Approaches

If left undetected, wash trading can significantly undermine the long-term sustainability and fairness of the incentive structure, ultimately discouraging honest participation in the supply chain ecosystem. Cluster-based transactions, in particular, are inherently resistant to conventional wash trading detection techniques due to their one-time, coordinated nature and lack of obvious cyclic patterns. In this section, we present our approach for enabling *EUs* to independently verify the presence of wash trading by accessing traceability data recorded on the blockchain. While our analysis primarily focuses on the chiplet lifecycle, the same framework can be readily extended to ICs.

A. Cycle Detection

The previously established semiconductor supply chain model is represented as a Directed Acyclic Graph (DAG) [14], which naturally enforces a unidirectional flow of chiplets and ICs, thereby preventing cycles. However, during a wash trading attack, one or more malicious entities may collude to fabricate artificial transactions that introduce cyclic paths into this otherwise acyclic graph. These cycles violate the expected flow of components and serve as indicators of potential fraudulent behavior. To combat this, we propose a mechanism that enables downstream entities in the lifecycle, such as IC manufacturers and system integrators, to efficiently detect the presence of such cycles by inspecting the trace paths of the chiplets or ICs they receive. This trace inspection can be initiated via a function call in the smart contract, which, upon detecting a cycle, returns a list of suspected wash traders involved in the cyclic trading pattern. Furthermore, we assume the existence of trusted authorities who can access and analyze these reports over time. By aggregating the frequency with which specific entities are flagged in cyclic patterns, these authorities can monitor and potentially penalize organizations repeatedly implicated in wash trading activities.

Algorithm 1: DFS-Based Canonical Cycle Detection with Threshold

Input : chiplet ID, threshold τ
Output: Suspect Wash Traders

function `DetectCyclesDFS`$(chipletID, \tau)$**:**
  $trace \leftarrow$ `GetAssociatedTrace`$(chipletID)$;
  $G \leftarrow$ `BuildChipletTraceGraph`$(trace)$;
  $visited, recStack, path \leftarrow \emptyset, \emptyset, []$;
  $cycleCounter \leftarrow$ empty map;
  function `DFS`$(node)$**:**
    Add $node$ to $visited$ and $recStack$;
    Append $node$ to $path$;
    foreach $neighbor \in G[node]$ **do**
      if $neighbor \notin visited$ **:**
        `DFS`$(neighbor)$;
      elif $neighbor \in recStack$ **:**
        $i \leftarrow$ index of $neighbor$ in $path$;
        $cycle \leftarrow path[i:] + [neighbor]$;
        $canonKey \leftarrow$ `MatchOrRegisterCycle`$(cycle)$;
        $cycleCounter[canonKey] + +$;
    end
    Remove $node$ from $recStack$ and $path$;
  end
  foreach $node \in G$ **do**
    if $node \notin visited$ **:**
      `DFS`$(node)$;
  end
  return $\{ c \mid cycleCounter[c] > \tau \}$;
end

Algorithm 1 implements a depth-first search (DFS)-based approach to detect repeated cycles in chiplet transaction traces that exceed a specified threshold τ. Here, τ represents the maximum number of permissible re-ownership of the same device by an identical group of entities and is defined based on acceptable operational and supply-chain policies. Cycles exceeding this threshold are flagged as anomalous, as they may indicate collusive or wash-trading behavior. The algorithm begins by retrieving the trace associated with a given chiplet ID and

constructs a directed graph representing the sequence of hand-offs between organizations. It then initializes four key data structures: `visited` to track explored nodes, `recStack` to maintain the current recursion path for cycle detection, `path` to reconstruct potential cycles, and `cycleCounter` to store the frequency of each detected cycle in its canonical form, lines 4-5. During DFS traversal, each unvisited neighbor is recursively explored; if a node is encountered that already exists in `recStack`, a cycle is detected, lines 6-17. The cycle is then extracted from the `path` (Lines 12-14) and passed to `MatchOrRegisterCycle` (Lines 15-16), which canonicalizes it by rotating the sequence to a standard specified form, ensuring that cycles like A→B→C→A and B→C→A→B are treated as identical loops before incrementing its frequency count. This is because, as we aim to catch wash trading loops, if loops are formed by the same members, we can treat them as part of the same cycle. After exploring all neighbors, the current node is removed from both `path` and `recStack` to enable accurate backtracking at line 18. This process is repeated for all nodes in the graph. Finally, suspect wash traders (i.e., organizations with cycles exceeding the threshold τ) are returned, in line 24.

