Anti-Counterfeiting in Semiconductor Chip Industry Supply Chain Using Blockchain

***Abstract*—The detection of counterfeit products in the supply chain has become the task of the hour. According to the Semiconductor Industry Association (SIA), counterfeiting has contributed to more than 7.5 billion USD annually in lost revenue and a loss of nearly 11,000 American jobs in 2020 in the semiconductor industry. These counterfeits are created with the intention of deceiving various entities in the supply chain (e.g., distributors, retailers, end-users) into believing that the product is genuine. These counterfeits usually have subpar performance and poor quality. They may even be hazardous for public consumption. Most of the existing solutions have been developed assuming the ideal scenario, not accounting for the real-world situations that may arise (illegitimate transfers, party disputes, etc.) during transactions. This paper aims to develop a tamper-proof B2B (Business-to-Business) system that can accurately detect counterfeit products and identify the malicious stakeholders in the supply chain using blockchain technology. The paper also aims to study and optimise the transaction process between any two entities in the supply chain (manufacturers, distributors, retailers, etc.) while ensuring the authenticity and traceability of each product.**

***Index Terms*—Supply chain, blockchain, security, smart contracts, electronic chips.**

I. Introduction

Counterfeit products in the supply chain pose a significant threat, causing financial losses and damaging trust, reputation, and brand image for all the stakeholders (manufacturers, distributors, and retailers) involved. Despite successful detection efforts in various industries including agriculture, pharmaceuticals, bills, etc., there is a research gap in addressing counterfeit issues, specifically within the electronic chip industry. Bridging this gap is crucial for preventing counterfeit electronic chips from entering the market. These counterfeit chips are usually of two types: one that is a clone of the original product and another that is, in essence, a component recycled from electronic waste. The COVID-19 pandemic caused a global semiconductor shortage, which led to an increase in demand for chips and created an environment ripe for the infiltration of counterfeit products into the market [1]–[3]. Counterfeit chips pose significant risks to the reliability, safety, and security of electronic devices. This shortage highlighted vulnerabilities in the global supply chain, prompting collaborative efforts to address the issue and strengthen supply chain resilience to ensure a more robust semiconductor ecosystem in the face of future disruptions. This paper aims to establish a robust system for real-time monitoring, tracking, and traceability of the product throughout its entire journey within the supply chain, achieved through the use of blockchain technology. The primary focus of this paper is to optimise the transaction processes occurring between two stakeholders or entities within the supply chain. Through this solution, any entity involved in the supply chain can seamlessly verify the authenticity of the product at any given moment which increases transparency and acts as a powerful tool against counterfeiting. The solution also aims to pinpoint the source of maliciousness, i.e., the entity that has introduced the counterfeit products on the chain. This can be achieved via the decentralised nature of blockchain, which ensures immutable and secure records. The use of cutting-edge blockchain technology makes it possible to track and analyse product data in great detail, providing stakeholders with useful information about status and location, hence enhancing traceability in the supply chain [4], [5]. The following section will discuss some of the related work in the semiconductor industry using blockchain technology.

II. Related Work

In this section, the current knowledge of the area is presented, and substantial findings that contribute to shaping, informing, and reforming this paper are reviewed. As part of this comprehensive literature survey, sources in the intersecting fields of the supply chain, blockchain, and electronics industry have been covered by the authors. Islam et al. [6] propose an embedded physically unclonable function (PUF) to establish the distinctive correspondence. The blockchain ensures the legitimacy of an Integrated Circuit's (IC) current owner, while the PUF safeguards against IC counterfeiting and tampering. Anita et al. [7] use Radio Frequency Identification (RFID) tags and blockchain technologies. The Ethereum platform, which is a public blockchain, is used for transactions. Proof of Authority (PoA) consensus algorithm was used. The confidentiality of transactions is ensured by making use of "zk-SNARKS" on the blockchain. Xu et al. [8] propose a consortium blockchain-based Certificate Authority (CA) framework for chip information management, involving four steps: enrollment, ownership release, verification, and ownership acquisition. A Merkle tree hash algorithm is used to create PCB identification (PID) from Electronic Chip Identification (ECID), with SHA-256 as the hash function.

