A Modular Blockchain Framework for Enabling Supply Chain Provenance

Yadi Zhong*, Amaar Ebrahim*, Ujjwal Guin*, and Vivek Menon†
*Dept. of Electrical and Computer Engineering, Auburn University
†National Reconnaissance Office
Emails:{yadi, aae0008, ujjwal.guin}@auburn.edu

***Abstract*—The exponential growth of electronic devices manufactured and produced is made possible due to the globalization of the semiconductor supply chain. However, this globalization of design, manufacturing, and distribution of electronic components and systems could potentially introduce counterfeit integrated circuits (ICs), devices, or systems blended with genuine products. These counterfeit components pose a severe threat to our critical infrastructures as they heavily rely on electronics. Due to the lack of sufficient observability and transparency, it is exceptionally challenging to monitor, manage, and control a healthy electronics supply chain. Besides, an adversary can easily compromise the electronic component's integrity and remain undetected due to the lack of traceability of parts and systems in the supply chain. In this paper, we propose a modular blockchain network for building a tamper-resistant record for the electronics supply chain. Each supply chain entity records specific information about the electronic product manufactured/distributed/assembled with product-dependent details. This allows each electronic system, as well as its embedded IC components, to be traced back to its origin, providing a thorough history of manufacturing, distribution, and integration records for supply chain provenance. Our proposed blockchain framework protects all the propriety information of all entities in the blockchain, where only the constant-size cryptographically secure hashes of the internal documentation/files are being recorded on chain.**

***Index Terms*—Supply chain, blockchain, traceability, provenance, IP piracy, counterfeit, globalization.**

I. Introduction

With the advent of globalization, ensuring the security, integrity, and authenticity of electronic components and systems and the supply chain that delivers them becomes highly challenging. The exponential growth of electronics becomes feasible due to the globalization of semiconductor design, manufacturing, and test processes, and the markets and nation-state incentives that support the investments needed for building the production capability and capacity. Unfortunately, the same globalization opens Pandora's box of threats, including (i) counterfeit ICs [1]–[5], (ii) piracy of intellectual properties (IPs) and cloning [6]–[9], and (iii) malicious modifications or tampering with hardware Trojans [10]–[12], as shown in Figure 1. These threats could present in multiple stages in the electronics supply chain, including design, fabrication, assembly, distribution, and system integrations, etc. Due to the sophistication of today's critical infrastructures, electronic products could be manufactured from multiple levels of system integration. For example, smaller systems, such as FPGAs and microcontroller boards, can be assembled first using discrete components, and we call it level-1 (L1) system integration.

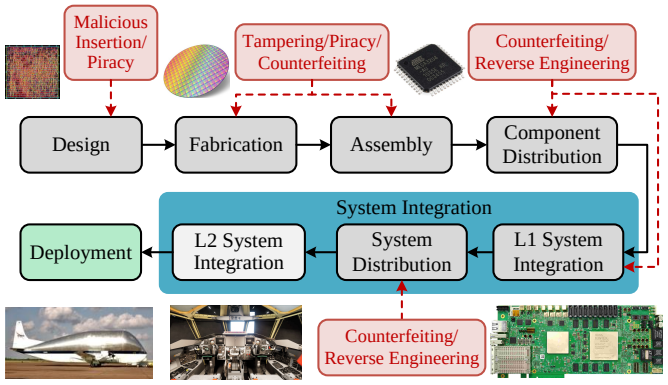

Figure 1: Overview of electronics supply chain and possible attack surface.

While complex systems, such as helicopter electronics, require integrations of multiple smaller L1 systems, and we denote it as level-2 (L2) system integration. Unfortunately, due to the complex globalized supply chain, an adversary could control or disrupt the supply chain or launch cyber attacks by exploiting hardware vulnerabilities. The hardware hack reported by Bloomberg shows a tiny chip, the size of a grain of rice, can be covertly hidden in a larger system to infiltrate data in U.S. companies [13], [14]. The threat was undetected due to the difficulty of observing and understanding the complete functionality of the electronic system and its supply chain. Observing and understanding the electronics and supply chain operations has many challenges and, if improperly conducted, can expose further vulnerabilities and threats to intellectual property and trade secrets.