B. Cluster Identification

Traditional cycle-based detection schemes are effective only when chiplets are circulated repeatedly among the same group of organizations, therefore forming one or more detectable loops. However, such approaches may not capture manipulative behaviors that do not involve loops. Adversaries can participate in cluster-based wash trading to circumvent traditional cycle detection algorithms while still achieving the underlying goal of reputation inflation through artificial interactions. This poses a significant challenge, as they may resemble legitimate transaction flows within the supply chain.

To overcome this limitation, it is imperative to incorporate auxiliary behavioral signals that may indicate artificial activity. Notable examples include pricing anomalies, where identical chiplets are acquired at inconsistent price points despite the availability of more economical suppliers, and unrealistically short transfer intervals that defy normal logistical constraints. When these signals are analyzed alongside traditional cycle-based methods, they offer a more robust and comprehensive framework for identifying wash trading behavior within blockchain-enabled semiconductor supply chains.

1) Anomalous Pricing Detection: As the reward scheme is tied to sale prices, it is reasonable to assume that wash traders will likely employ manipulation tactics to maximize profits and minimize detection. We assume that CMs and $ICMs$ are non-malicious actors and therefore, transactions involving these endpoints can be treated as reliable reference points for expected pricing behavior. There can be other intermediate trusted members whose transactions can be chosen to determine the markup. Markup refers to the difference between the selling price relative to the cost of purchase. For each chiplet lifecycle, the expected markup M_E can be computed by averaging the markups of some trusted buyers and sellers:

$$M_E = \frac{1}{N}\sum_{k=1}^{N} m_k, \quad m_k = \frac{P_{S,k} - P_{B,k}}{P_{B,k}},$$

where N denotes the number of trusted hops, typically the first and last few transactions involving CMs, trusted CDs, and the ICM; $P_{S,k}$ denotes the selling price and $P_{B,k}$ denotes the buying price in the k_{th} trade.

Each intermediate transaction within the chiplet's path is compared against M_E. Any transaction with a markup deviation exceeding a governance-defined threshold Δ is flagged:

$$|m_i - M_E| > \Delta.$$

This additionally flags "pump-and-dump" patterns, where entities inflate the price through a sequence of high-markup transactions before selling the chiplet at a lower-than-expected price, masking opportunistic trust gains.

2) Geo-Temporal Feasibility Score: Organizations engaging in wash trading can conduct illicit transactions virtually on the blockchain without physically transferring the chiplets from one entity to another. This allows wash traders to fabricate transactional activity and inflate their reputation while avoiding the logistical costs, time delays, and risks associated with physically shipping devices. Since the actual transfer of devices may not be economically viable or justified by the marginal profit gained through such manipulation, these virtual on-chain transactions present a low-cost, high-impact strategy for exploiting incentive mechanisms for the wash traders.

To detect such activities, we focus on the time intervals between chiplet transfer initiation and confirmation as a potential indicator for identifying wash trading. A short time interval may signal transactions that exist only on-chain without corresponding physical movement. These anomalies, when compared with typical shipping or operational delays, can help identify suspicious, non-genuine transfers within the supply chain. We assume that each *EU* or trusted verifying authority has access to a function $f_T(L_s, L_r)$, which estimates the minimum physically plausible time required to transport a chiplet between two geographic locations L_s (sender) and L_r (receiver). This estimate may be derived from distance-based heuristics depending on available shipping information.
For any transaction, Tx, we define:

- t_I: The timestamp when the chiplet transfer was initiated by the sender.
- t_C: The timestamp when the chiplet transfer confirmation was sent by the receiver.
- $\Delta t = t_C - t_I$: The observed transfer time for the chiplet.