Cui et al. [9] present a Hyperledger Fabric-based blockchain framework using Proof of Work (PoW) algorithm for electronic parts traceability in the supply chain, utilising ECIDs and PUFs. Cryptographic techniques ensure the privacy and security of sensitive supplier and buyer data. The system proposed by Benčić et al. [10] use a combination of DLT and "Smart Tags" to create a secure and decentralised network

[*] These authors contributed equally.

using an asynchronous message passing system for managing supply chain data. DLT provides a tamper-proof and immutable record of all transactions and changes made to the supply chain, while smart tags allow for real-time tracking and monitoring of products throughout the supply chain. Vosatka et al. [11] propose a novel methodology to address the detection and tracking of recycled ICs by leveraging intrinsic and internal hardware centric properties checked by the combating die and IC recycling (CDIR) sensor at each stage of the electronics supply chain. Herrgoß et al. [12] designed a blockchain solution to enhance the analytic capabilities of this facility using the design science approach and evaluate the economic value of the designed application using the analytical hierarchy process. Oi et al. [13] propose the utilisation of Physically Unclonable Function (PUF), a device-specific and challenging-to-copy information, instead of traditional RFID or QR codes. It employs sensors to capture measured features and separate transaction information, converting them into keys recorded on the blockchain for reproducibility and uniqueness. In the work presented by Chaudhary et al. [14], they have highly reduced the cost of implementing the interaction by storing the CRP on a distributed file system called the InterPlanetary File System (IPFS) and have also implemented and analysed the interfacing for 'IC traceability' to ensure the current ownership of a product, its point of origin, and ownership history in the SCM system. write in third person. Khan et al. [15] provide an IoT-enabled blockchain-based system for tracking all post-production activities, business processes, and electronic device operations. Five smart contracts underpin the system, recording user actions on an immutable distributed ledger to help guarantee transparent, traceable, and secure business processes carried out by participants. The relevant information is stored on a distributed storage system.

In the following section, we present our methodology designed to bridge the gap between two entities within the supply chain system.

III. Proposed Methodology

The analysis of existing literature has exposed a significant void in current solutions. This gap pertains to the lack of comprehensive discussions regarding the transactional processes between entities and the verification procedures that follow product transfers. Additionally, there is a dearth of exploration into the repercussions or corrective measures in cases involving counterfeit products. These challenges arise due to the physical form of the products, necessitating their physical delivery across different locations. This overhead introduces potential issues and opportunities for malicious activities. Our proposed solution makes use of different verification techniques, to identify the entity responsible for maliciousness.

The features of blockchain provide a robust foundation for a secure and reliable counterfeit detection system in complex supply chains. The solution relies on the implementation of a permissioned blockchain network, which is known for its controlled and secure environment. A preference for permissioned networks over public ones arise from several advantages. Access control limits participation to a predefined group, ensuring control over network membership for enhanced security. Permissioned networks often demonstrate higher transaction throughput and more controlled scalability. Additionally, participants can manage data confidentiality and selective disclosure, allowing for private transactions and controlled information sharing. In this section, we will delve into the proposed methodology, wherein we will discuss key assumptions underlying the paper, elucidate the architectural framework, and explore the algorithms in depth.

A. Assumptions

This section shall discuss the assumptions made prior to commencing the paper.

- The primary emphasis will center on optimising the transactional processes that occur between any two entities on the chain.
- The specific focus will be directed towards the semiconductor supply chain.
- Manufacturers are regarded as trusted and verified entities. All verification values provided by the manufacturers are assumed to be true and binding. All the remaining stakeholders must undergo verification, prior to their inclusion in the network.
- It is assumed that all raw materials utilized by the manufacturer in the production of semiconductor chips are authentic. The sourcing of these concerned materials is considered to be outside the scope of this paper.

In the upcoming section, a thorough exploration of the architecture will be conducted, aiming to provide a detailed understanding of its structural components, design principles, and underlying mechanisms.

