Electronics Supply Chain Integrity Enabled by Blockchain

Xiaolin Xu[1], Fahim Rahman, Bicky Shakya[2], Apostol Vassilev[3], and Domenic Forte*, Mark Tehranipoor†[4]

[1] University of Illinois at Chicago, 851 S. Morgan St., Chicago, IL 60607 ‡

[2] University of Florida, 601 Gale Lemerand Dr, Gainesville, FL 32611

[3] National Institute of Standards and Technology§

[4] University of Florida, 601 Gale Lemerand Dr, Gainesville, FL 32611

February 20, 2019

Abstract

Electronic systems are ubiquitous today, playing an irreplaceable role in our personal lives as well as in critical infrastructures such as power grid, satellite communication, and public transportation. In the past few decades, the security of software running on these systems has received significant attention. However, hardware has been assumed to be trustworthy and reliable "by default" without really analyzing the vulnerabilities in the electronics supply chain. With the rapid globalization of the semiconductor industry, it has become challenging to ensure the integrity and security of hardware. In this paper, we discuss the integrity concerns associated with a globalized electronics supply chain. More specifically, we divide the supply chain into six distinct entities: IP owner/foundry (OCM), distributor, assembler, integrator, end user, and electronics recycler, and analyze the vulnerabilities and threats associated with each stage. To address the concerns of the supply chain integrity, we propose a blockchain-based certificate authority framework that can be used to manage critical chip information such as electronic chip identification (ECID), chip grade, transaction time, etc. The decentralized nature of the

*dforte@ece.ufl.edu

†tehranipoor@ece.ufl.edu

‡xiaolin8@uic.edu

§apostol.vassilev@nist.gov

proposed framework can mitigate most threats of the electronics supply chain, such as recycling, remarking, cloning, and overproduction[1].

1 Introduction

Driven by the continuous and aggressive scaling of semiconductor fabrication technology, integrated circuits (ICs) have become more complicated than ever. In accordance with Moore's Law [31], the total number of transistors on a single chip has roughly doubled every two years since the 1960s while the costs have gone down at approximately the same rate. Consequently, consumer electronics such as laptops, smart-phones, and even electronic medical instruments are commonly seen and used in everyday life. Moreover, almost all critical infrastructures such as power grid, public transportation systems, and national defense systems are built on numerous electronic devices ranging from high-end digital processors to small controllers, from analog, digital, to mixed-signal sensors or systems. The security, quality, and assurance of these systems are closely related to the trustworthiness of the underlying integrated circuits.

The security of software, firmware, and communication channels has received a lot of attention due to numerous underlying vulnerabilities, threats, and attacks. The security aspect of ICs and electronic systems has been limited to various vulnerabilities and attacks such as side-channel analysis that exploits the hardware implementation of cryptographic algorithms for leaking secret keys, and invasive/semi-invasive attacks enabling tampering and adversarial reverse engineering [42]. However, the supply chain integrity of ICs and electronic systems are equally important, because hardware produced from an untrusted supply chain cannot serve as the underlying root of trust. The globalization of semiconductor industry makes it a *joint effort* to produce an electronic system. Threats arise from various untrusted parties involved in the design, fabrication, development, and distribution of ICs and electronic systems. For example, each component on the system (e.g., digital ICs, analog devices and sensors, printed circuit boards (PCBs), etc.) may come from a group of diverse suppliers who might often be scattered throughout the globe [9, 48]. Therefore, one needs to analyze relevant threats and vulnerabilities at each stage of the life cycle of a component moving through the electronics supply chain. An electronics supply chain that is not secured and trusted opens up opportunities for adversaries to introduce counterfeit ICs and systems, such as recycled, remarked, and cloned, as legit ones to the end users [49]. If the counterfeit devices are not detected and prevented, the user may unknowingly use them to build a system that has potential vulnerabilities. More importantly, although such counterfeit devices (e.g., recycled ICs) may work initially, they may suffer from reduced lifetime,

[1]DISCLAIMER: This paper is not subject to copyright in the United States. Commercial products are identified in order to adequately specify certain procedures. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the identified products are necessarily the best available for the purpose.

pose reliability risks, and impact computers, telecommunications, automotive, or even military systems in which they are deployed. Around 1% of semiconductor products on the market were believed to be counterfeit in 2013, and this number continued to rise [20]. Furthermore, it was predicted that the tools and technologies used for producing such counterfeit ICs/systems would become increasingly sophisticated as well [14].

It is imperative to employ an integrated approach to build a trusted electronics supply chain, ensuring the authenticity of the devices and systems from the device fabrication stage to systems' end-of-life, to thwart the threats and vulnerabilities posed by counterfeit electronics. To this extent, researchers have proposed a number of techniques to detect and avoid counterfeit electronic components [48]. Unfortunately, such individual methods only target to thwart selective threats to some extent and do not offer a holistic solution to create a secure and trusted supply chain. For example, combating die and IC recycling (CDIR) sensor can only detect recycled ICs [53, 52]. Hardware metering [23, 24, 28, 7, 21] and PUFs [46, 37] can only be used to prevent overproduction and cloning. Secure split test (SST) can only be used to prevent overproduction and piracy by locking the correct function of the design during the test [8]. Therefore, none of these techniques can ensure the trust and integrity of the electronics supply chain at system level. Additionally, one of the most important features to build a trusted electronics supply chain - track and trace - is not readily established throughout the supply chain via such techniques. Another critical concern is the management of all necessary information in a trusted and distributed manner so that only the trusted entities can query and verify authentic devices and systems, as they move through a potentially untrusted channel without creating a single point of data-breaching vulnerability.

Infrastructures such as Blockchain [38] can address the data authenticity and confidentiality concerns, and it can be used for virtual financial transactions or commodity transportation. A similar technique can be employed for a trusted supply chain for electronic systems. However, because of the inherently complex nature and vulnerabilities of the electronics supply chain, it is not readily suitable for creating a trusted electronics supply chain among the many involved entities. Noted that several recent papers have also begun to look into the potential of using blockchain for hardware-oriented security, like tracking the IC transactions with PUFs [18], authenticating the IoT devices [13], or protecting the information flow in IoT devices with blockchain and SRAM PUFs [12]. However, they only focus on one of out the several security issues with the electronics supply chain, e.g., tracking every single electronic device before it is utilized in a system. Moreover, the PUF-based solutions also suffer from the reliability and security issues that are inherent to PUFs [10][43], which incurs extra cost for helper data storage and protection. In this paper, we look into the integrity of electronics supply chain from a different angle: an end-to-end framework to provide a comprehensive solution for existing supply chain challenges, rather than focusing only on one problem. Our proposed *blockchain-inspired framework* offers the trust and integrity throughout the electronics supply chain. We make the following contributions:

1. For the first time, we apply the concept of blockchain to protect the electronics supply chain from end to end. A blockchain-based monitoring framework is proposed to mitigate the vulnerabilities throughout the whole electronics supply chain.

2. A blockchain-style tracking system based on certificate authority (CA) nodes is proposed. An interactive communication mechanism between all entities of the electronics supply chain and CA nodes is also presented with details.

3. The tracking mechanism of the blockchain-based framework fully leverages existing hardware identification modules like electronic chip ID (ECID) and chip marking. The proposed framework offers good scalability and can be used together with other existing primitives, such as Physical Unclonable Function (PUF).

4. The resistance of our proposed framework against various supply chain threats (such as overproduction, remaking, recycling, and cloning) is evaluated in detail.

The remainder of this paper is organized as follows. Section 2 reviews some concerns with the trust and integrity of current electronics supply chain. The state-of-the-art mitigation techniques are also briefly introduced. Section 3 presents the threat model of electronics supply chain and discusses the feasibility of employing blockchain to build a trusted electronics supply chain. Section 4 conceptualizes a blockchain-inspired verifiable framework for the electronics supply chain. Section 5 evaluates the performance of the proposed monitoring framework and its resistance against various threats. Section 6 concludes the paper.

2 Background and Related Work

The complexity of the electronics supply chain renders it hard to track the authenticity of each component (e.g., IC, PCB) that goes into an electronic system when it goes through the supply chain. Unless all the entities of electronics supply chain including the distributors are trusted, the authenticity and integrity of the components and the system remain under question. The most common threats arising from the untrusted electronics supply chain are the presence of different types of counterfeit devices and systems, such as:

- Recycled electronic components are collected from used PCBs that are discarded as electronic-waste (E-waste), repackaged and sold in the market as new components. Although such devices and systems might still be functional, there exist performance and life expectancy issues due to silicon aging as well as the chip harvesting process.

- Remarked electronic components are those whose marking on the package (or even on the die) is remarked with forged information. New electronic devices could also be remarked with a higher specification, e.g., from commercial grade to industrial or defense grade.

- Overproduction is usually done by an untrusted foundry, assembly, or a test site that has access to the original design. These parties could potentially produce more than the contracted amount and sell these chips or systems illicitly.

- Defective and out-of-spec components are devices or systems that do not meet the functional or parametric specifications or grades (i.e., commercial, industrial, or military) but are put into the market as authentic ICs or systems.

