Thwarting Counterfeit Electronics by Blockchain

Muhammad Monir Hossain*, Nidish Vashistha*, Jeffery Allen†, Monica Allen†, Farimah Farahmandi*,Fahim Rahman*, and Mark Tehranipoor*
*Electrical and Computer Engineering, University of Florida,
Gainesville, Florida 32611 USA
†Air Force Research Laboratory, Eglin Air Force Base, FL 32542 USA

Abstract

Counterfeit electronics are ubiquitous in various applications, from computing devices to space applications. Thesemay raise severe safety concerns in security-critical applications and incur a significant revenue loss for original device manufacturers. Several approaches are developed based on hardware intrinsic properties and sensor systems to thwart counterfeit electronics. However, most of these approaches demand a technical skill-set and sophisticated tools, making the supply chain entities inconvenient to verify on the go. In this article, we propose a blockchain-based framework, which leverages traceability and provenance records to overcome the existing limitations in verifying the authenticity of electronic devices.

I. Introduction: counterfeiting and traditional verification challenges

Today electronic devices are found in almost every partof our life and society. For this reason, counterfeit devices open the door to significant loss of revenue and reputation to the industry as well as harm to society as a whole. Makingthe situation worse, during the Covid-19 pandemic, high demand and insufficient production of genuine microelectronic components lead to opportunists injecting counterfeit parts into the supply chain. Furthermore, these counterfeit parts area major concern for both industry and government alike. A recent report prepared by the US armed services committee shows that around 15% of all spare and replacement electronicparts used by the Pentagon are counterfeits [1].

Several entities are involved in a typical semiconductorsupply chain from the manufacturing stage to the final productdelivery to the end-users. An overview diagram in Figure 1 illustrates various supply chain entities (or stages) and some possible types of counterfeiting devices associated with every stage. Original Component Manufacturer (OCM) designs and manufactures electronic ICs. OCM can be classified into two categories: Integrated Device Manufacturer (IDM), who owns the foundry, and the other is a fabless design house. In the case of fabless OCM, the layouts of ICs are given to an outsourced foundry for production. Only OCM is considered trusted while distributors, PCB Assembler, System Integrator, and Recycler are untrusted as they may sell counterfeit ICs or insert them into Printed Circuit Boards (PCB) or hardware systems. For example, foundry may clone ICs and manufactureout-of-contract, known as overproduced ICs. The foundry can sell them to the chip distributors, and thus these counterfeit ICs can traverse the supply chain. On the other hand, recyclers may resell the used ICs to the distributors in the black market. They can also remark the ICs to sell them at a higher price. These counterfeit ICs are embedded in PCBs by the PCB assembler and later used in developing hardware systems by the System Integrator. Finally, the counterfeited hardware systems are sold to the end-users.

There is a significant amount of research on the techniques for authenticating electronics by leveraging hardware intrinsic properties or on-chip sensory systems to distinguish genuine and counterfeit ICs. Some commonly used sensors are Combat Die and IC Recycling (CDIR) [2], silicon odometers to prevent recycled ICs, and PUF [3], [4] against cloning. Active hardware metering approaches such as CSST [5] are developed to prevent untrusted foundry and assembly from counterfeiting, such as overproduction. However, these approaches require a sophisticated technological setup, skill set, and significant time and cost. As a result, most supply chain entities are reluctant to use these techniques. On the other hand, existing centralized IC verification approaches useunique identifiers such as serial numbers, which can help the end-users identify an IC but cannot establish provenance. Hence, they are not an effective solution for IC verification.

II. Blockchain-based solution

Blockchain is a distributed ledger technology that enables storing transactions as a chain of blocks [6]. Blockchain technology relies on the certificate authority network rather than a centralized operation, consisting of distributed nodes and making transactions posted in the ledger through the consensus by collecting votes from the participating nodes. Blockchain technology is a promising solution for the following featuresto mitigate the limitations of existing approaches for thwarting counterfeit devices.