B. Architecture

Integral units include a multitude of stakeholders, including manufacturers, producers, distributors, retailers, etc., the execution of smart contracts among these participants; and their involvement in a unified blockchain network. This integration between the various components ensures comprehensive end-to-end visibility and transparency throughout the supply chain process. The integration of blockchain technology into the supply chain introduces a decentralised and transparent framework, enhancing traceability, security, and trust. The system incorporates a distributed ledger network, ensuring every product's journey is recorded and traceable across multiple nodes. Smart contracts, encoded on the blockchain, automate and enforce agreements among supply chain participants, fostering transparency and minimising disputes. Each product is assigned a unique digital identity, allowing stakeholders to access detailed information through a decentralised network. This combination of features reduces reliance on intermediaries, promotes collaborative practices, and accelerates processes such as payment settlements, ultimately optimising the efficiency of the entire supply chain.

Fig. 1 shows our high-level design of the flow that we propose and have implemented in the further sections. This

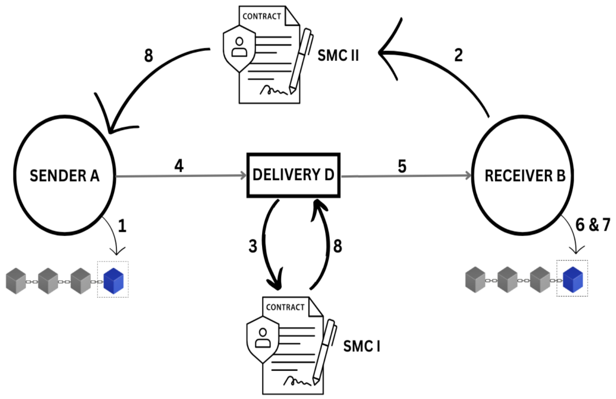

Fig. 1. Data Flow between two entities at High Level

consists of two entities (any of the stakeholders) and the delivery system in between them. There are two smart contracts involved as a part of this.

In this transaction flow, the Sender (A) puts product verification values on the blockchain. After a deal is agreed between A and Receiver (B), B transfers the full amount to escrow, and Delivery Entity (D) deposits a stake. The product moves from A to D and then to B. B verifies the product against the original manufacturer's values and A's values. If everything matches, B pushes verifications to the blockchain, and the full amount goes to A. If not, malicious parties are flagged, and stakes are handled accordingly.

C. Algorithms

1) Process Flow: In the process of conducting a transaction between parties A and B, A initiates the verification of chip values on the blockchain. Upon reaching an agreement, B transfers the complete amount to a Smart Contract II (SmC II) escrow. Subsequently, party D deposits a predetermined stake amount, S, into Smart Contract I (SmC I). The product is then transferred from A to D, followed by another transfer from D to B. At this point, B performs a meticulous verification of the product, comparing its values with both the original manufacturer's values and those asserted by A. If all three values match, the process proceeds to the next step. However, if A's values match those of the manufacturer and B's values do not align with A's, D is deemed malicious, resulting in the non-return of the delivery stake to D, with the escrow money reverting to B. D is then flagged from the network, and a party dispute with D ensues, leaving A without financial compensation despite the loss of their product. Conversely, if A's values do not match those of the manufacturer, A is considered malicious, leading to the return of the delivery stake to D and the escrow money to B, while A is flagged from the network. Upon successful verification, B pushes the values onto the blockchain, and the stake amount is returned to D, with the full transaction amount transferred to A, completing the process. The algorithm is summarised as follows:

Algorithm 1 Process Flow

```
1: A puts verification values of the chip on the chain.
2: Deal agreed by A & B. Starts process. B transfers the complete amount into Escrow II.
3: D deposits stake amount $S$ (decided by agreed by A & D) into Escrow I.
4: Transfer product from A to D.
5: Transfer product from D to B.
6: B does verification of the product and compares with original manufacturer values and A's values. ($M = Manufacturer$)
7: B should push verification values onto the blockchain.
8: Stake amount is returned to D, and the full amount is transferred to A on successful transfer.
```