- Cloning can be performed by any untrusted entity in the electronics supply chain. A clone is a direct copy of the original design produced without the permission of the original component manufacturer (OCM), as the IP owner. Cloning can be done in two ways: by reverse engineering the IC or system obtained from the market or by directly gaining access to the intellectual property used to develop the electronic system (e.g., masks used during IC fabrication) [3].

- Printed circuit boards (PCBs), as the basic component of electronic systems, are also vulnerable to various attacks, such as reverse engineering, overproduction, counterfeit [50], and Trojan insertion [11].

- System integration is the last step of the electronics supply chain towards building a functional electronic product for the end users. Several vulnerabilities may emerge in this step. For example, the system integrator may utilize counterfeit PCB boards or ICs in building the electronic systems.

2.1 Review of the State-of-the-art Mitigation Techniques

Most of the proposed techniques to date for combating counterfeit ICs and electronic systems can be classified into two groups: 1) Counterfeit detection techniques and 2) Counterfeit avoidance techniques.

2.1.1 Counterfeit Detection

Counterfeit detection techniques extract various parameters from suspect ICs to distinguish them from authentic ones. They can be roughly classified into two categories [49]:

- Physical inspection mainly focuses on measuring the physical properties of electronic components. Low-power visual inspection (LVPI) employs low-power microscopes or magnification lamps to examine the leads and packaging of electronic parts. A counterfeit component (e.g., a chip) could

be one with deformed leads or scratches on the package. Other techniques include X-ray imaging, which can be used to find defects on the die or bond wires of ICs, without the need for depackaging. Other detection methods include chemical composition analysis through spectroscopy or imaging using SEM/TEM/FIB [2].

- Electrical measurements refer to techniques that characterize the electrical or functional defects and anomalies of the suspect components. The effectiveness of these methods relies on the changes of electronic parameters since prior usage will either shift the electrical characteristics or degrade the reliability of the devices [36]. Therefore, any testing method that can reveal such changes can be used. Popular methods in this class of detection techniques include parametric test, functional test, and structural test.

2.1.2 Counterfeit Avoidance and Design for Anti-Counterfeit

Most counterfeit detection techniques require known-good or "golden" data to compare against, which is not always readily available. Further, most detection techniques are time-consuming, expensive, and cannot be applied to large batches of ICs or systems (e.g., SEM imaging can only be done on a sampling basis). Therefore, avoidance techniques are required to prevent counterfeit ICs/systems from entering the market in the first place. Popular counterfeit avoidance techniques can be categorized as below:

- Recycling detection sensors have been proposed to measure the lifetime of ICs, as they are used in the field. For example, the combating die and IC recycling (CDIR) sensor, composed of aging-accelerated ring oscillators, allows the measurement of the frequency shift, to decide whether a chip has been previously used. This helps in detecting any potential recycling [53, 52].

- Secure split test (SST) is a method that secures the semiconductor fabrication process from a testing perspective [8]. In this technique, the IP owner can lock the correct function of the design during the test, to prevent an untrusted foundry from engaging in overproduction and piracy.

- Hardware metering enables the design house to lock/unlock the manufactured chips selectively, and this is done by embedding a unique key onto each fabricated chip for identification or locking. Since the design house is in control of how many chips to activate, it can meter or count the number of chips produced by the foundry; this prevents the foundry from fabricating more than the contracted amount of chips (i.e., overproduction) [23, 24, 28].

- Split manufacturing was proposed to protect design intellectual property against untrusted foundry [40]. In this technique, the layout of the design to be fabricated is split into (1) front end of line (FEOL) which consists

of an active layer and several lower metal layers and (2) back end of line (BEOL) which consists of the remaining metal interconnect layers. Since the untrusted foundry only fabricates the FEOL, he/she cannot pirate the overall design that is completed by fabricating the BEOL at a trusted foundry and thus protects against overproduction and cloning.

- IC camouflaging is a countermeasure against reverse engineering of the chip design, once it enters the market [39]. Unlike normal designs, the camouflaged layout is a mix of real and dummy contacts, which makes it much harder for attackers to extract the correct netlist and pirate the design.

- Hardware watermarking allows designers to embed a signature into their designs, which only they can extract to claim authorship. This signature can then be used during litigation if the designer finds that another party pirated their design. Common methods of implementing watermarking include modifying the unused logic of the bitstream file or adding constraints to the original design [21, 6, 26, 22]. Watermarking facilitates the proof of IP ownership, but does not actively protect against counterfeiting.

- Physical unclonable functions (PUFs) enable interactive authentication by converting the static key on devices into an intrinsic function. In particular, such intrinsic functions leverage the microscopic process variations of electronic devices and thus are unique. The input (challenge) and output (response) behavior of PUFs have been proposed for many applications like identification, authentication, key generation and storage [46, 17].

- Package ID-based techniques mitigate counterfeit ICs by adding package IDs onto electronic components. They are lightweight counterfeit avoidance techniques which do not consume extra hardware on the original designs. Some methods that are used to embed the package ID onto the chip/system include DNA marking and nanorods [30, 25].

The resistance against known vulnerabilities of existing counterfeit mitigation techniques is summarized in Table 1. However, none of these methods can adequately address all vulnerabilities. For example, though *SST* can effectively prevent the overproduction and out-of-spec problems (which are marked as *High*), it has limited effectiveness in combating the recycling and remarking of ICs. Keeping these limitations in mind, we propose a blockchain-based framework for the integrity of electronics supply chain, to provide a unified solution against these vulnerabilities. Moreover, to be shown later, the proposed framework can address all the listed supply chain threats leveraging some existing techniques. *Additionally, our solution provides secure and distributed track and trace of electronic components, which is not possible with other techniques.*

Table 1: Threat coverage of existing mitigation techniques [14] and proposed framework.

Mitigation techniques	Overproduction	Recycling	Remarking	Cloning	Out-of-spec/Defective
Physical inspection [2]	NA	Low	Low	NA	NA
Electrical measurement [5]	NA	Medium	Medium	NA	Low
Recycling detection sensor [52]	NA	High	High	NA	NA
Secure split test [8]	High	NA	Low	Medium	High
Hardware metering [28]	Low	NA	Low	Low	NA
Split manufacturing [40]	High	NA	NA	Low	NA
IC camouflaging [39]	NA	NA	NA	Medium	NA
Hardware watermarking [6]	NA	NA	NA	Medium	NA
PUF [46, 17]	Low	Low	NA	Medium	NA
Package ID-based technique [21]	NA	Medium	Medium	NA	NA
Proposed framework	High	High	High	High	High

2.2 Blockchain

Blockchain was first conceptualized by Satoshi Nakamoto in 2008 and then utilized for the digital cryptocurrency: Bitcoin [33]. Blockchain is a distributed database that stores a continuously increasing chain of blocks [45, 32]. Since the most well-known and mature blockchain structure has been developed for Bitcoin, we briefly review the background of blockchain with respect to Bitcoin as a case study in this section.

In the Bitcoin scheme, a blockchain is an ordered, back-linked list of blocks of transactions. In most literature, the blockchain is visualized as a vertical stack, in which all blocks are layered vertically, and the first block serves as the stack foundation, as shown in Fig. 1. In this visualization, one feature associated with each block is its "height", that is used to quantify the distance from it to the first block. Within the blockchain, each block can be identified by its header hash and block height number. The header hash of 32-byte length is generated by hashing the block header twice through the SHA256 cryptographic algorithm. Besides the identifier information, each block also refers to a previous block, which is called the parent block. A block keeps the header hash of its parent in its header to link and backtrack. In this stacked architecture, each block has just one parent in the blockchain.

Blockchain is believed to have great potential to revolutionize the traditional supply chain of various commodities, e.g., from cryptocurrency to food products. This is because:

- In the blockchain scheme, there is no central administrator (node) as shown in Fig. 2(a), where the separated nodes are connected via the central node. In a centralized network, the corruption of the administrator will violate the trust and integrity of the whole network. The nodes of blockchain are connected with each other as shown in Fig. 2(b). There is no administrator and any single node can broadcast to the whole network.

- More specifically, in a Bitcoin database, *the transaction updates broadcasted by any single node will be verified by all other nodes before it is audited*. Therefore, it is ideal to employ such a scheme to ensure the integrity of products in various supply chains [41, 47].

Besides these applications, a critical potential of blockchain is improving the efficiency of globalized supply chains for different businesses. For example, IBM has begun developing blockchain based tracking service in "building systems to record the movement of diamonds from mines to jewelry stores" for Everledger [34]. Walmart has also started testing a blockchain-oriented technology for supply chain management [35].

Depending on the target applications and involved parties, there are three classes of blockchain:

- Public blockchain is open to anyone, and any user can participate in verification of new blocks.
- Private blockchain is only accessible to those who have the permissions to write and read, and such permissions are maintained by an administrative entity within the private blockchain.
- Consortium blockchain is a semi-public blockchain managed by a group of verified users instead of by all of them. This type of blockchain combines the beneficial attributes like efficiency (of private blockchain) and decentralization (of public blockchain).