Microelectronics systems will continue to proliferate and increase in complexity, as will the motivation to control and disrupt the supply chains for economic, military, and political gains. The advancement of ubiquitous computing in the Internet of Things (IoT) and Cyber-Physical Systems (CPS) applications increased the number of connected devices in the last decade. The prevalent use of IoT applications with pervasive sensing enables billions of devices to be connected to the internet [15]. The widespread use of low-cost devices in critical infrastructures and applications, such as smart grids, smart cities, industry 4.0 (smart manufacturing), and healthcare, will increase the number of devices. Keeping track of all these devices becomes crucial for enabling supply chain integrity. There will be a significant impact on national security if an adversary understands the intricacies of the

supply chain better than us and controls the flow of electronics. In addition, the recent shortage of chips [16] can provide a glimpse of an apocalyptic future if we do not control our supply chain.

The security community continuously develops various solutions to address these complex hardware security threats [1], [17]. Unfortunately, these solutions have not been universally adopted. First, it is necessary to ensure integrity so that any entity participating in transactions can rely on the supply chain and ensure the protection of their IPs and their advantage in the marketplace. This is crucial as the exposure of any details of an IP can provide an adversary with the necessary means for future exploitation. Second, incentives are necessary to encourage an entity in the supply chain to add security measures. Finally, trust and security measures must be evaluated based on observable and quantifiable metrics.

A significant issue with current supply chain record-keeping is scalability and storage. As a supply chain grows, the amount of storage needed grows astronomically. Consider the microelectronics supply chain; various companies use millions of components, and every detail of the creation and assembly process needs to be documented and securely accessed. Our proposed framework allows for the scalability of this complex system to simplify the overall approach and utilizes multiple blockchain instances to preserve privacy and enable security. Only permissioned users can access specific records in the framework. Our proposed modular blockchain-based framework consists of multiple blockchain instances. Blockchain instances can ensure independent data privacy and access control. Each instance will maintain its internal ledger with smart contracts so that necessary functions can only be run on them. The proposed layered infrastructure (see Figure 2 for details) uses B_C and B_S for tracking electronic components/devices and systems, respectively, whereas B_F and B_D maintain the details for manufacturing and design of chips, respectively. The end-user can track the details of an electronic part in B_C or an electronic system in B_S. Additional blockchains can also be added for suppliers and manufacturers if necessary. Note that all information for each blockchain can be stored either in a local database or in a distributed cloud environment based on the system administrator's preferences. The reference of the actual data (i.e., cryptographic hash) will be added to the blockchain ledger. This hash would then be used as an index to point to the data (which can be encrypted as well), which would be stored on a local database or secure cloud server.

The blockchain architecture proposed in this paper can address a wide variety of supply chain-related issues. First, the framework provides observability as the inherent properties of blockchain allow monitoring of the data it contains. As our proposed infrastructure is built upon Hyperledger Fabric, a permissioned blockchain, anyone with proper authorization can access the data. Second, the integration of modular blockchains creates a clear separation between different types of organizations. One can protect sensitive information locally and grant access to the data for authentication and verification purposes only. Additional privileges can be granted to authorized personnel and auditors (e.g., various DoD agencies) if it requires more information during the authentication. We believe that integrating the modular blockchain infrastructure will encourage more institutions to participate in this proposed infrastructure. It will ensure the protection of an institution's intellectual properties and trade secrets even though it is participating in the overall framework. Note that the compromise of one blockchain will not affect the overall security of the proposed infrastructure. Third, our proposed framework is scalable. The scalability arises from using a modular blockchain-based framework in which new types of institutions can be added without modifying the original infrastructure. Only the respective blockchain needs to be configured to communicate with the overall framework. Finally, the security of the system relies on the blockchain's intrinsic hashing properties, as well as the constant-size digests being used as data stored in distributed databases or cloud servers.