- Integrity assurance of the transactions due to decentralized systems.
- Posting transactions on the blockchain ledger (BCL) upon the approval of all participating peers.
- Immutable ledger, the posted transactions can't be tampered with or deleted.
- Availability and traceability of provenance records from BCL.

Several existing techniques leverage the core features of blockchain technology to detect counterfeiting and achieve supply chain integrity, such as [7–10]. In [7], supply chain modeling and protocols have been implemented for detecting counterfeit devices based on ECID and PUF based verification. These approaches also suggest utilizing intrinsic device properties (e.g., PUF), odometers, and blockchain for detecting counterfeit devices. In [8], [10], algorithms and confidence modeling on the genuineness of ICs are implemented based on ECID and PUF verification. However, these approaches lack practicability and implementation capability for achieving end-to-end traceability to detect counterfeit devices.Again, these approaches have some dependencies on hardware modules (e.g., PUF), which makes some supply chain entities, such as distributors, unable to verify them on the go.

We propose a blockchain-based verification infrastructure for detecting counterfeit hardware devices for the electronic life cycle. Our proposed framework covers a wide range of counterfeiting by analyzing tracking and provenance certifications among various entities throughout the supply chain recorded in BCL. A fully functional prototype of the proposed framework has been developed. The details can be found in [11].

III. Proposed framework

There have been numerous solutions introduced to the market since the invention of the blockchain. Their style can beof the public, private, or consortium. Like the crypto-currency Bitcoin,

public blockchains are open to everyone. While private blockchains can be accessed through a single point of contact, they are more common within larger organizations with multiple departments. Consortium-style blockchains have more than one central point of contact, making them better suited for multi-organizational enterprises. Every peer can join after the approval process, and hence all peers are known to the blockchain administrator. In consortium-style blockchains, fewer transactions are posted, and the consensus is achieved through a multi-party consensus algorithm. Compared to the public blockchain, a smaller number of peers usually participate in the consensus; as a result, it can provide a higher transaction rate. Furthermore, a new peer node, asset verification, and transactions are approved by voting of other peers involved in the blockchain network, bringing transparency to supply chain activities. Again, unlike public blockchain, transactions in the consortium-style blockchain do not require any fees. As a result, consortium-style blockchain is best suited for the electronics supply chain. Henceforth, the developed blockchain network will be referred to as *eChain*.

A. Overview of Proposed Architecture

OCMs, IC Distributors, PCB Assemblers, PCB Distributors, System Integrators, and System Distributors are all considered in our design as blockchain peers. Each peer has the most recent copy of the distributed ledger database and smart contracts. Any peer can access this blockchain network using distributed applications (DApps) to conduct various supply chain operations and verification. The technical architecture of *eChain* is based on the Hyperledger Fabric [12]. *eChain* architecture includes the following components (see Figure 2):

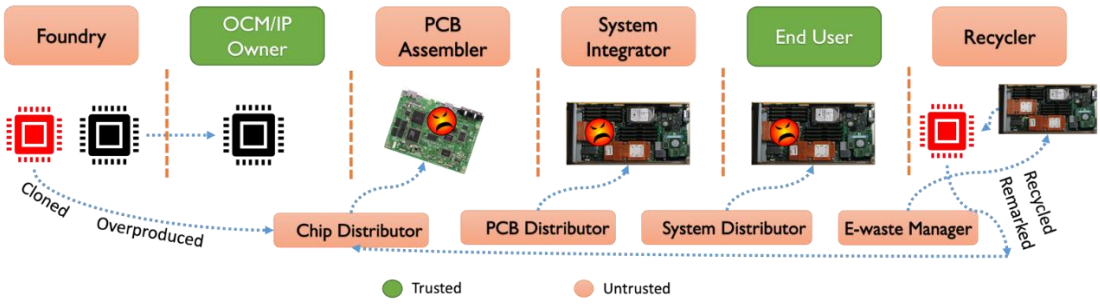

Fig. 1. Overview of supply chain entities and example sources of counterfeits in the electronic supply chain

- **Consortium Configuration Manager** establishes the *eChain* infrastructure's rules and policies. For example, this component configures and controls *eChain* enrollment operations and prevents other peers except for OCM from enrolling electronic chips.