3 Blockchain for electronics supply chain Integrity

3.1 Integrity Concerns in Electronics Supply Chain

During the past few decades, the business model of the semiconductor industry has drastically changed. Previously, design, fabrication, and testing were usually completed by a single entity. With the increasing costs of fabrication at advanced process nodes, most semiconductor companies have chosen to operate as fabless design houses and outsource manufacturing to external foundries. This model dramatically benefits the whole consumer electronics industry, since new products with more features and functionalities can be released with shorter turnaround times. It is common for fabricated ICs to go through multiple stages of the electronics supply chain depending on the functionality and application of the component. The participants of the electronics supply chain can be roughly classified into the following categories: IP owner/foundry(fab), distributor, PCB assembler, system integrator, end user, and electronics recycler, as shown in Fig. 3.

- IP owner refers to the participants that either design the complete IC, PCB, or system by themselves or source various intellectual property (IP) cores from multiple vendors to produce a complete system-on-chip (SoC).

- Foundry (also called fab) is the fabrication facility that gets the design file (e.g., GDSII format for IC, or Gerber format for PCB) from the IP owner and manufactures electronic ICs or PCBs as per its contract with the IP owner. The foundry may provide packaging services to put the die into the chip package, or it may send the wafer to another packaging facility. This is the step where the electronic design becomes a physical entity (IC or PCB). Also, manufactured ICs and PCBs are tested and sorted for potential hardware faults and given a physical identity (ECID and marking) at this stage.

- PCB assemblers and system integrators (e.g., original equipment manufacturers in the supply chain) refer to the parties who use ICs and PCBs to build board-level or system-level products.

- Distributors include all the possible buyers and sellers of ICs and board-level systems. They act as the transportation channel among the previously described parties. Commonly, there exist one or more distributors between each of the stages (foundry, PCB assemblers, and system integrators) to facilitate the supply of components among various design parties.

- Electronics recyclers are the participants responsible for handling E-waste (the discarded end-of-life entity of the electronic components and systems). Such E-waste consists of devices that have reached the end-of-life, i.e., destroyed or not operating anymore, as well as working devices and systems that have been discarded at end users' will.

3.2 Threat Model

Counterfeit electronic components are one of the leading threats to the integrity of the electronics supply chain. As one can assume, the existing global electronics supply chain can only be trusted if all participants are trusted. In such a scenario, all entities, such as IP owners, foundries, PCB assemblers, system integrators, distributors, and end users would be able to verify the authenticity of an electronic component throughout its lifetime. However, such an ideal scenario is far-fetched for ensuring the integrity of the electronics supply chain. Instead, we focus on developing a trusted electronics supply chain using a blockchain-based framework to mitigate the existing vulnerabilities. At a high level, we assume that the five main entities (including IP owner, PCB assembler, system integrator, end user, and electronics recycler) can enroll the associated information of a device/component/system into a secure and trusted database. On the other hand, an entity can inquire the authenticity verification of a component or system without gaining secret information. Any component that is not verified through this framework falls outside of this trusted electronics supply chain, and hence should be considered as untrusted.

From Fig. 3, we see that counterfeit electronic chips and systems can be introduced at different stages in the electronics supply chain, either by untrusted

distributors or the main participants like foundry, PCB assembler, and system integrator. The adversarial role played by each of them is described as follows:

- Distributors widely exist throughout the electronics supply chain and are responsible for mediating the purchasing and selling of components (e.g., between foundries and PCB integrators, PCB integrators and system integrators). They can feed counterfeit components to other entities. For example, distributors may choose to supply recycled or remarked products (collected from the sources located outside of this trusted electronics supply chain) for higher profit.
- Additionally, a PCB assembler (or system integrator) can possibly use recycled components on the PCB (or system); therefore, counterfeit parts are also possibly introduced by them.
- In our proposed framework, we do not claim the foundry is trusted. Instead, we make the observation that: either the fab needs other participants to inject the cloned or overproduced chips into the electronics supply chain, or the fab chooses to introduce the overproduced components directly into the supply chain by itself.

3.3 Blockchain-based Electronics Supply Chain

In this work, we propose to employ a blockchain-based electronics supply chain. Though blockchain has been successfully employed to enhance the supply chain integrity of various commodities, it is not straightforward to apply it as-is to the electronics supply chain. Compared to other industries, the semiconductor industry has some unique characteristics. For example, the food supply chain can be monitored by tracking the temperature variations and the time taken for the transit of food commodities [35]. It is impractical to evaluate the integrity of electronic products only by the shipping time. Moreover, it is also difficult to authenticate electronics from their packaging appearance alone. An example is shown in Fig. 4, in which an authentic differential line transceiver chip (left) from *Analog Devices* and a counterfeited copy (right) are shown. It is obviously difficult to differentiate between genuine chips and counterfeit ones, just by looking at their exterior package. When threats such as recycled or remarked ICs are considered, the problem becomes even worse.

The merit of the blockchain-powered electronics supply chain is that it enables all participants to track, verify, and then choose to deny or accept any single transaction, i.e., an electronic component or system. Correspondingly, the integrity of electronic devices can be guaranteed if they can be tracked throughout the supply chain. To realize such tracking, it is necessary to assign a unique ID for each electronic component. Fortunately, there already exists a unique electronic chip ID (ECID) and/or marking embedded in/on many modern chips that can be used as identifiers [14]. The ECID is a well-established technique following the IEEE standard 1149.1, to facilitate the adaptive testing

and tracking of ICs. It is commonly utilized in many consumer electronic products, such as iPhone [44]. When carrying an ECID, the chip can be identified and tracked throughout its lifetime. For example, if a chip has been denoted as "E-waste" in the blockchain-based framework, any device found with the same ID should be classified as counterfeit since it is very likely recycled, remarked, overproduced, or cloned.

To build an authentication infrastructure via blockchain, a database accessible to all the registered participants of the proposed trusted supply chain should be maintained to record the ECIDs of ICs. However, in practice, design houses may prefer to keep a record of its electronic products private. Therefore, it is difficult for a user to check the authenticity of a set of chips if they are not directly bought from these companies. Another limitation is that for an assembler which uses a large number of different chips, it is inconvenient to validate the authenticity of all chips from various companies. These limitations imply that before applying blockchain to track electronic devices, a proper ID database and accessing scheme should be designed first.

3.4 Advantages of Blockchain-enabled Framework

3.4.1 Security:

Compared with the scenario that the IDs of hardware components are maintained by each vendor, a blockchain-enabled framework provides more security advantages. For example, when the chip IDs are being stored in a centralized manner, they are vulnerable to being modified by malicious insiders without being noticed. In a blockchain-based framework, all such tracking information is stored in a distributed manner, and different stages of the electronics supply chain are linked by the time stamp. This can prevent such vulnerabilities by providing tamper-resistance and evidence.

3.4.2 Convenience:

As the modern electronic systems become more complicated, it becomes infeasible for a downstream participant to authenticate the chips with all upstream vendors. A trusted third-party like blockchain provides such convenience that all participants of the electronics supply chain can verify the authenticity of hardware devices.

3.5 Notation and Terminology

Here, we list some notations and terminologies often used in this article for readers' clarity:

- **Certificate Authority (CA) Network** serves as the consortium blockchain (i.e., the trusted third party entity) that maintains the electronic chip identification (ECID) information of electronic components in the supply

chain. The CA network is responsible for providing the enrollment and verification service to different entities in the electronics supply chain.

- **CA node** is the primary component of the CA network. Each CA node of the CA network maintains a database that stores the information regarding each chip in the electronic system (e.g., marking, ID, and transaction time, etc.).
- **Marking** provides the device identification and manufacturing traceability information on the package of electronic components. It is usually composed of several codes denoting wafer fab and assembly plant, date of manufacture, wafer lot, device family, and packaging information, etc. [19].
- **ID** denotes the embedded identification of an electronic component. It can be the electronic chip ID (ECID) of an integrated circuit in this work. The ECID of a chip includes the fabrication and test information, for example, the die location, wafer number, binning information for temperature, speed grade and any other information deemed appropriate for traceability.
- **PCB ID (PID)** stands for the unique identification of the PCB board with chips on it. In our proposed framework, this ID is derived from the IDs of the chips on the PCB, as shown in Fig. 9 (described in detail in Section 4.4.1).
- **System ID (SID)** is the ID of the electronic system which is composed of various chips, PCB boards, and operating system (described in detail in Section 4.4.2).
- **Transaction Time** is a record of the time when the CA network receives the enrollment or verification request for a certain ID.
- **Stage** denotes the instant of the electronic life-cycle when verification is requested. The CA network can identify the requester as an entity such as PCB assembler or system integrator, etc. For example, an electronic part is with stage "End User" as shown in Fig. 5 means that it has been sold and is with the end user. Therefore, any new verification request for the ID (chip-, PCB- and system-level) related to this product corresponds to counterfeit.

3.6 Assumptions

In this paper, we make the following assumptions:

- The proposed framework creates a trusted electronics supply chain only for the entities that are part of the blockchain-enabled electronics supply chain, like IP owner/Fab, PCB assembler, system integrator, and end user. This allows us to create a peer-to-peer connection among the entities.