Contributions. We propose a layered, scalable, and permissioned blockchain [18] based traceability framework that is portable to broader industries to automate the tracking and traceability of electronic parts and systems from design to end of life. The proposed infrastructure can protect privacy, trade secrets, and integrity of the parts and the supply chain while delivering evidence and metrics of proper functionality. The scalability is ensured by integrating multiple blockchains from companies to the infrastructure without increasing the complexity and exposing sensitive data. The contributions of this paper are summarized as follows:

- *Modular Blockchain Framework:* Our proposed blockchain framework can create a modular system in which multiple organizations can be a part of a larger network seamlessly by adopting modular blockchain infrastructures to allow for the transfer of ledger assets from one blockchain ledger to another. No modifications in the preexisting infrastructure are necessary to bring organizations into the traceability framework. In addition, we adopted the data storage model presented in [19] to protect trade secrets. The publicly available information in the blockchain ledger is only the reference (a cryptographic hash) of the data (often an organization's trade secrets). The actual data needs to be encrypted and stored in a local database or cloud server and can be accessed by authorized personnel only.
- *Security and Trust Information Collection:* We propose to collect a wide variety of security-related data corresponding to the life cycle of an electronic device or system. The IP integrity information when a chip is in the design phase, whereas the data related to the manufacturing process, materials, masks, and tests in the fabrication phase are to be recorded. The traceability-related information for a part or system will be collected during the rest of the phases. Our proposed blockchain framework is designed for security and in a privacy-preserving manner. The proposed framework provides a clear separation between different blockchain instances. The Membership Service Provider (MSP) can grant (revoke) access to certain entities that are (not) able to query the blockchain. In addition, the queries can be approved or denied based on the requested information.
- *Seamless Integration:* It is necessary to maintain up-to-date security information to ensure the authenticity of a device or system. New threats and attacks are emerging, and ongoing

research is directed to map and document them so the community can benefit from them. For example, detailed vulnerability information can be found in the National Vulnerability Database (NVD) [20] and Common Weaknesses and Enumeration database (CWE) [21]. If new attack surfaces, a new set of design/fabrication data must be collected based on the mitigation strategy. We provide options for adding new entries by personnel with the proper security authorization.

The rest of the paper is organized as follows: In Section II, we present a general overview of blockchain technologies, including consensus algorithms and different consensus algorithms to update the blockchain ledger. In Section III, we provided detailed information regarding our proposed framework. Section IV is our conclusions and future works.

II. Related Work

A significant amount of research has been directed to ensure the security and integrity of the supply chain. Different researchers have proposed various solutions to address the detection and prevention of – counterfeit ICs [1], [2], [5], IP piracy and IC overproduction [7], [9], [22], and tampering ICs with a hardware Trojan [10]–[12]. First, counterfeit detection approaches can be grouped into different categories – G-19A Test Laboratory Standards, statistical data analysis, on-chip sensors and structures, and unique markers [1]. Second, the countermeasures for preventing IP piracy can be categorized as – logic locking [22], split manufacturing [23], and hardware watermarking [24]. Among them, logic locking is the most prominent key-based hardware obfuscation technique which is based on the inclusion of key-bit controlled XOR gates. Finally, hardware Trojan detection approaches can be broadly classified into detection and prevention approaches. The detection approaches can further be classified into four different categories, such as logic testing [25], side-channel analysis [17], image processing [26], and reverse engineering [27]. On the other hand, prevention approaches can be categorized as design-for-trust measures [28] and split manufacturing [23]. Even though these solutions can provide adequate protection against hardware threats, integrating all these different countermeasures and seamless verification can be extremely challenging.

The integration of blockchain for ensuring supply chain provenance receives widespread attention in academia, industry, and government due to the inherent properties and features of blockchain that could significantly enhance the traceability, transparency, and reliability of the supply chain [4], [29]–[31]. The authors in [32] introduced a blockchain-based framework, which ensures the authenticity of electronics with the help of an unclonable ID generated from an SRAM-based PUF. Xu et al. provided a comprehensive solution and summary for using blockchain to improve and secure the integrity of electronic supply chain [29]. Islam et al. proposed a method that uses PUF and blockchain to enhance the authenticity and traceability of parts in the supply chain [33]. However, the device ownership transfer is triggered and controlled by device owners. This design may lead to potential security issues. Human errors, delivery and management failures, in-transit thefts, and dishonest participants still threaten the supply chain even with blockchain implementation for tracking [34]. Cui et al. proposed a confirmation-based ownership transfer in the HyperLedger blockchain framework to address these threats, where the ownership transfer will be completed once the mutual agreement between sender and receiver [4].