We then define the *Geo-Temporal Feasibility Score* as the observed transfer time to the minimum feasible time implied by sender and receiver locations and described as:

$$S_{\text{GT}} = \max\left(0,\ 1 - \frac{\Delta t}{f_T(L_s, L_r)}\right)$$
$$\begin{cases} = 0 \text{ if } \Delta t \geq f_T(L_s, L_r) & \textit{(feasible Tx)} \\ \approx 1 \text{ if } \Delta t \ll f_T(L_s, L_r) & \textit{(suspicious Tx)} \end{cases}$$

A score closer to 1 signifies an increased likelihood that the transaction is artificially recorded on-chain, without a corresponding physical transfer of assets. The exact threshold for S_{GT} at which a transaction is flagged as suspicious or potentially fraudulent is determined by the relevant blockchain authorities and may vary based on the specific application or use case. While attackers can intentionally introduce delays to mimic realistic transfer scenarios, it ultimately reduces the practical advantage of wash trading. Artificial delays would slow down the transaction pipeline and potentially delay the delivery of chiplets to legitimate downstream buyers.

EUs of each chiplet (or IC) lifecycle can compute these anomaly indicators to flag potential cluster wash trading behaviors. Our framework does not rely on any single detection signal, as certain heuristics (e.g., geographical location) may not always be available or verifiable. Instead, it leverages a combination of complementary indicators to ensure detection. These flags can be submitted to trusted authorities decided by the blockchain consortium. By aggregating such flagged reports across multiple *EUs*, trusted authorities can analyze the transaction paths of mutual intermediaries (e.g., frequent appearances of certain distributors) to identify recurring patterns indicative of wash trading. They can further incorporate inventory data, such as the monitoring framework proposed in [12], to detect cases where entities source identical chiplets at higher prices despite the availability of cheaper suppliers with sufficient inventory.

C. Wash Trading Mitigation

Entities engaging in wash trading have the potential to rapidly and unjustifiably inflate their reputation scores if such activities go undetected. To preserve the integrity of the reputation system, it is essential to implement a corrective mechanism that can swiftly and proportionally reduce these artificially inflated scores. To address this risk, we propose a *penalize strictly* scheme. Under this policy, any entity identified as participating in wash trading will incur a reputation penalty reflecting the severity of its involvement.

For each entity along the path, the fraction of reputation to be reduced is governed using a multiplicative decrease parameter k, a global blockchain-level constant that defines the base reduction rate.

For each participating entity, we update its reputation by dividing the previous reputation by a penalizing factor k when wash trading is detected:

$$\texttt{reputation}_{\texttt{new}} = \frac{\texttt{reputation}_{\texttt{old}}}{k}.$$

This penalty can be applied immediately upon detection and operates independently of whether the associated chiplet or IC is found to be defective. By decoupling reputation penalties due to functional correctness from wash trading penalties, the system ensures that strategic manipulation is discouraged regardless of the product's end quality.

V. Results and Discussions

To evaluate the effectiveness of our proposed approach, we simulate a simplified supply chain focusing solely on the chiplet lifecycle, comprising 20 *CMs*, 100 *CDs*, and 20 *ICMs*. For simplicity, each chiplet can pass through up to five distributors before being integrated into an IC. We simulate 10,000 supply chain paths and partition them into five groups based on the number of participating CDs. For each group, we execute 20 million transactions, where each transaction represents the sale of chiplets from manufacturers to distributors, followed by integration into ICs by the *ICMs*.

In each transaction, we take a base price and apply a 15 to 20% markup per hop along the path. We assume a defect probability of one part per million and that each *ICM* can perfectly detect whether a chiplet is defective or tampered. For the reward scheme, we use the sale amount as the rewarding unit divided by the number of entities in the path. However, if the chiplet is defective, we use the same penalty scheme as in [14], where we use a multiplicative decrease parameter (mentioned in Section II) $m = 0.999$ to slash their reputation. The discount factor, d, is set to '2' for trusted consortiums and '1' for untrusted consortiums. Therefore, considering the non-wash trading path in Figure 2(a) as a trusted consortium, CM_1, CD_1, and CD_2 will have their reputation slashed by m, m/d, and m/d^2 respectively. In contrast, for untrusted consortiums, every entity in the transaction path experiences a uniform reputation reduction of m. This approach ensures that reputation decay is more gradual for trusted consortiums than for untrusted consortiums.

We model cyclic wash trading by designating a loop initiator among the chiplet distributors and using previously simulated, non-manipulated paths as a baseline traditional path for comparison. For each occurrence of the initiator in the original path, we insert a predefined set of intermediary distributors immediately following the loop initiator. The path then resumes along its original route, forming the manipulated or wash trading path (see Figure 2(b) for an example path). In the manipulated path, pricing inside the cycle is adjusted slightly to avoid detection of the wash trading activity, while all other entities retain their original baseline price points. This comparison offers insights into the impact of wash trading on reputation scores and the broader supply chain dynamics.