- The **Certificate Authority** component issues digitallysigned certificates to consortium members for identification and transaction signing prior to posting.

- The **Membership Service Provider** authenticates, authorizes, and manages the consortium members' identities.

- The **Data Privacy Manager** module encrypts incoming data to the *eChain* and prevents

intellectual property theft.

- A **Smart Contract** is a self-executing contract that translates the terms of the agreement between peers into lines of code. Smart contracts can carry out supply chain operations such as creating, updating and verifying ownership records from the distributed ledger to track andprove the provenance of ICs. The code and the business agreements contained within it are distributed across the *eChain's* distributed peer nodes.

- **Verification Manager** does not reflect an actual component of the *eChain*. Still, it collectively manages enrollment of ICs, supply chain transactions, and verificationof records from the ledger by using smart contracts.

- In *eChain*, the **Transaction Manager** is critical to the execution of supply chain operations. This component accepts supply chain operation requests from smart processes. It collects simulated transaction results from peer nodes after dispatching the request to all peers. It reachesa consensus and executes the requested transactions based on the majority voting policy. Finally, it appends theapproved transactions into the distributed ledger databaseas blocks.

- **Blockchain Application Programming Interface (API)** provides application developers with a remote programmable interface to the *eChain* management core. A developer, for example, can use API to process transactions, membership services management, node traversal to search records, and event handling to broadcast posted transactions to peers [12].

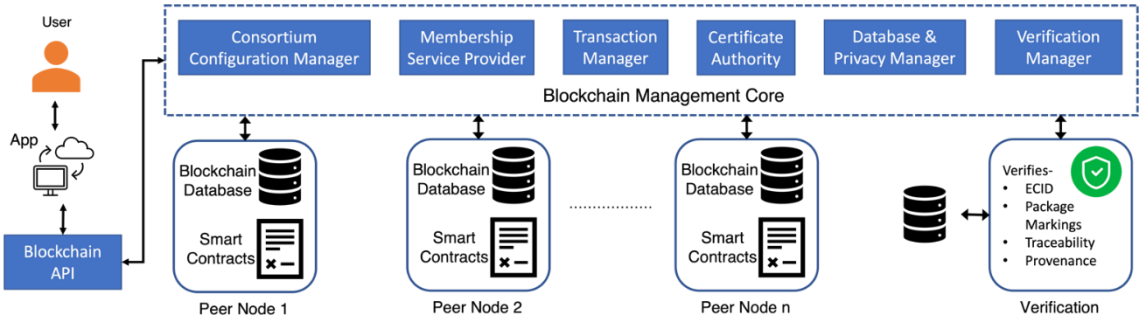

Fig. 2. A high-level architecture of eChain for electronic supply chain integrity

B. *Enrollment and Supply Chain Operation*

Smart contracts can enroll IC and execute supply chainoperations between different entities. An IC can go through various entities by changing hands until it reaches the end-user. Here are the mainstream entities and respective events that allow the movement of an IC in the supply chain:

- Secure enrollment of ICs by OCM; it ensures every IC with a unique identifier (Electronic Chip ID (ECID) or Serial Number) is loaded into the *eChain* ledger.

- Dispatching ICs to distributors by OCM to sell into the market.
- A PCB assembler buys IC from IC distributors.
- (Optional) A PCB distributor sells PCB assembled by PCB assembler to a system integrator.
- A system integrator builds a system with PCB.
- (Optional) A system distributor sells systems to an end-user.
- An end-user buys a system directly from the system integrator.

C. Counterfeits Detection in eChain

The *eChain* detects counterfeit chips embedded in any system by leveraging the tracking and traceability information obtained from the blockchain ledger. This section discusses the schemes for detecting recycled, remarked, cloned, and overproduced ICs. A high-level detection algorithm is shown in Figure 3.