The success of Bitcoin, introduced in the seminal paper published in 2008 by Satoshi Nakamoto, triggered a rapid development and general interest in designing blockchain technology and applying it to different fields. Primarily, the blockchain infrastructure relies on consensus mechanisms that guide how the data blocks to be added and can be permissionless or permissioned. There are four primary consensus mechanisms including Proof-of-Work (PoW) [35], Proof-of-Stake (PoS) [36], and Practical Byzantine Fault Tolerance (PBFT) [37]. A few other consensus mechanisms are also in practice, such as Proof of Elapsed Time (PoET), and Proof of Authority (PoA) [38]. Hyperledger Fabric [18], a permissioned blockchain that uses the Raft consensus algorithm, can be used for supply chain management. In addition, it is non-resource intensive, making it a preferable candidate for our framework. Note that anyone can join the consensus as long as they are a member of the blockchain infrastructure.

III. Proposed Approach

A significant issue with current supply chain record-keeping is scalability and storage. As a supply chain grows, the amount of storage needed grows astronomically. It is necessary to keep records of every detail of the design, manufacturing, and test process of an electronic component or system and to provide secure access to these data when required. Our proposed provenance framework utilizes multiple blockchain networks to allow each company/entity involved to provide the details of their product while keeping them secure.

TABLE I: Participating entities in electronics supply chain.

Entity	Description
Design House	Designs the complete IC.
3PIP Owner	Develops an IP and sells, or gives contracts to a design house for use.
Manufacturer	Owns a foundry and fabricates ICs.
Material Supplier	Supplies materials to a foundry.
System Integrator	Designs electronic systems. System Integrators can be at different levels. For example, FPGA boards (L1 system) can be used in a helicopter (L2 system).
System Assembler	Manufactures systems, e.g., most Raspberry Pis are made in a Sony factory in Pencoed, Wales, while others are made in China and Japan.
Component Distributor	Distributes ICs.
System Retailers	Distributes systems, e.g., Raspberry Pis can be purchased from Newark, PiShop.us, Amazon, etc.

Table I summarize the various entities and their roles in the electronics supply chain. In the proposed modular blockchain framework, we include (i) design house, (ii) third-party IP (3PIP) owners, (iii) Manufacturer, (iv) Material Suppliers, (v) System Integrator, (vi) System Assembler, (vii) Component Distributors, and ($viii$) System Retailers. The above-mentioned entities represent the design, manufacturing, integration, assembly, and distribution phases in the supply chain. Figure 2 shows an abstract view of our proposed layered blockchains-based framework,