- The electronic components, PCBs, and systems can contain and generate necessary identification information. For components that do not have ECID information such as analog ICs, package markings can be used by the proposed framework.
- The communication between any two Certificate Authority (CA) nodes is secure and is maintained by the CA network. Details of CA network and CA nodes are discussed in Section 4. This can be ensured by using the appropriate mode of secure communication. Details of such an infrastructure are beyond the scope of this paper.
- The confidentiality and integrity of communication for all messages in the framework are guaranteed.
- The main entities like IP owner, PCB assembler, system integrator, and end user have permission to enroll the information of their products to the CA network, and this enrollment is secure.
- All entities have permission to verify the information of electronic components from their upstream entities (by using the CA network), and this verification is secure.
- All distributors (of chip-, PCB- and system-level) and end users can verify components or systems with the CA network but have no authority to do the enrollment.

4 Blockchain-Enabled electronics supply chain Integrity Framework

4.1 Consortium Ledger: the Certificate Authority Network

Unlike the public ledger of Bitcoin that can be accessed by anyone, it is undesirable to make the ID database of electronics supply chain fully public, as doing so may leak trade secrets (e.g., yield information) of semiconductor companies. In practice, the entities who care about the authenticity of electronic chips include:

1. Original component manufacturer (OCM) (e.g., IP owner) who wants to prevent all possible vulnerabilities of electronics supply chain and ensure the economic benefits of their design/products.
2. Original equipment manufacturer (OEM) (e.g., PCB assemblers and system integrators) that do not design but choose to buy chips from the IP owners and distributors, and would like to build their products with genuine chips.

3. End users who want to ensure that the electronic products they bought are composed of authentic electronic components, and that the product is trusted.

Adhering to the "decentralized" feature of the blockchain, we build a consortium blockchain: a networked monitoring system that is composed of several distributed certificate authority (CA) nodes, as shown in Fig. 5. This proposed CA network is decentralized in the sense that: 1) every pair of CA nodes are connected and can exchange information with each other, 2) all nodes keep a database for chip ID enrollment and verification, 3) all CA nodes need to reach consensus before adding a block, as denoted by the "mutual verification" operation in the following sections.

4.2 Proposed Framework

The proposed blockchain-enabled framework is as shown in Fig. 6, where in addition to the normal stages like PCB assembly, system integration, four more steps are included namely enrollment, ownership release, verification, and ownership acquire to enhance the integrity of supply chain. These four steps stand for the interactive communication between various entities and the CA network. The meaning of each step is described below:

4.2.1 Enrollment

In the proposed framework, enrollment denotes that entities of the electronics supply chain enroll the information of their products into the database of CA network. Specifically, OCM (e.g., IP owner) enrolls the information (e.g., ECID, marking, grade and the intrinsic ID generated by PUF) of all chips they build, which generates the first block for each hardware device in the CA database. The CA network will store the enrolled chip information among all CA nodes, and issue an "enrollment certificate" to the supply chain entity.

4.2.2 Ownership release

When OCM finishes information enrollment, the next step is selling their products. In this process, the OCM will first request the ownership release to CA network with corresponding chip information and the "enrollment certificate". All CA nodes will *mutually* verify this information and "enrollment certificate". If authentic, they will issue the "ownership release" certificate (token) to the entity. To finish the transaction while facilitating the verification of PCB assembler (or next-stage distributor), the OCM will sell the chips with the CA-issued "ownership release" token.

4.2.3 Verification

In this step, the PCB assembler will first conduct the semi-verification of the electronics with CA network, by sending the public information (e.g., marking),

and the CA-issued token of chips to the CA nodes. The CA network will perform a quick search for this information in its database. If found and matched, the CA network will then do a "full-verification" with the intrinsic IDs (e.g., challenge and response pairs (CRPs) of PUF) of the chips, which cannot be modified by the PCB assembler.

4.2.4 Ownership acquire

When the CA network confirms the validity of the intrinsic IDs, the "full-verification" will pass. The PCB assembler can then send an "ownership acquire" request to the CA network. The CA network will issue an "ownership certificate" to the PCB assembler, and change the stage information of the electronic products in its database to "PCB Assembly".

4.3 IP Owner and Foundry (OCM)

As the starting point of electronics supply chain where an integrated circuit originates, the IP owner suffers the most economic loss from counterfeited chips. Therefore, in the proposed scheme, IP owner is assumed trusted and in charge of enrolling the information of their chips. The information enrolled by the IP owners include marking, chip ID, grade (military or commercial), and CRPs of PUFs etc. The enrollment flow is as shown in Fig. 7.

1. **ID enrollment request:** The IP owner or Fab (OCM) sends ID enrollment request to CA network.

2. **Mutual verification:** Each CA node will broadcast the received request to all other CA nodes for mutual verification, if yes, then go to (3); otherwise, the enrollment request is marked as failed. Note that the OCM can still send enrollment requests, but such requests will only be accepted if they satisfy "mutual verification".

3. **Ready to receive:** The transaction time of the chip information will be updated in the CA database, and a "Ready to receive" decision will be sent to the IP owner (or fab).

4. **Enroll chip information:** The IP owner (or fab) sends the information of chips to CA network (all CA nodes), including marking, ECID, grade and CRPs;

5. **Mutual verification:** Each CA node will broadcast the information it receives to other CA nodes for mutual verification, e.g., whether they also get the verification request for the same IDs.

6. **Enrollment result:** If all CA nodes *mutually* confirm the ID enrollment by OCM, then the enrolled information will be stored in the database, as shown in the table in Fig. 7. CA network sends a decision to the IP owner (or fab) about the enrollment. If the enrollment succeeds, the CA network

issues an "enrollment complete certificate" to the OCM. The enrollment fails if the enrolled IDs are found pre-existing in the CA database.

7. **Ownership release request:** When the OCM finishes the enrollment, it will consider releasing the ownership of the chips. To complete this step, the OCM will send an ownership release request to the CA network, with the chip information and "enrollment complete certificate". The CA network will do a quick search in its database, if the information matches, it will issue an "ownership release" certificate (step (8)) to the OCM.

An example of the enrolled chip information is shown in the table of Fig. 7, where the marking, ECID, grade and intrinsic ID of the chip have been enrolled. Since this chip is newly enrolled into the database, no corresponding PID (*null*) and SID (*null*) will be found. The transaction time ("Trans. time") records the time when this electronic component is enrolled in the CA database. Since this is a newly enrolled chip, the stage record is labeled as "IP owner/Fab". Note that the IC enrollment fails if any of the above-mentioned steps do. For example, if the ID enrollment request is not "mutually conducted/sent" by/to all CA nodes, or if the chip IDs already exist in the CA database, the enrollment will fail.

4.4 Assembly Stage

In this section, we use "assembly stage" to generally denote two stages: PCB assembly and system integration as shown in Fig. 3.

4.4.1 PCB Assembly

The first step of building electronic systems is assembling various electronic chips onto a PCB. In this step, PCB assemblers buy chips from the OCM (or distributors). These chips are then mounted onto PCBs. Note that after the chips are mounted onto PCBs, the embedded chip ID like ECID can be read out by the PCB assemblers (e.g., through JTAG) and verified with the CA nodes. For example, after getting the ECID information, the PCB assembler can send a verification request to the CA network and get the feedback. The objective of such verification is to detect counterfeit electronic components introduced into electronics supply chain during the distribution stage. We propose a verification procedure as shown in Fig. 8. The detailed operation of each step is provided below:

1. **Verification request:** The PCB assembler sends ID verification request to CA network.

2. **Mutual verification:** Each CA node will broadcast the ID verification request he received to all other CA nodes and get their feedback (e.g., whether they also get the verification request from the same PCB assembler).

3. **Ready to respond:** All CA nodes check with each other to ensure that all nodes receive the same request, if yes, then go to (4); otherwise, the verification request is marked as failed.

4. **Send public information of chips:** To complete the semi-verification, the PCB assembler sends the public information (e.g., marking, grade, etc) of chips to CA network for verification. Note that not all these chips will be necessarily used in building electronic products.

5. **Mutual verification:** Each CA node will broadcast the information he received to all other CA nodes and get their feedback (e.g., whether they also get the verification request for the same IDs). If yes, then go to (6); otherwise, the verification request is marked as failed.

6. **Authentic/Counterfeit:** After all CA nodes *mutually* authenticate the information from PCB assembler, the transaction time will be updated, and the stage of these chips will be labeled as "PCB Assembly" if the verification succeeds. The authentication fails if the requested IDs are either not found in the database or found as being used in other PCB boards. The verification results will then be sent to the PCB assembler.

7. **Full verification based on CRPs:** If the semi-verification confirms that the chips are authentic, then the CA network will do a full-verification based on the CRPs of PUFs. Note that in our framework, we assume this step can be done automatically, i.e., the PCB assembler has no access or permission to control or change the challenges and responses of PUFs.

8. **Verification result:** The CA network will send the full-verification result to PCB assembler.

9. **Ownership acquire request:** After fully verifying the authenticity of the chips, the PCB assembler can then request the ownership, by sending an "ownership acquire" request to the CA network.

10. **Ownership release information:** The CA network will issue the ownership release information to PCB assembler.