A. Impact of Wash Trading on Honest Participants

Figures 4 demonstrate that the presence of wash traders in the supply chain systematically diminishes the reward potential of all honest, non-wash participants, regardless of whether the consortium is trusted or untrusted. This occurs because the reputations of honest traders are diluted across a larger number of entities during wash trading, unlike in genuine transactions. These findings suggest that under a reputation scheme, if wash trading is not addressed, honest actors are negatively impacted merely through association.

B. Impact of Wash Trading on Wash Traders

We next examine which entities benefit most from wash trading. The loop initiators and intermediary entities involved originate from both trusted and untrusted consortiums. As can be observed in Figures 5(a-j), loop initiators experience a

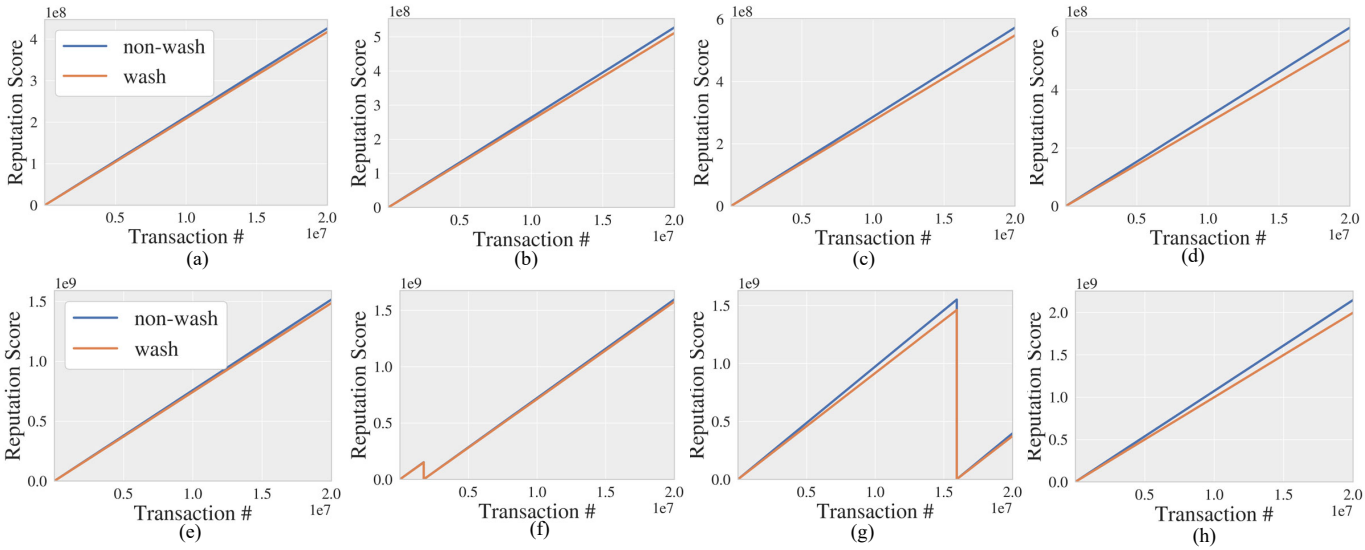

Fig. 4. Reputation comparison of honest traders for cyclic wash trading in a trusted consortium with (a) 2, (b) 3, (c) 4, (d) 5 group of distributors and in an untrusted consortium with (e) 2, (f) 3, (g) 4, and (h) 5 group of distributors.

smaller loss in reputation due to wash trading when engaging in longer trading chains, particularly when no defective chiplets are observed. This advantage arises because, in genuine trading, rewards are distributed among all entities in the chain, resulting in smaller individual shares for participants in longer paths. In contrast, during wash trading, loop initiators appear repeatedly across multiple transactions, thereby accumulating multiple reward instances, unlike genuine trading, where each reward is divided among the entities in the path. However, this advantage diminishes when defective chiplets are detected, as shown in Figures 5(i) and (j). In such cases, repeated appearances can result in multiple penalties being compounded. Given that our reputation scheme applies a multiplicative decrease in reputation scores during a penalty, wash traders find it increasingly difficult to recover their reputation once it declines.