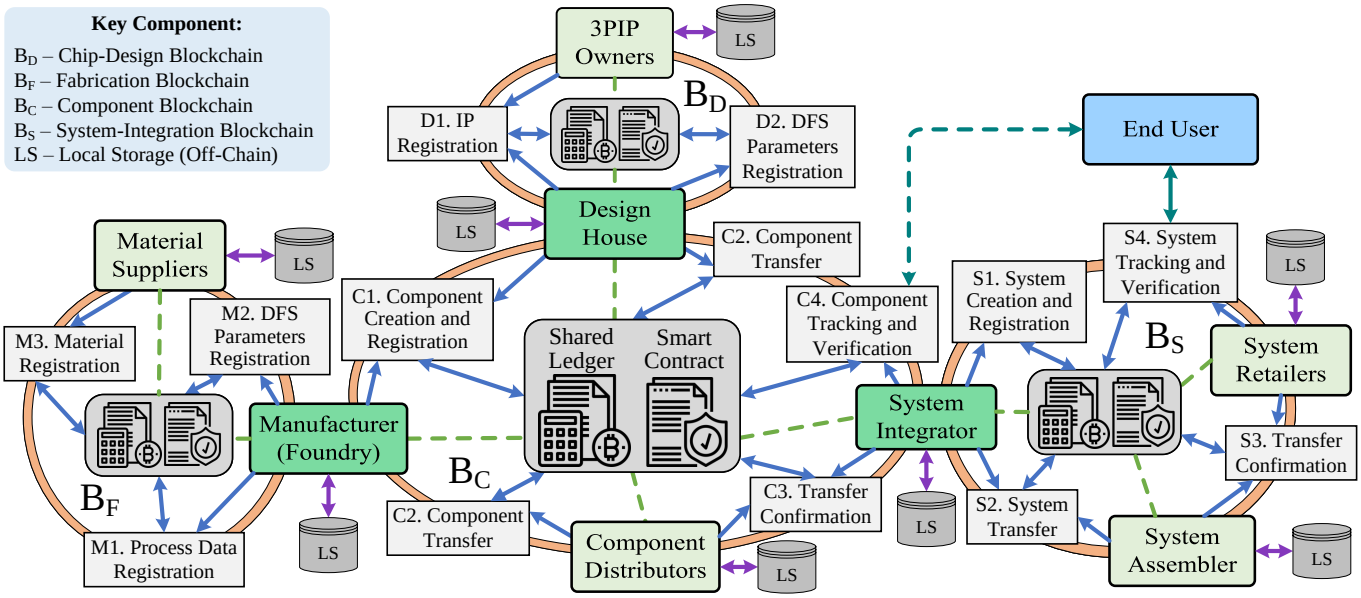

Figure 2: The proposed approach for the modular blockchain framework for supply chain provenance.

which consists of multiple blockchain instances. The blockchains, B_C, B_F, B_D, and B_S are independent of one another to preserve data privacy and access control. Each blockchain instance maintains its own internal ledger with smart contracts so that necessary functions can only be run on them. The proposed infrastructure uses B_C and B_S for tracking electronic components/devices and systems, respectively, whereas B_F and B_D maintain the details for manufacturing and design of chips, respectively. The end user can track the details of an electronic part in B_C or an electronic system in B_S. If necessary, additional chains (B_P and B_M) can also be added for material suppliers and manufacturers.

We have various participating entities within our proposed infrastructure, as visualized with green boxes. The entities directly involved with the component blockchain, B_C are the design houses, foundries, component distributors, and system integrators. Material suppliers and the foundries are included in the fabrication blockchain, B_F. The entities involved with the design blockchain, B_D, are the design houses and third-party intellectual property (3PIP) owners. System integrators, manufacturers, and distributors participate in the system blockchain, B_S. Depending on the entity's role in the electronics supply chain, it will only have privileged access to certain functions consistent with its role in a blockchain. Smart contract functions within each blockchain, and the proper invocation by authorized entities are depicted with a light gray text box and blue arrows in Figure 2, respectively. Note that all information for each blockchain can be stored either in a local database or in a distributed cloud environment based on the system administrator's preferences. The reference of the actual data (i.e., cryptographic hash) will be added to the blockchain ledger. This hash would then be used as the file digest to point to the data or documentation which the corresponding entity has stored on its off-chain local storage space [19]. To guarantee device authenticity and allow for component tracking in the component blockchain, B_C, the proposed framework will follow a similar approach as first proposed in [4]. Each electronic component will be labeled with a unique chip ID or an unclonable ID generated by an on-chip physically unclonable function (PUF) [39]. Note that PUFs use manufacturing process variations to create an unclonable ID.

The overall infrastructure can be viewed in four different life cycles: design, manufacturing, component, and system life cycles. In general, any entity on the blockchain is considered untrusted. We, nonetheless, conform to the common perception that design houses, foundries, system integrators such as Apple, AMD, Nvidia, TSMC, Samsung, Boeing, etc., and end users as trusted entities. There are no additional assumptions on manufacturers, suppliers, 3PIP owners, or distributors. Any unauthorized entity or adversary can enter the supply chain at any stage. The overall objective of this proposed framework is to ensure trust using efficient verification/authentication methods on components/systems based on their life-cycle data. Besides, the framework must allow the sensitive data (IPs) to be separated and can only be accessed by authorized personnel only. The detailed descriptions of these life cycles are described as follows:

A. *Component Life Cycle*

The component Life Cycle plays a central role in our proposed framework. It starts when a foundry sends manufactured parts for distribution. The component supply chain comprises design houses, foundries, distributors, and system integrators. Note that many of the designers of microelectronic devices do not own a manufacturing plant and outsource the fabrication to a foundry/fab due to the prohibitively high cost of building and maintaining a foundry [40]. The fabrication and assembly of an IC may happen at the same fabrication facility. Once the chips are fabricated, two possible distribution scenarios may occur – the designer could ask the fab to send back all the parts and distribute them by itself, or the fab directly sends the parts to the customer or authorized component distributors. Note that many distributors may not be certified by the designer to distribute their parts. Distributors that are not certified

are called independent distributors or brokers. Finally, the system integrators (commonly known as an original equipment manufacturer, OEM) acquire parts and build an electronic system. A part may travel to tens of different distributors in this complex component supply chain before being used in a system.