11. **PID generation:** If the chips are genuine, then the PCB assembler will assemble them in PCB boards, a PCB ID (PID) will be generated based on the rule proposed in Fig. 9.

12. **PID enrollment request:** The PCB assembler sends PID enrollment request to CA network.

13. **Mutual verification:** Each CA node will broadcast the PID enrollment request he received to all other CA nodes and get their feedback (e.g., whether they also get the verification request from the same PCB assembler).

14. **Ready to receive:** After all CA nodes *mutually* authenticate this enrollment request, if yes, the CA network sends a "Ready to receive" response to PCB assembler. Otherwise, the verification request is marked as failed.

15. **PID enrollment:** The PCB assembler sends the generated PID and its composition (e.g., the chip IDs that are used to generate this PID) to CA network.

16. **Mutual verification:** Each CA node will broadcast the received information to all other CA nodes and get their feedback (e.g., whether they also get the verification request for the same IDs). The CA network will also verify the owner of these chips, only if the PCB assembler is the current owner of these chips, the PID enrollment is allowed. After all CA nodes *mutually* authenticate this information, they will update the PID in the database, as shown in Fig. 8.

17. **PID enrollment result:** The transaction time and the stage of this chip will be updated, then the CA network sends a decision to the PCB assembler about the success (or fail) for the enrollment.

Note that the verification fails if any of the above-mentioned steps fails. For example, the verification is not "mutually conducted/sent" by/to all CA nodes, or the IDs under verification do not exist in the CA database.

Building a PID is advantageous for the tracking and management of electronic components in electronics supply chain for two reasons: 1) When several electronic components are assembled, the labels ("stage = PCB Assembly" in Fig. 8) will mark them as in use. 2) When the used parts move forward in the electronics supply chain, a board ID can help managing these parts together, i.e., for verification and deactivation purpose once the system reaches its end-of-life.

As shown in Fig. 9, one possible method to build a PID is by organizing the ECID of chips in a "Merkle tree" structure, i.e., each leaf node of the hash tree is filled with a chip ID and the PID is the root of this tree [29]. In this PID generation algorithm, SHA-256 protocol is employed as the hash function. The advantage of using this data structure is that each chip ID (leaf node) can be tracked by computing a number of hash calculations, which is linearly proportional to the logarithm of the number of leaf nodes of the tree. Compared with linear search, this technique greatly decreases the workload for CA network. Once the PCB ID is generated, the "PID enrollment" procedure can be done similarly as that between the IP owner/Fab and CA network. The difference is that for each enrolled PID, the PCB assembler also sends the chip IDs to the CA nodes, and CA nodes will update their database correspondingly to build the relationship between the chip IDs and PCB IDs.

4.4.2 System Integration

An example of system integration is as shown in Fig. 3, where a computer is composed of several PCB boards as sub-components. To facilitate the database

management for CA nodes and tracking of all components in the electronics supply chain, we again propose to build an ID, namely system ID (SID) for each electronic system. Like PID, the SID can be a hashed result of the PCB IDs in this system. The verification and SID enrollment between system integrator and CA network is similar to that of the PCB assembler. Note that the verification and enrollment request from the system integrator changes the stored information in CA network. For example, the SID will be generated and more "transaction time" will be recorded, and the "stage" will be updated as "System Integration", as shown in Fig. 10.

4.5 End User

When the system integration finishes, the electronic products will be sold to end users (or distributors). Similarly, the end users would like to verify the authenticity of the products with CA network. As shown in Fig. 11, the user can first send verification request to the CA nodes and provide some public information of the products. Then the CA network can make a quick search in the database, and do the full-verification by checking the authenticity of all electronic components in the product. If the verification result is authentic, the CA network marks the stage of the product as user. The user can then send an ownership acquire request to the CA network after confirming the authenticity of the product.

4.6 Distribution Stage

In this work, we use the term "distribution stage" to denote the distribution of components at each stage of the supply chain. As shown in Fig. 3, electronic components that have been sold at one stage may be bought or sold again among different chip distributors. The PCB distributors connect PCB assembler and system integrators. The system distributor sells electronic products to end users. Since we assume that the distributors are untrusted, they do not have authority to enroll any information into the CA network but can send verification requests, if they want to check the authenticity of the products they acquired. One advantage of this regulation is that the "stage" information of electronic components cannot be changed by these distributors. This prevents remarked or recycled chips from re-entering the supply chain.

4.7 Electronic Waste

In this work, E-waste stands for the final stage of electronics supply chain, which is the source of many counterfeit components like recycled chips. In our proposed framework, the electronic recyclers are responsible for collecting and updating electronic components with the "end-of-life" status to CA network, thus preventing them from re-entering the supply chain by marking the stage in the database as "E-waste".

5 Evaluation of the Proposed Method

As stated earlier in this paper, there are several known vulnerabilities in the traditional electronics supply chain: overproduction, recycling, remarking, cloning, etc. In this section, we discuss how each vulnerability can be mitigated with our proposed framework for the integrity of electronics supply chain.

5.1 Compatibility for Validation and Maintenance

In the practical electronics supply chain, validation and maintenance are necessary steps to guarantee the quality of electronic products. Therefore, the proposed framework should be compatible with these operations, i.e., the ID generation and enrollment should not be impacted. In this paper, we use validation to denote the functionality and performance evaluation by the PCB assembler or system integrator. In this procedure, some of the chips (or PCB boards) owned by PCB assembler (or system integrator) may be discarded during validation, due to deficiency or performance inefficiency. The proposed framework is compatible with this practical concern, as shown in Fig. 12, in which PCB assembly is used as an example (note that the similar rule applies for the system integration).

Maintenance is another practical operation that mostly happens with the end users, for example, a user may want to upgrade (or replace) some components of his computer for better performance. According to the proposed rules for SID generation in Section 4.4.2, this may impact the integrity of the SID that is stored in the CA database. To allow such in-field maintenance and the enrollment of new SID, we propose two rules: (1) when the CA network receives a new SID enrollment request from user, it will first verify the ownership of this SID (i.e., the system), to confirm that the user sending request is the same owner as stored in the CA database; (2) the enrollment is only allowed if (1) is satisfied, and the IDs (ECID or PID) of most sub-components are not changed.

5.2 Resistance Against Recycling

Following our proposed framework, the recycled chips, boards, or system would contain IDs that have been enrolled by the IP owner, PCB assembler, and system integrators, respectively. Therefore, they can be prevented from re-entering the electronics supply chain again by verifying with the CA network. An example of recycling detection is as shown in Fig. 13, where a recycled chip with an already enrolled ID can be detected by the system integrator since it has an existing ID with the "stage" information as system integration.

5.3 Resistance Against Overproduction

In the conventional threat model of electronics supply chain, the foundry is usually untrusted due to threats such as overproduction. In our proposed framework, even if the foundry can manufacture more chips than contracted, they are

not allowed to put them into the blockchain-enabled electronics supply chain. As shown in Fig. 14, if the overproduced chips enter the electronics supply chain, they will be detected since the ID information is not enrolled and stored in the CA database. In the worst case, the overproduced chips will have the same IDs as that of the genuine chips, and such chips can also be detected by verifying the "stage" information.

5.4 Resistance Against Remarking

In our proposed monitoring framework, all important information about an electronic component is recorded. Therefore, the verification information from the CA network would detect the discrepancies for a remarked chip. An example of the remarking detection is as shown in Fig. 15, where the marking changes from commercial to defense grade can be detected by the CA network.

5.5 Resistance Against Cloning

During the fabrication process, cloned chips can be manufactured in an unauthorized fab through reverse engineering or IP theft. In this scenario, these cloned chips will have the *same* functionalities and electronic IDs and cannot be effectively detected by our proposed framework. To mitigate this potential vulnerability, we propose to employ PUF in the verification and authentication with CA network. As PUF is built on manufacturing process variations, the input and output (CRPs: challenges and responses) behavior of a cloned chip will not be the same as that of the genuine chip.

Due to the large number of CRPs of strong PUFs, it is difficult for the IP owner to maintain a database for all PUFs of their products. Moreover, due to the reliability issue of PUFs, the verification may fail if the PUF circuit is being measured in a different environmental condition. To solve these problems, we propose that the IP owner pre-store a model for each PUF instance in their database, with which they can predict the responses for any given challenges even without the presence of PUF circuitry [51]. Using a PUF model instead of storing CRPs has many benefits: 1) This makes it possible to conduct as many verifications as possible. For example, multiple CRPs can be reproduced from the PUF model used for one authentication if PUF noise/reliability of one CRP is an issue. 2) It is not necessary to store an exponentially large number of CRPs for each PUF. Note that in this scenario, machine learning attacks are not a threat because the cloned hardware needs to produce the same responses, which are nontrivial.