We next analyze the reputation scores of intermediary entities artificially inserted into wash trading cycles. Note that these entities never participated in the supply chain transactions. Our simulation results, as illustrated in Figures 5(k-t), indicate that these intermediaries are often the primary beneficiaries under the current reputation mechanism. Even in cases where their artificial trades incur penalties due to defective chiplets, as seen in Figures 5(s) and 5(t), these entities can gradually recover their net losses over time, thereby maintaining an unfair advantage within the system.

In cluster-based wash trading, cluster initiators are expected to experience reputation changes similar to those of honest traders. This is because, unlike loop initiators, there is no change in the number of appearances between wash trading and genuine trading. However, cluster intermediaries are expected to exhibit reputation score dynamics similar to those of loop intermediaries, as both engage in the same underlying malicious behavior. Likewise, honest traders are expected to show comparable changes in reputation scores in both cluster-based and cyclic wash trading, since they are similarly impacted by the negative effects of longer transaction chains due to the normalization of reward scores.

C. Impact of the Multiplicative Decrease Factor k

The multiplicative decrease factor k governs how aggressively the system removes illegitimate reputation gained through wash trading. Conceptually, this parameter serves as a *correction and punishment mechanism* where larger values result in steeper penalties and eventually a faster convergence back to fair reputation levels. In environments where wash-trading behavior is monitored closely and detected quickly, only limited artificial inflation can occur. In such tight-detection settings, small values of k are sufficient because only modest correction is needed. Conversely, when detection lags and malicious entities are able to accumulate inflated reputation over many iterations, the distortion grows disproportionately. Under these loose-detection settings, larger values of k are necessary to counteract the accumulated gains and restore system-wide fairness. In this way, k ensures proportionality between the scale of manipulation and the intensity of the corrective response.

A multiplicative decrease punishment scheme ensures fairness by reducing reputation in proportion to the total reputation accumulated, regardless of whether that growth resulted from legitimate trading activity or wash trading. As outlined in Section III-A, we classify attackers into two categories, namely foundational wash traders, who initiate malicious behavior from their entry into the framework, and opportunistic wash traders, who first build a substantial reputation through genuine trading activity before engaging in manipulation. If both types of wash traders are detected within the same time window, it may appear that opportunistic actors are penalized more heavily, since they lose a larger amount of genuine reputation compared to foundational attackers. However, this asymmetry is a deliberate and desirable property of our punishment mechanism. Opportunistic wash traders benefit from the system's trust from their earlier legitimate behavior. When they