The primary objective of this life cycle is to provide traceability of electronic parts or devices. The traceability can be ensured using a unique device ID, which can be programmed into the device using one-time programmable memory (e.g., electronic chip ID or ECID [41]), or a unique identification can be obtained for an on-chip physically unclonable function (PUF) [42]–[46]. We adopt the blockchain framework introduced in our previous paper [4]. One can find the details of functions 'C1: Component Creation and Registration', 'C2: Component Transfer', 'C3: Transfer Confirmation', and 'C4: Component Tracking and Verification' equivalent as 'C1: Device Creation and Registration', 'C2: Device Transfer', 'C3: Transfer Confirmation', and 'C4: Device Tracking and Verification' in [4], respectively.

B. Design Life Cycle

The design life cycle ensures the proper design of chips and is the first stage of the semiconductor supply chain. The participating entities are the chip designer or design house and third-party IP (3PIP) owners. The ASIC design flow involves several major design activities. The design starts with system specification and then undergoes functional design using behavioral modeling using Verilog or VHDL and its verification. The design is then synthesized to obtain a gate-level netlist, and post-synthesis design validation is performed. Finally, physical design is obtained after cell placement, scan chain, and clock tree insertion and routing [47]. The design is then signed off, and the mask set is ready for fabrication. CAD tools are extensively used for design synthesis, verification, place and route, and manufacturing test pattern generation in this complex design process. Besides, the increased complexity in ASIC design and reduced time to market forces the design house to include third-party developed IPs (3PIPs) in the SoC design. The entire design flow, from functional specification to design sign-off, is performed in many different places, even in different countries. Note that, for a design house, the design details and layout are the company's proprietary information, which is kept secret in the local storage. Only the cryptographic hash is posted on the B_D blockchain, which helps build a reference if authorized auditors (*e.g.*,, DoD personnel) later request for inspections and validations. Attacks on the design stage can be of two types. First, an adversary (an untrusted entity) can steal the IPs, commonly known as IP piracy. Second, an adversary (can be an untrusted 3PIP owner) can tamper a 3PIP with codes to create a secret backdoor that can be exploited in the field. The functions 'D1: IP Registration' and 'D2: DFS Parameters Registration' can be described and implemented as 'C1: Device Creation and Registration'.

C. Manufacturing Life Cycle

The manufacturing life cycle begins when the sign-off design (GDSII file) is transferred to a foundry or fab. Typically, the manufacturing starts with the processing of silicon wafers by cutting into a very thin disk on which hundreds of dies are developed. This wafer undergoes a series of steps, such as oxidation, lithography, etching, doping, and metal deposition. A wafer test is then performed to discard defective dies. The defect-free dies are then sent to an assembly for packaging. Many of the fabs maintain an assembly for packaging. Finally, molding is performed after the dies are placed on the lead frame or PCB. The entire semiconductor manufacturing is exceptionally complex, involving hundreds of steps, and often requires hundreds of materials. Building and maintaining such a fab requires billions of dollars, forcing most design houses to outsource semiconductor manufacturing. The IP rights generally protect the design house from potential misuse of IPs. Unfortunately, an untrusted fab (often located offshore) can pirate the design details and clone the original design. IP piracy has become one of the significant problems for the semiconductor industry that require immediate attention. Besides, a sensitive design can maliciously be tampered with a hardware Trojan so that an adversary can exploit the backdoor while it is being used in our critical infrastructure. We believe that the proposed blockchain framework provides visibility and transparency in semiconductor manufacturing so that many of these threats can be eliminated. The functions 'M1: Process Data Registration', 'M2: DFS Parameters Registration', and 'M3: Material Registration' can be described and implemented as 'C1: Device Creation and Registration'.