The new verification procedure including "CLONE-checking" option is as proposed in Algorithm 1: when an end user resorts to the CA nodes for chip authentication, the CA nodes will first communicate with each other to verify whether this request has been received by all of them, as in line 3. Per a mutually received verification request, all the CA nodes will search the registered ID in their database (line 4). An ID found in the CA database will be sent back to the consumer (6) and an option for "CLONE-checking" will be available to the

end user (line 7). In the "CLONE-checking", the CA network is responsible for connecting the IP owner and end user and transferring the input and output behaviors of the embedded PUF instances (line 9-11). A cloned chip will be detected and reported if its ID is found in the CA database, but the PUF behavior does not match with that of the IP owner's record, as shown in line 16. Otherwise, the chip will be confirmed as authentic (line 13-14).

ALGORITHM 1: An example of verification procedure against cloning.

Require: Whether a chip for verification is cloned or not.
Ensure: YES or NO from the CA network.

1: The end user reads out the chip ID and send it to the verifier: CA network.
2: The CA nodes check with each to ensure that all nodes are mutually receiving the same verification request.
3: **if** (Mutual-Verification == YES) **then**
4: CA nodes search for the end user provided ID in their database
5: **if** (ID-Found == YES) **then**
6: CA nodes verify other entries of the requested chip: grade, package, etc.
7: Send "CLONE-checking" option to the end user
8: **if** (CLONE-checking option chosen by end user) **then**
9: Get challenges from the IP owner
10: Send challenges to end user and collect responses R_{user}
11: Send the responses to IP owner (who keeps the golden responses R_{golden}) for verification
12: **if** (HD(R_{user}, R_{golden}) $\leq R_{thres}$) **then**
13: Send the verification result to the end user: *the chip is not cloned.* (R_{thres} stands for the upper bound of acceptable Hamming Distance (HD) between collected responses R_{user} and golden responses R_{golden})
14: Update the "Trans. time" of this ID
15: **else**
16: Send the verification result to consumer: *This chip is possibly a cloned one.*
17: **end if**
18: **else**
19: Send verification result to end user: *This ID is found in the database with the grade information.*
20: **end if**
21: **else**
22: Illegal request, send warning to the end user: *Should verify with all CA nodes.*
23: Authenticate the identity of the end user
24: **end if**
25: **end if**

5.6 Other Possible Vulnerabilities

Besides the aforementioned vulnerabilities, there may also exist other potential vulnerabilities in the electronics supply chain. For example, one PCB assembler

may solder a set of chips onto PCBs, but desolders and resells them after a short period of testing. These chips are not recycled or remarked. Such a short-time usage or testing cannot be detected by our proposed monitoring framework. To mitigate these potential vulnerabilities, we propose that counterfeit detection sensors be combined into the IC design to aid counterfeit mitigation, as shown in Fig. 7. Correspondingly, the measurements of these sensors can also be enrolled into our proposed CA database for verification purpose. For example, the enrolled measurements of CDIR sensor, Flash memory, SRAM memory and path delay of look-up-table on FPGAs can be used to detect recycled ICs [52], Flash memory [16], and SoCs [15], respectively.

Moreover, the flexibility of our proposed framework makes it feasible to combine any new counterfeit avoidance techniques in the future. As an example, the products of electronics Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program launched by Defense Advanced Research Projects Agency (DARPA) can also be used together with our framework [4]. The main purpose of SHIELD program is to eliminate counterfeit ICs from the electronics supply chain, by adding a "hardware dielet" called "root of trust". The measurements of a "dielet" can also be enrolled into our proposed framework.

6 Conclusion and Future Work

In this paper, we propose a blockchain-based framework to monitor the integrity of electronics supply chain. We also analyze the role of all entities in the proposed trusted electronics supply chain. The resistance of our proposed framework against some common vulnerabilities within electronics supply chain is analyzed with details. The proposed CA framework can effectively mitigate vulnerabilities such as recycling, remarking, overproduction and cloning. However, the framework still has some limitations that need to be addressed. For example, overproduced chips can circumvent the monitoring of the proposed framework, when these chips are sold to entities outside the blockchain enabled supply chain. Mitigation of these vulnerabilities are currently beyond the reach of our proposed framework but can be realized with some previously proposed countermeasures. Another limitation of the proposed framework is that all CA nodes store the same copy of tracking information of electronic products. This scheme achieves the decentralization feature of blockchain but also makes it expensive to manage the database. Future work includes developing communication protocols between different entities and CA network and exploring efficient data management and searching techniques.

References

[1] A. M. Antonopoulos. *Mastering Bitcoin: unlocking digital cryptocurrencies.* " O'Reilly Media, Inc.", 2014.

[2] N. Asadizanjani, M. Tehranipoor, and D. Forte. Counterfeit electronics detection using image processing and machine learning. *Journal of Physics: Conference Series*, 787(1):012023, 2017.

[3] N. Asadizanjani, M. Tehranipoor, and D. Forte. Pcb reverse engineering using nondestructive x-ray tomography and advanced image processing. *IEEE Transactions on Components, Packaging and Manufacturing Technology*, 7(2):292–299, 2017.

[4] K. Bernstein. Supply chain hardware integrity for electronics defense (shield), 2014.

[5] M. Bushnell and V. Agrawal. *Essentials of electronic testing for digital, memory and mixed-signal VLSI circuits*, volume 17. Springer Science & Business Media, 2004.

[6] E. Castillo, U. Meyer-Baese, A. García, L. Parrilla, and A. Lloris. Ipp@ hdl: efficient intellectual property protection scheme for ip cores. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 15(5):578–591, 2007.

[7] E. Charbon. Hierarchical watermarking in ic design. In *Custom Integrated Circuits Conference, 1998. Proceedings of the IEEE 1998*, pages 295–298. IEEE, 1998.

[8] G. K. Contreras, M. T. Rahman, and M. Tehranipoor. Secure split-test for preventing ic piracy by untrusted foundry and assembly. In *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2013 IEEE International Symposium on*, pages 196–203. IEEE, 2013.

[9] Defense Science Board. *Defense science board task force on high performance microchip supply*. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2005.

[10] J. Delvaux and I. Verbauwhede. Key-recovery attacks on various RO PUF constructions via helper data manipulation. In *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*, pages 1–6. European Design and Automation Association, 2014.

[11] S. Ghosh, A. Basak, and S. Bhunia. How secure are printed circuit boards against trojan attacks? *IEEE Design & Test*, 32(2):7–16, 2015.

[12] Guardtime and I. ID. Internet of things authentication: A blockchain solution using sram physical unclonable functions, 2017.

[13] U. Guin, P. Cui, and A. Skjellum. Ensuring proof-of-authenticity of iot edge devices using blockchain technology. In *2018 IEEE International Conference on Blockchain*, 2018.

[14] U. Guin, D. DiMase, and M. Tehranipoor. Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. *Journal of Electronic Testing*, 30(1):9–23, 2014.

[15] Z. Guo, M. T. Rahman, M. M. Tehranipoor, and D. Forte. A zero-cost approach to detect recycled soc chips using embedded sram. In *Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium on*, pages 191–196. IEEE, 2016.

[16] Z. Guo, X. Xu, M. Tehranipoor, and D. Forte. Ffd: A framework for fake flash detection. In *Proceedings of the 54nd Annual Design Automation Conference*. ACM, 2017.

[17] D. Holcomb, W. Burleson, and K. Fu. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. *Proceedings of the Conference on RFID Security*, 2007.

[18] M. N. Islam, V. C. Patii, and S. Kundu. On ic traceability via blockchain. In *VLSI Design, Automation and Test (VLSI-DAT), 2018 International Symposium on*, pages 1–4. IEEE, 2018.

[19] H. James and T. Cles. Standard linear & logic semiconductor marking guidelines, 2002. http://www.ti.com/lit/an/szza020c/szza020c.pdf.

[20] N. Kae-Nune and S. Pesseguier. Qualification and testing process to implement anti-counterfeiting technologies into ic packages. In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013*, pages 1131–1136. IEEE, 2013.

[21] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe. Constraint-based watermarking techniques for design ip protection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 20(10):1236–1252, 2001.

[22] D. Kirovski, Y.-Y. Hwang, M. Potkonjak, and J. Cong. Protecting combinational logic synthesis solutions. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 25(12):2687–2696, 2006.

[23] F. Koushanfar and G. Qu. Hardware metering. In *Proceedings of the 38th annual design automation conference*, pages 490–493. ACM, 2001.

[24] F. Koushanfar, G. Qu, and M. Potkonjak. Intellectual property metering. In *Information Hiding*, pages 81–95. Springer, 2001.

[25] C. Kuemin, L. Nowack, L. Bozano, N. D. Spencer, and H. Wolf. Oriented assembly of gold nanorods on the single-particle level. *Advanced Functional Materials*, 22(4):702–708, 2012.

[26] J. Lach, W. H. Mangione-Smith, and M. Potkonjak. Fingerprinting techniques for field-programmable gate array intellectual property protection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 20(10):1253–1261, 2001.

[27] Learn to Know the Difference with AS5553. Learn to know the difference with as5553, 2009. https://escs9120.wordpress.com/.

[28] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas. A technique to build a secret key in integrated circuits for identification and authentication applications. In *VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on*, pages 176–179. IEEE, 2004.

[29] R. C. Merkle. Method of providing digital signatures, Jan. 5 1982. US Patent 4,309,569.