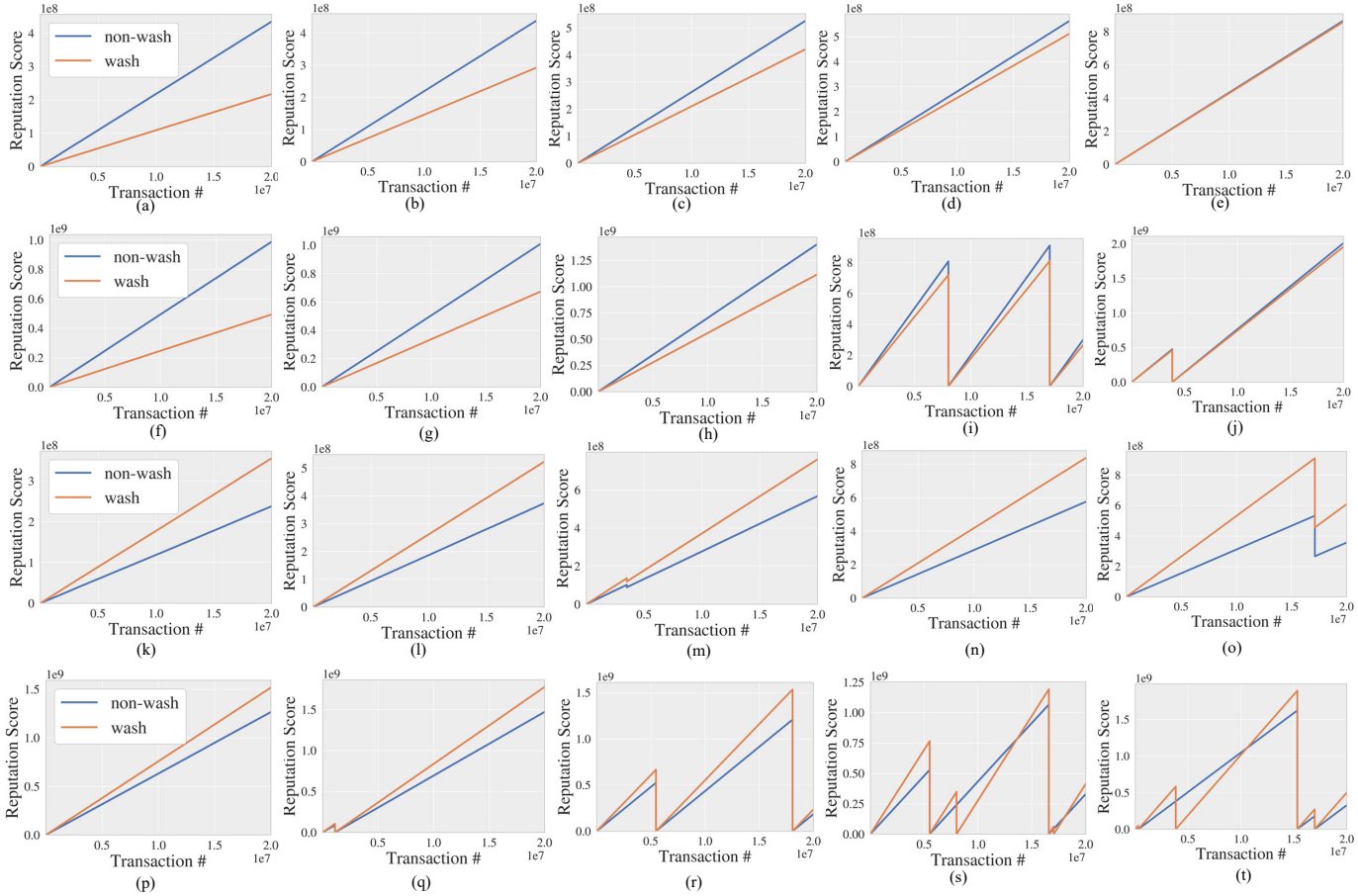

Fig. 5. Reputation comparison for loop initiators for cyclic wash trading in the trusted consortium for (a) 1 (b) 2 (c) 3 (d) 4 (e) 5 group of distributors and in an untrusted consortium for (f) 1 (g) 2 (h) 3 (i) 4 (j) 5 group of distributors. Reputation comparison for loop intermediaries for cyclic wash trading in the trusted consortium for (k) 1 (l) 2 (m) 3 (n) 4 (o) 5 group of distributors and in an untrusted consortium for (p) 1 (q) 2 (r) 3 (s) 4 (t) 5 group of distributors.

deviate from expected norms, the system must enforce stronger penalties to reflect the breach of trust and deter such high-impact manipulation. Therefore, the multiplicative decrease factor not only restores fairness but also reinforces honest participation by allocating punishment in proportion to the influence an entity has accrued within the network. We leave a more detailed investigation of the impact of k across different attacker classes for future work.

VI. Conclusion

In trust-based mechanisms where transactional volume influences reputation, wash trading poses a significant threat by enabling malicious actors to artificially inflate their standing trust score in the incentive scheme. To mitigate this issue, our framework introduces a modified reputation allocation scheme that rewards tighter transaction chains more heavily than longer ones, reducing the incentive for repetitive artificial trades among certain supply chain members. We further strengthen the system through a combination of detection and prevention strategies, implemented in the blockchain framework. Cyclic wash trades can be identified using graph-based cycle detection, while more sophisticated cluster-based behaviors require external markers such as irregular timing between transactions, suspicious trading patterns, and anomalous sale prices. We also discussed the idea that adopting a firm penalization policy, one that sharply reduces the reputation of confirmed wash traders, helps restore fairness and discourages manipulation. Penalties for wash trading were handled independently from those for introducing defective components. Finally, through simulations, we showed the difference in the reputation trajectories of honest participants and wash traders in normal versus wash trading, underscoring the importance of our mitigation strategies.

Acknowledgment

This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-23-1-0312. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Air Force.