D. System Life Cycle

The system life cycle is essential to integrating ICs obtained from component distributors, assembling PCBs, and producing electronic systems before they are shipped to the end user to be deployed to the respective infrastructures. The system integration blockchain includes system integrators, system assemblers, and system retailers. Any details or information internal to the respective party are stored locally in their own database, while only the cryptographically secure digest is published on the B_S blockchain. Note that system integrators can be categorized by levels of electronics integration. For example, a finished PCB board such as Raspberry Pis and FPGAs can be done by level-1 (L1) system integrators. To complete the integration for more sophisticated electronics systems like helicopters and cars, PCB boards assembled from L1 system integrators becomes building blocks for manufacturing these large-scale electronics. The system integrators that incorporate products from L1 system integrators to manufacture more complex electronics are denoted as level-2 (L2) system integrators. Depending on the end users and the use case of an electronics product, it may need only L1 or both L1 and L2 to assemble and build it. From the end user's perspective, system integration is the last phase in the supply chain and also the initial point for providing system-level traceability and provenance for electronics deployed in the infrastructure. Component-level traceability and tracking, as well as design and manufacturing-related details, can be recursively extracted from the corresponding blockchain ledgers by tracking each IC/component on the system. Functions 'S1: System Creation and Registration', 'S2: System Transfer', and 'S3: Transfer Confirmation' are included in the smart contracts

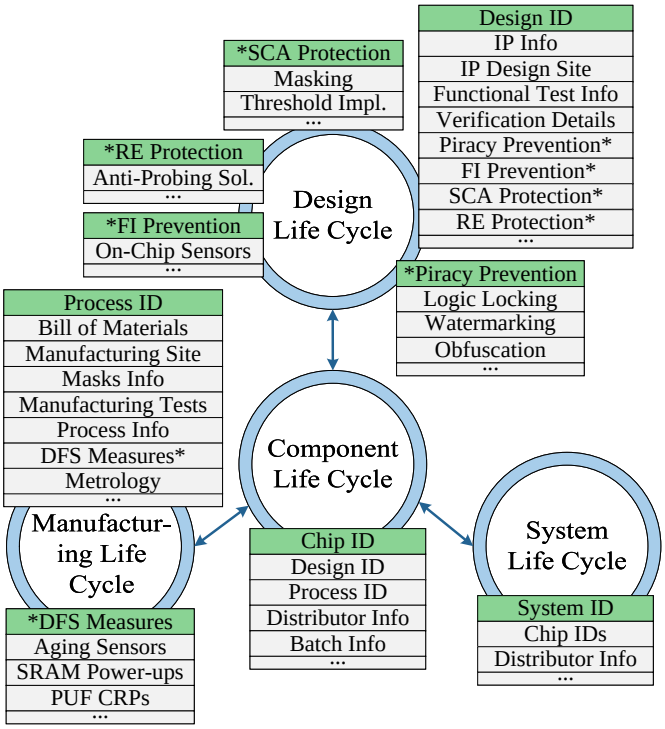

Figure 3: Key data collection for supply chain provenance.

for blockchain B_S and are analogous to'C1: Device Creation and Registration', 'C2: Device Transfer', and 'C3: Transfer Confirmation' in [4], respectively.

E. Data Collection

Figure 3 shows the overview of how information is collected across different entities of the electronics supply chain. Essentially, this figure depicts the entire life cycle of an electronic system, from raw materials for fabrication and IPs to the completed system. First, the manufacturing life cycle captures the required information regarding the manufacturer details, materials and process information, metrology and manufacturing test data, and designed-for-security (DFS) parameters. Second, the design life cycle contains information regarding the 3PIP information, functional test information, and DFS methods. Third, the component life cycle incorporates all these previous stage information using their references (e.g., process ID and design ID). It also includes traceability information by adding distributors. Finally, the system life cycle includes the reference of the previous stage (i.e., unclonable chip ID) and the system's traceability information. When the research communities and industry discover new vulnerabilities and/or possible solutions, the DSF parameters must be updated by incorporating state-of-the-art solutions to counter new threats and attacks. Details related to vulnerability information can be found in the National Vulnerability Database (NVD) [20] and Common Weaknesses and Enumeration database (CWE) [21], which will be used as the basis and scope for creations of DFS parameters, as shown in Figure 3. Below is a summary of key DFS parameter information to be collected.