[30] M. Miller, J. Meraglia, and J. Hayward. Traceability in the age of globalization: a proposal for a marking protocol to assure authenticity of electronic parts. Technical report, SAE Technical Paper, 2012.

[31] G. E. Moore et al. Cramming more components onto integrated circuits. *Proceedings of the IEEE*, 86(1):82–85, 1998.

[32] D. Z. Morris. Leaderless, blockchain-based venture capital fund raises $100 million, and counting. *Fortune (magazine)*, pages 05–23, 2016.

[33] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[34] K. S. Nash. *"IBM Pushes Blockchain into the Supply Chain"*. Wall Street Journal, 2016.

[35] K. S. Nash. *"Wal-Mart Readies Blockchain Pilot for Tracking U.S Produce, China Pork"*. Wall Street Journal, 2016.

[36] G. F. Nelson and W. F. Boggs. Parametric tests meet challenge of high-density ics. *Electronics*, 48(25):108–111, 1975.

[37] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026–2030, 2002.

[38] M. Pilkington. Blockchain technology: principles and applications. *Browser Download This Paper*, 2015.

[39] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri. Security analysis of integrated circuit camouflaging. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 709–720. ACM, 2013.

[40] J. J. Rajendran, O. Sinanoglu, and R. Karri. Is split manufacturing secure? In *Proceedings of the Conference on Design, Automation and Test in Europe*, pages 1259–1264. EDA Consortium, 2013.

[41] S. Raval. *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology.* " O'Reilly Media, Inc.", 2016.

[42] J. A. Roy, F. Koushanfar, and I. L. Markov. Ending piracy of integrated circuits. *Computer*, 43(10):30–38, 2010.

[43] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas. Puf modeling attacks on simulated and silicon data. *Information Forensics and Security, IEEE Transactions on*, 2013.

[44] Sauriks. Ecid –the iphone wiki. *https://www.theiphonewiki.com/wiki/ECID*, 2009.

[45] E. Staff. Blockchains: The great chain of being sure about things. *The Economist. Retrieved*, 18, 2016.

[46] G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th annual design automation conference*, pages 9–14. ACM, 2007.

[47] D. Tapscott and A. Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* Penguin, 2016.

[48] M. Tehranipoor and C. Wang. *Introduction to hardware security and trust.* Springer Science & Business Media, 2011.

[49] M. M. Tehranipoor, U. Guin, and D. Forte. Counterfeit integrated circuits. In *Counterfeit Integrated Circuits*, pages 15–36. Springer, 2015.

[50] L. Wei, C. Song, Y. Liu, J. Zhang, F. Yuan, and Q. Xu. Boardpuf: Physical unclonable functions for printed circuit board authentication. In *Computer-Aided Design (ICCAD), 2015 IEEE/ACM International Conference on*, pages 152–158. IEEE, 2015.

[51] X. Xu, W. Burleson, and D. E. Holcomb. Using statistical models to improve the reliability of delay-based pufs. In *VLSI (ISVLSI), 2016 IEEE Computer Society Annual Symposium on*, pages 547–552. IEEE, 2016.

[52] X. Zhang and M. Tehranipoor. Design of on-chip lightweight sensors for effective detection of recycled ics. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 22(5):1016–1029, 2014.

[53] X. Zhang, N. Tuzzio, and M. Tehranipoor. Identification of recovered ics using fingerprints from a light-weight on-chip sensor. In *Proceedings of the 49th Annual Design Automation Conference*, pages 703–708. ACM, 2012.

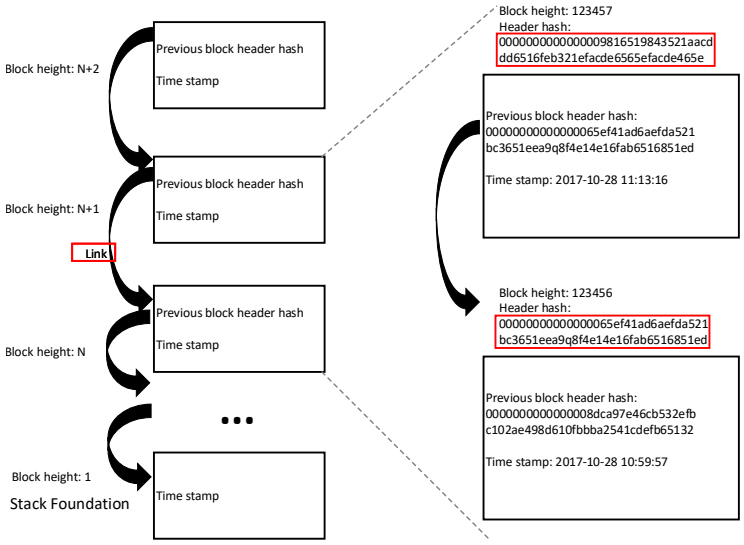
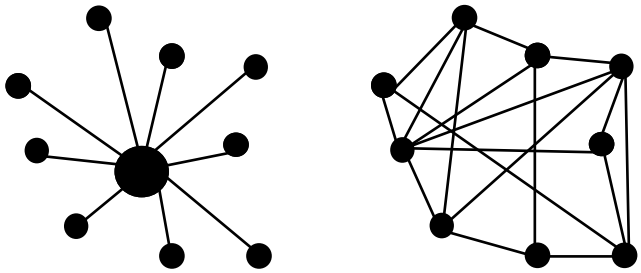


Figure 1: The schematic of vertically layered blockchain structure in Bitcoin scheme, each block is linked and referred back to a previous block by the header hash value [1].



(a) A schematic of centralized network.

(b) A schematic of decentralized network.

Figure 2: Comparison between centralized and decentralized network. (a) In the centralized network, all nodes are connected through the administrator node (denoted with the larger node in the middle). (b) In the decentralized network, nodes are directly connected with each other.

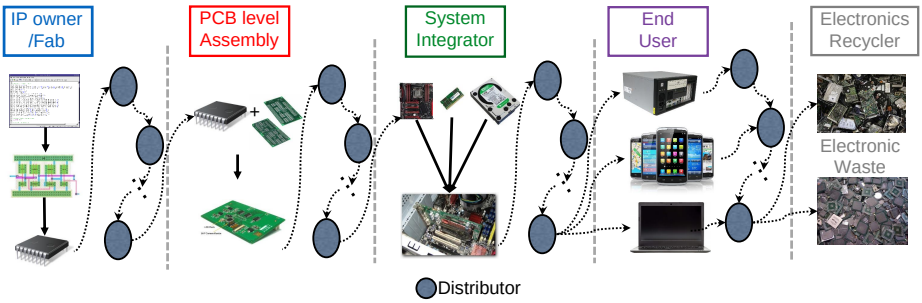


Figure 3: The schematic of electronics supply chain. In each stage, there exist several distributors who connect these major entities.

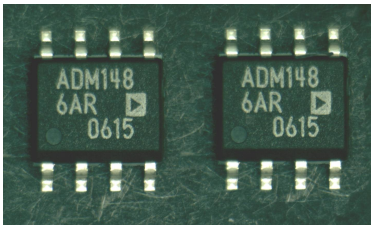


Figure 4: An example differential line transceiver chip from *Analog Devices* and a corresponding counterfeit copy [27].

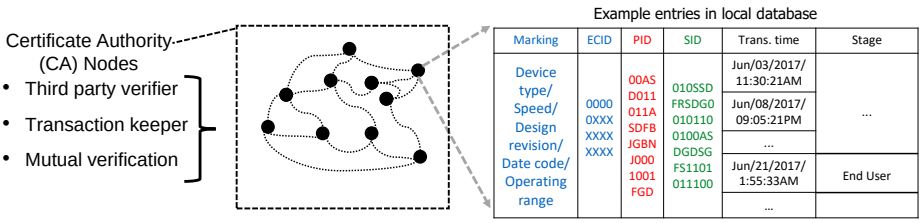


Figure 5: A decentralized "ledger" composed of several certificate authority (CA) nodes (denoted with the black dot •). Each CA node keeps a local database for the chip ID enrollment and verification, in which the detailed information like marking, ECID, PCB ID (PID), system ID (SID), transaction time and stage of an electronic component are stored. Upon the deployment, this CA network can serve for mutual authentication with each other, and provide verification service to different electronics supply chain participants.

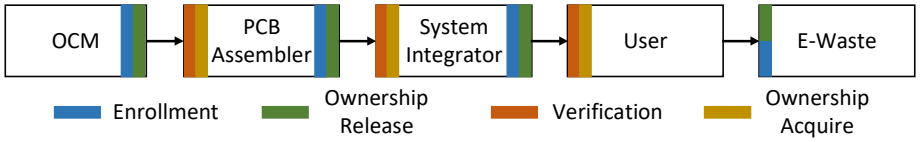


Figure 6: The schematic of a blockchain-enabled electronics supply chain, in which four extra steps are added: enrollment, ownership release, verification, and ownership acquire. These four steps denote the interactive communication between supply chain entities and the CA network.