1) Recycled IC Detection: Recycled ICs are those in the electronic supply chain which are de-soldered from a rejected PCB or a system and reentered into the electronic supply chain. These recovered ICs are claimed as new ones by the seller and thus again used in PCB or system development. For detection, our framework first verifies the validity of the requested chip ID. If the chip ID is enlisted in the BCL (proof of valid ID), it puts a data pull request from the BCL. Our framework then analyzes data from the blockchain ledger and extracts traceability information from all recorded transactions for the IC. If the current owner of the IC is found in any later stages, it is classified as a recycled IC. For example, assume an adversarial IC distributor buys used ICs from a recycler, and a used IC is inserted in lots of genuine ICs. Later, a PCB assembler purchases the ICs and requests to verify the authenticity. The *eChain* network will find the current stage of the IC as end-user level, where the IC distributor claims as the owner; hence it is a recycled IC.

2) Remarked IC Detection: Package markings are embedded on the top of the IC package. These markings contain short codes that resemble various manufacturing and performance grade data. The adversary has a very strong motivation to tamper with the IC grade among all package information. For example, a BAE radiation-hardened processor (e.g., RAD750) costs around $200000 as compared to a commercial processor of only a few hundred dollars [13]. Our proposed framework stores the package markings of the authentic chips in BCL against the chip ID during the enrollment phase. A remarked IC will have modified external package marking, but the internal ID such as ECID remains the same. Verification by the IC owner of the claimed chip grade against its ID from the ledger detects the remarked IC in the supply chain. Thus, our proposed technique detects the remarked ICs in the supply chain. However, in the case of a cloned ECID, an unclonable-based ID (e.g., PUF-based IDs) is required, which is outside of the scope of this article.

3) Cloned IC Detection: Cloning is a common counterfeiting approach that allows adversaries to develop a chip without any substantial investment in intellectual property, large research facilities, and development work. Cloning of ICs can be done in various ways, such as by reverse engineering, by illegally stealing Intellectual Property (IP) such as layouts, netlists, etc.

Reverse engineered cloned ICs may possess valid ECID leading to typical ECID-based verification recognizing them as genuine ICs. On the other hand, our proposed framework detects these cloned ICs by analyzing the traceability information obtained from the BCL. Traceability plots the traversing of the IC from the OCM to the current stage. The IC is detected as cloned if the selling entity does not exist as an owner in the traceability information.

4) Overproduced IC Detection: The process of manufacturing and selling ICs out of contract by the foundry is known as overproduction. The overproduction often leads to a significant loss of revenue for the OCM. In the case of overproduced ICs with valid ID, our framework can detect them by analyzing the traceability information of ICs. Andif the overproduction ends up in nefarious hands with invalid IDs, our framework can quickly identify them because they are not enrolled in the blockchain ledger by the

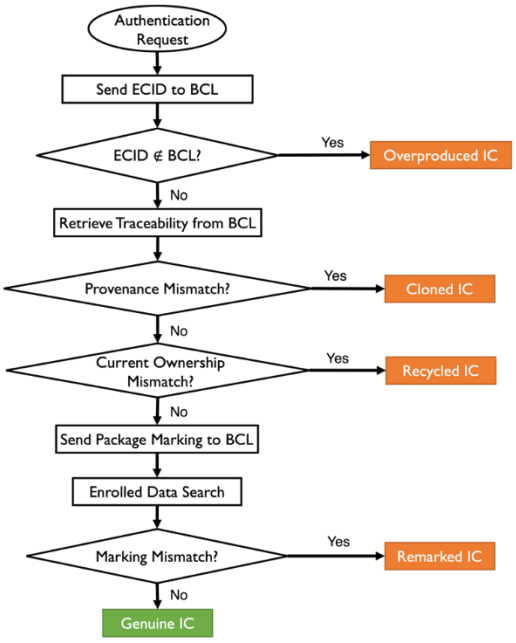

Fig. 3. Workflow for various counterfeit ICs detection.