2) Verification: The verification process is done on the receiver's end when the receiver (B) receives the product from the sender (A). This step is crucial in order to maintain and verify the product's authenticity. Proper verification is required to be done at each stage in order to enable traceability of the product in cases of mishap. The verification algorithm is as follows:

Algorithm 2 Verification

```
Input: Manufacturer values (M), Sender values (A), Receiver values (B)
Output: Boolean
if all 3 values match then
    Product isn't counterfeit, return True
else if $A = M$ & $B \neq A$ then
    Product is counterfeit, return False. (D is malicious. Delivery stake isn't returned to D. Escrow money returns to B. D is flagged from the network. A doesn't get money even though he has lost his product. Party dispute with D.)
else if $A \neq M$ then
    Product is counterfeit, return False. (A is malicious. Delivery stake returns to D. Escrow money returns to B. A is flagged from the network.)
```

When B receives the product from A, B performs physical verification of the product in terms of performance, compute, etc. in order to ensure authenticity. B then proceeds to compare these metrics with the values uploaded by the predecessors (P) and the original Manufacturer (M) on the chain. If the product is not counterfeit, B uploads their testing values to the chain. If the product is detected to be counterfeit, necessary further action is taken.

IV. Algorithm Discussion

The resilience of the proposed system is examined here with the exploration of different hypothetical scenarios.

A. Scenario 1: Sender is malicious

Suppose A is a malicious entity. It has received a genuine product and is sending a counterfeit product to B via D. B receives the product and tests the verification values. Since the product is counterfeit, the values will not match those uploaded by the manufacturer. Similarly, A's uploaded values will also not match the manufacturer's values when cross-checked. This leads to the conclusion that A is malicious. A party dispute is raised against A with necessary refund measures like delivery stake returning to D and escrow amount returning to B due to them not receiving their product.

B. Scenario 2: Delivery entity is malicious

Suppose D is a malicious entity. A is trying to send a genuine product to B via D. D interferes in the transfer and sends counterfeit product to B. Like in the previous scenario, B receives the product and tests the verification values. Since the product is counterfeit, the values will not match those uploaded by the manufacturer. However, A's uploaded values will match the manufacturer's values when cross-checked.We can conclude that D is malicious. A party dispute is raised against D. D loses the delivery stake as well.

V. Conclusion

The solution successfully optimised transaction flow in the semiconductor chip supply chain, enhancing efficiency and reducing counterfeiting risks.Demonstrated blockchain's effectiveness in terms of transparency and immutability for combating counterfeiting. This has been proposed keeping in mind the real-world scenario. This solution precisely identifies the specific point at which malicious activities occur, aiding in the detection of the entity causing counterfeiting. While the implementation involves the use of blockchain, which may incur additional costs, the tradeoff is justified given the high-value nature of the industry.

VI. Future Work

Going ahead, the aim is to implement this solution on a blockchain platform like Ethereum or Hyperledger Fabric. Post that, the solution can be adapted in real-world industries where adaptability and efficacy can be ascertained. Moving forward, these are the avenues for future research and development in the realm of blockchain-based supply chain solutions. Firstly, optimising energy consumption is essential to any blockchain-based system. This will encourage adoption from an environmental standpoint. Additionally, addressing the scalability challenge and researching low-latency solutions will be important as the number of transactions grows. It is important to address this as the solution is implemented in the real world.

References

[1] Katsaliaki, K., Galetsi, P. and Kumar, S. ”Supply chain disruptions and resilience: a major review and future research agenda” Ann Oper Res 319, 965–1002 (2022). doi: 10.1007/s10479-020-03912-1

[2] Alok Raj, Abheek Anjan Mukherjee, Ana Beatriz Lopes de Sousa Jabbour, Samir K. Srivastava, ”Supply chain management during and post-COVID-19 pandemic: Mitigation strategies and practical lessons learned”, Journal of Business Research, Volume 142,2022, Pages 1125-1139, ISSN 0148-2963, https://doi.org/10.1016/j.jbusres.2022.01.037