Disclosure of AI use. An AI-based language model (ChatGPT, OpenAI) was used to improve grammar and readability of the manuscript. No scientific content was generated by the tool, and the authors retain full responsibility for the accuracy and integrity of the work.

REFERENCES

[1] SEC Charges Two Individuals for Wash Trading Scheme Involving Options of "Meme Stocks", U.S. Securities and Exchange Commission, 2021. https://www.sec.gov/newsroom/press-releases/2021-195.

[2] M. La Morgia, A. Mei, A. M. Mongardini, and E. N. Nemmi, "A game of nfts: Characterizing nft wash trading in the ethereum blockchain," in *2023 IEEE 43rd international conference on distributed computing systems (ICDCS)*, pp. 13–24, IEEE, 2023.

[3] The White House, "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Supply Chain Review Report," 2021.

[4] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware trojans: Lessons learned after one decade of research," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 22, no. 1, pp. 1–23, 2016.

[5] A. Jain, Z. Zhou, and U. Guin, "Survey of Recent Developments for Hardware Trojan Detection," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, 2021.

[6] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[7] M. Tehranipoor, U. Guin, and D. Forte, *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer International Publishing, 2015.

[8] U. Guin, Q. Shi, D. Forte, and M. M. Tehranipoor, "FORTIS: A Comprehensive Solution for Establishing Forward Trust for Protecting IPs and ICs," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 21, no. 4, pp. 1–20, 2016.

[9] S. Bhunia and M. Tehranipoor, *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018. ISBN: 0128124784.

[10] Y. Zhong, A. Ebrahim, U. Guin, and V. Menon, "A modular blockchain framework for enabling supply chain provenance," in *IEEE Physical Assurance and Inspection of Electronics (PAINE)*, pp. 1–7, 2023.

[11] P. Cui, J. Dixon, U. Guin, and D. DiMase, "A blockchain-based framework for supply chain provenance," *IEEE Access*, vol. 7, pp. 157113–157125, 2019.

[12] A. Saha and U. Guin, "Optimizing supply chain management using permissioned blockchains," in *Proceedings of the 43rd IEEE/ACM International Conference on Computer-Aided Design*, pp. 1–7, 2024.

[13] P. E. Calzada, M. S. U. I. Sami, K. Z. Azar, F. Rahman, F. Farahmandi, and M. Tehranipoor, "Heterogeneous integration supply chain integrity through blockchain and chsm," *ACM Transactions on Design Automation of Electronic Systems*, vol. 29, no. 1, pp. 1–25, 2023.

[14] S. T. Valapu, A. Saha, B. Krishnamachari, V. Menon, and U. Guin, "Reward-based blockchain infrastructure for 3d ic supply chain provenance," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 370–380, 2025.

[15] Y. Liu, Z. Liu, Q. Zhang, J. Su, Z. Cai, and X. Li, "Blockchain and trusted reputation assessment-based incentive mechanism for healthcare services," *Future Generation Computer Systems*, vol. 154, pp. 59–71, 2024.

[16] D. Zhu, Y. Li, Z. Zhou, Z. Zhao, L. Kong, J. Wu, J. Zhao, and J. Zheng, "Blockchain-based incentive mechanism for electronic medical record sharing platform: An evolutionary game approach," *Sensors*, vol. 25, no. 6, p. 1904, 2025.

[17] S. Zhou and T. Gao, "Vanets road condition warning and vehicle incentive mechanism based on blockchain," in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 40–49, Springer, 2021.

[18] H. Han, M. Zhang, Z. Xu, X. Dong, and Z. Wang, "Decentralized trust management and incentive mechanisms for secure information sharing in vanet," *IEEE Access*, 2024.

[19] F. Victor and A. M. Weintraud, "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges," in *Proceedings of the Web Conference 2021*, pp. 23–32, 2021.

[20] M. A. H. Ismail, S. B. Zaibon, M. N. A. Hamid, S. I. Mustajap, and A. I. Ismail, "Consumer perceptions and decision-making in the non-fungible token (nft)," *PaperASIA*, vol. 40, no. 3b, pp. 72–80, 2024.

[21] S. Imisiker and B. K. O. Tas, "Wash trades as a stock market manipulation tool," *Journal of behavioral and experimental finance*, vol. 20, pp. 92–98, 2018.