IV. Conclusion and future work

A blockchain-based electronic device counterfeiting detection framework was presented in this article. We have presented the architectural design to show the practicality of the proposed scheme. We have discussed the detection schemes for recycled, remarked, cloned, and overproduced ICs. However, it can be extended to detect other counterfeitings, such as forged documentation and malicious activity in the supply chain to determine the specific counterfeiting entity. In the future, the framework can be extended to comply with comprehensive data privacy, the conjunction of multiple ledgers in case of numerous blockchain ledgers from various OCM, PCB assemblers, or System Integrator. Thefuture works can also include quick data search in the ledger, faster enrollment, and enhancements of blockchain parameters such as peer nodes policy, consensus, etc.

V. Acknowledgment

The authors MMH, NV, FF, FR, and MT would like to acknowledge funding support through award number FA8651- 19-F-1032 (AFRL). The authors JA and MA would like to acknowledge funding support through AFOSR lab task 22RWCOR002.

VI. References

[1] https://www.govinfo.gov/content/pkg/CHRG-112shrg72702/html/CHRG-112shrg72702.htm

[2] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "Low-cost on- chip structures for combating die and ic recycling," in *51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2014,pp. 1–6.

[3] M. M. Tehranipoor, U. Guin, and D. Forte, "Counterfeit integrated circuits,", in *Counterfeit Integrated Circuits.* Springer, 2015, pp. 15–36.

[4] M. Tehranipoor, H. Salmani, and X. Zhang, "Integrated circuit authentication," *Switzerland: Springer, Cham.*, vol. 10, pp. 978–3, 2014.

[5] M. T. Rahman, D. Forte, Q. Shi, G. K. Contreras, and M. Tehranipoor, "Csst: Preventing distribution of unlicensed and rejected ics by untrusted foundry and assembly," in *IEEE International symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFT)*, 2014, pp. 46–51.

[6] M. Pilkington, "Blockchain technology: principles and applications," in *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.

[7] X. Xu, F. Rahman, B. Shakya, A. Vassilev, D. Forte, and M. Tehranipoor, "Electronics supply chain integrity enabled by blockchain," *ACM TODAES*, vol. 24,no. 3, pp. 1–25, 2019.

[8] J. Vosatka, A. Stern, M. Hossain, F. Rahman, J. Allen, M. Allen, F. Farahmandi, and M. Tehranipoor, "Tracking cloned electronic components using a consortium-based blockchain infrastructure," in *IEEE PAINE*, 2020,pp. 1–6.

[9] 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.

[10] J. Vosatka, A. Stern, M. Hossain, F. Rahman, J. Allen, M. Allen, F. Farahmandi, and M. Tehranipoor, "Confidence modeling and tracking of recycled integrated circuits, enabled by blockchain," in *IEEE RAPID*, 2020, pp. 1–3.

[11] N. Vashistha, M. M. Hossain, M. R. Shahriar, F. Farahmandi, F. Rahman, and M. Tehranipoor, "echain: A blockchain-enabled ecosystem for electronic device authenticity verification," *IEEE Transactions on Consumer Electronics*, 2021.

[12] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[13] J. Rhea, "Bae systems moves into third generation rad-hard processors," *Military & Aerospace Electronics*, vol. 13, no. 5, 2002.

VII. Biography section

Muhammad Monir Hossain (S'14) received B.Sc. in EEE from Bangladesh University of Engineering and Technology (2015) and currently pursuing Ph.D. at ECE, University of Florida. He is an IEEE student member.

Nidish Vashistha (S'09) received M.S (2015) in ECE and currently a Ph.D. candidate at ECE department, University of Florida. He is an IEEE student member.

Farimah Farahmandi (S'13-M'18) is an Assistant Professor in ECE at University of Florida (UF). She completed Ph.D. from CISE at UF (2018). Currently, she is the associate director of Edaptive Computing Inc, Transition Center at UF. She is an IEEE member.

Fahim Rahman (S13-M19) received MS in ECE from University of Connecticut (2015). He received Ph.D. in ECE from University of Florida (2018). Currently, he is a Research Assistant Professor at ECE, UF. He is an IEEE member.

Mark M. Tehranipoor (F'18) is currently the Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity at University of Florida. He is currently serving as founding director for Florida Institute for Cybersecurity Research (FICS). He is a Fellow of IEEE and ACM.