[3] Wassen Mohammad, Adel Elomri, Laoucine Kerbache, ”The Global Semiconductor Chip Shortage: Causes, Implications, and Potential Remedies”,IFAC-PapersOnLine, Volume 55, Issue 10,2022, Pages 476-483, ISSN 2405-8963, https://doi.org/10.1016/j.ifacol.2022.09.439

[4] D. Shakhbulatov, J. Medina, Z. Dong and R. Rojas-Cessa, ”How Blockchain Enhances Supply Chain Management: A Survey,” in IEEE Open Journal of the Computer Society, vol. 1, pp. 230-249, 2020, doi: 10.1109/OJCS.2020.3025313.

[5] S. Johny and C. Priyadharsini, ”Investigations on the Implementation of Blockchain Technology in Supplychain Network,” 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 1-6, doi: 10.1109/ICACCS51430.2021.9441820.

[6] M. N. Islam, V. C. Patii and S. Kundu, ”On IC traceability via blockchain,” 2018 International Symposium on VLSI Design, Automation and Test (VLSI-DAT), Hsinchu, Taiwan, 2018, pp. 1-4, doi: 10.1109/VLSI-DAT.2018.8373269.

[7] Anita, N., Vijayalakshmi, M. and Shalinie, S.M , ”Blockchain-based anonymous anti-counterfeit supply chain framework,” Sādhanā 47, 208 (2022), https://doi.org/10.1007/s12046-022-01984-2

[8] Xu X, Rahman F, Shakya B, Vassilev A, Forte D, Tehranipoo M. Electronics Supply Chain Integrity Enabled by Blockchain. ACM Transact Des Autom Electron Syst. 2019;24(3):10.1145/3315571. doi: 10.1145/3315571. PMID: 32116465; PMCID: PMC7047669.

[9] P. Cui, J. Dixon, U. Guin and D. Dimase, ”A Blockchain-Based Framework for Supply Chain Provenance,” in IEEE Access, vol. 7, pp. 157113-157125, 2019, doi: 10.1109/ACCESS.2019.2949951.

[10] F. M. Benčić, P. Skočir and I. P. Žarko, ”DL-Tags: DLT and Smart Tags for Decentralized, Privacy-Preserving, and Verifiable Supply Chain Management,” in IEEE Access, vol. 7, pp. 46198-46209, 2019, doi: 10.1109/ACCESS.2019.2909170.

[11] J. Vosatka et al., ”Confidence Modeling and Tracking of Recycled Integrated Circuits, Enabled by Blockchain,” 2020 IEEE Research and Applications of Photonics in Defense Conference (RAPID), Miramar Beach, FL, USA, 2020, pp. 1-3, doi: 10.1109/RAPID49481.2020.9195666.

[12] L. Herrgoß, J. Lohmer, G. Schneider and R. Lasch, ”Development and Evaluation of a Blockchain Concept for Production Planning and Control in the Semiconductor Industry,” 2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, Singapore, 2020, pp. 440-444, doi: 10.1109/IEEM45057.2020.9309979.

[13] S. Oi, K. Kaneda and K. Iwamura, ”Implementation of Supply Chain Management System to Prevent Counterfeit Using IoT device and Blockchain,” 2022 2nd International Conference on Image Processing and Robotics (ICIPRob), Colombo, Sri Lanka, 2022, pp. 1-6, doi: 10.1109/ICIPRob54042.2022.9798734.

[14] C. K. Chaudhary, U. Chatterjee and D. Mukhopadhayay, ”Auto-PUFChain: An Automated Interaction Tool for PUFs and Blockchain in Electronic Supply Chain,” 2021 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Shanghai, China, 2021, pp. 1-4, doi: 10.1109/AsianHOST53231.2021.9699720.

[15] A. U. R. Khan and R. W. Ahmad, ”A Blockchain-Based IoT-Enabled E-Waste Tracking and Tracing System for Smart Cities,” in IEEE Access, vol. 10, pp. 86256-86269, 2022, doi: 10.1109/ACCESS.2022.3198973.