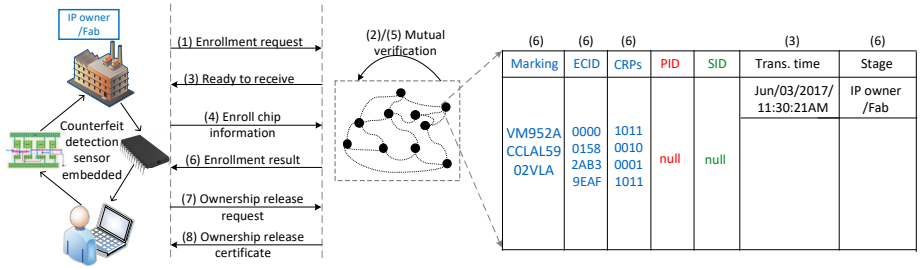


Figure 7: The ID enrollment procedure between IP owner and CA network. If the enrollment is successful, the detailed information of chips will be stored by CA network. Sequential steps are shown in brackets.

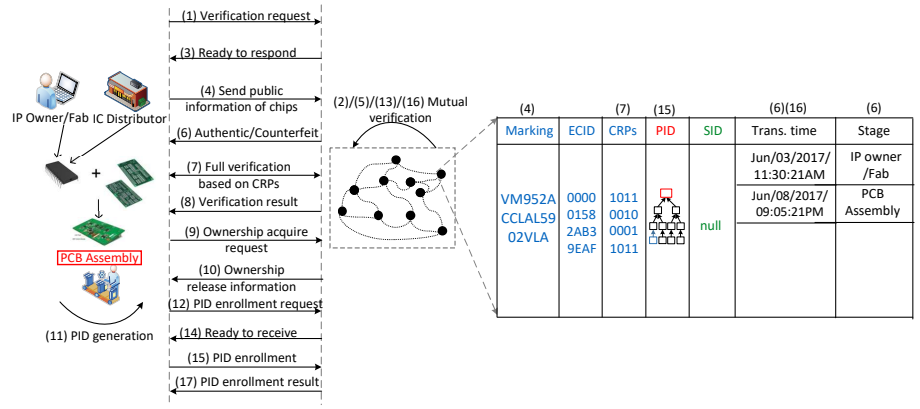


Figure 8: The proposed ID verification and PID enrollment procedure between PCB assembler and CA network. Note that for each verification or enrollment request, a "mutual authentication" will be conducted between all CA nodes, this greatly enhances the security and data integrity.

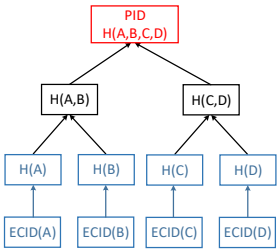


Figure 9: An example flow of PID generation based on hash tree structure, in which H stands for the hash computation. The root node refers to PID, which is the hashed results of several ECIDs (A, B, C and D in this example). Based on the algorithm of Merkle tree, SHA-256 protocol is employed as the hash function.

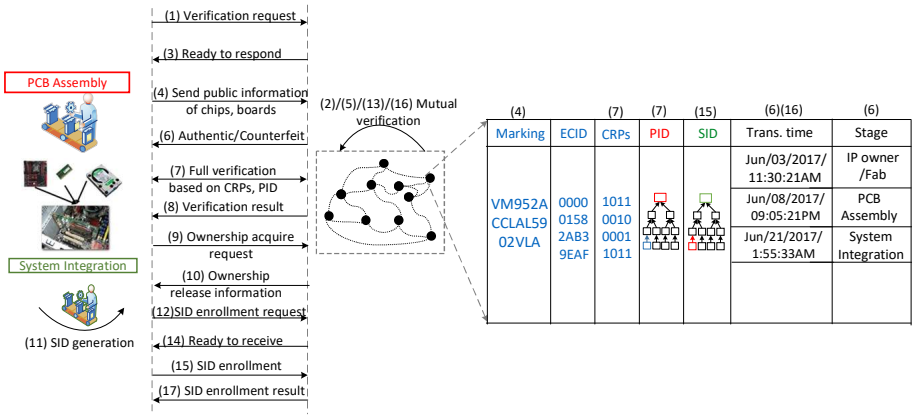


Figure 10: The proposed ID verification and SID enrollment procedure between system integrator and CA network.

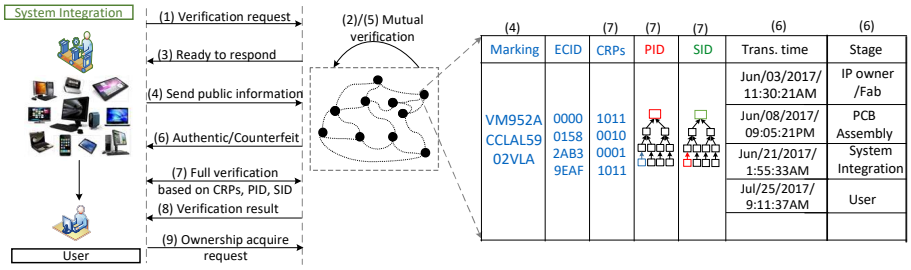


Figure 11: End user verifies the authenticity of the electronic products, and then get the ownership.

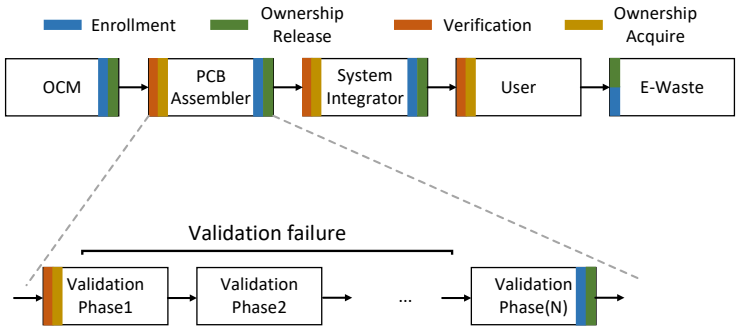


Figure 12: In the PCB assembly stage, an electronic product may go through several validation phases. Some of the validation phases may be classified as failed due to the deficiency of chips, or the performance inefficiency. The proposed framework is compatible with this practical scenario by only allowing the enrollment of the last electronic product that passes the validation.

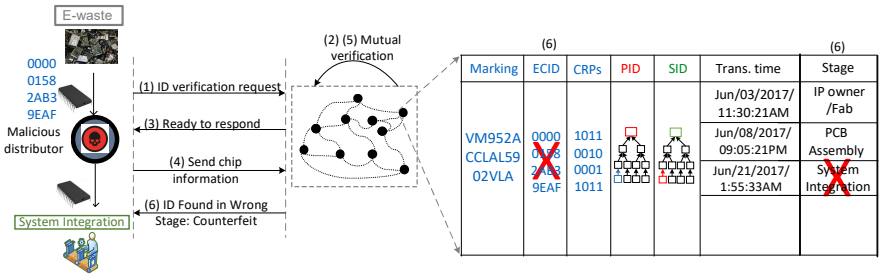


Figure 13: The recycled chips (or boards) can be detected by the CA network, even though they are with enrolled IDs stored in CA network, the stage prevents them from being deemed as new devices.

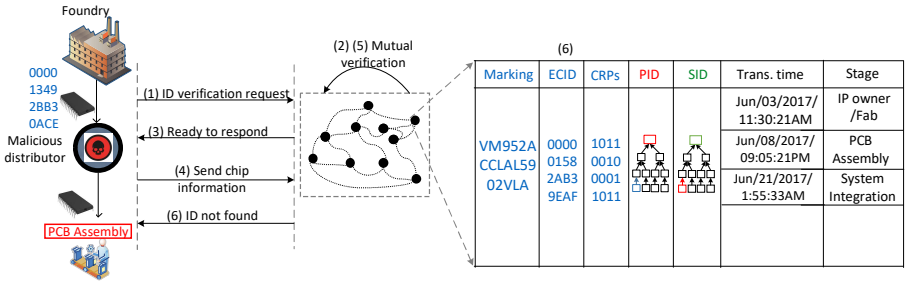


Figure 14: The overproduced chips can enter the electronics supply chain through untrusted entities. However, as the chip buyers can always resort to CA network for verification and tracking, such overproduced chips can be detected.

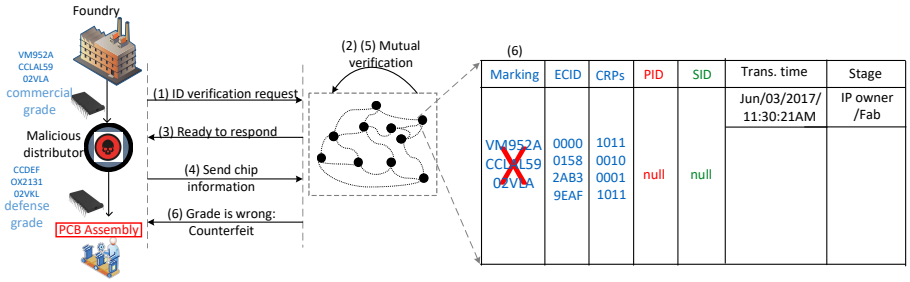


Figure 15: The CA network stores the marking information of the genuine electronic devices, hence any changes in the marking can be detected.