- A design that contains: (1) aging sensors, (2) physically unclonable functions, (3) piracy prevention techniques such as logic locking, watermarking, or obfuscation, (4) side-channel prevention techniques such as masking, threshold implementation, etc. (5) fault injection prevention methods and (6) Anti-probing methods.
- Aging sensor values, PUF challenge-response pairs (CRPs), SRAM power-up states, all manufacturing test status, manufacturing time and location, etc.
- All traceability-related information from all the distributors and end-users.

F. Implementation

We provide a reference implementation of the proposed modular blockchain framework using Hyperledger Fabric, one of the popular blockchain platforms initiated by the Linux Foundation [18]. It is an open-source and permissioned blockchain with the Raft consensus protocol. It supports building multiple channels across diverse peers in the blockchain while each channel maintains its ledger and list of channel memberships. To test our proposed implementation, we set up a Hyperledger Fabric network with two channels, five peer organizations, and two orderer organizations. One can find the details related to channels, peers, and orderers in [18]. All organizations run on a single computer in separate Docker containers, allowing us to simulate operation on a multi-computer network. The orderer organizations are configured to a Raft ordering service, with one orderer organization per channel. The channels we implement correspond to the Component Blockchain (B_C) and System Life Cycle blockchain (B_S), but they could be easily expanded to include B_F and B_D blockchains. The peer organizations correspond to a Manufacturer, Component Distributor, Design House, System Integrator, and End User. Each organization uses a LevelDB as storage, as opposed to CouchDB. We modify the default channel configuration file, configtx.yaml, by adding the organization definitions, creating a new application-level policy, and encoding channel profiles. We use Hyperledger Fabric's default cryptographic material generator, crytogen, to generate public keys, private keys, and certificates for organizations within the network [48]. We implement all smart contracts in B_C and B_S using the Node.js Fabric Contract API and Fabric Shim.

IV. Conclusion

In this paper, we proposed a modular blockchain framework for building a robust supply chain to provide transparency, traceability, and provenance for electronic components and products. Our framework allows end users to trace back the origin of a system with its complete history of (i) systems assembly, integration, and tracking details, (ii) components fabrication, registration, and distribution details, (iii) raw materials from suppliers during the IC fabrication, and (iv) IP/3PIP registration details from the design. As the proposed blockchain framework is modular, trade secrets from each entity in the supply chain can be compartmentalized and protected from unauthorized access. In addition, we propose to record the cryptographically secure

hash of information rather than the information itself on the blockchain ledger. The propriety information of the respective entity needs to be stored off-chain local servers. The proposed modular blockchain framework allows periodic updates of supply chain countermeasures and relevant parameters against newly discovered threats or vulnerabilities once they are reported.

ACKNOWLEDGMENT

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

REFERENCES

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

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

[3] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 9–23, 2014.

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

[5] U. Guin, W. Wang, C. Harper, and A. D. Singh, "Detecting Recycled SOCs by Exploiting Aging Induced Biases in Memory Cells," in *IEEE Int. Symp. on Hardware Oriented Security and Trust*, pp. 72–80, 2019.

[6] M. M. Tehranipoor, U. Guin, and S. Bhunia, "Invasion of the hardware snatchers," *IEEE Spectrum*, vol. 54, no. 5, pp. 36–41, 2017.

[7] E. Castillo, U. Meyer-Baese, A. García, L. Parrilla, and A. Lloris, "IPP@ HDL: efficient intellectual property protection scheme for IP cores," *Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 15, no. 5, pp. 578–591, 2007.

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

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

[10] S. Adee, "The hunt for the kill switch," *iEEE SpEctrum*, vol. 45, no. 5, pp. 34–39, 2008.

[11] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design&Test of Comp.*, pp. 10–25, 2010.

[12] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware Trojans: Lessons learned after one decade of research," *Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 22, no. 1, p. 6, 2016.

[13] J. Robertson and M. Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," 2018.

[14] J. Robertson and M. Riley, "The Long Hack: How China Exploited a U.S. Tech Supplier," 2021.

[15] I. Analytics, "State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally," 2022.

[16] CNBC, "The global chip shortage could last until 2023," 2021.

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

[18] A Blockchain Platform for the Enterprise, HYPERLEDGER FABRIC. https://hyperledger-fabric.readthedocs.io/en/release-2.5/, Date accessed: 07.24.2023.

[19] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in *Proceedings of 2017 on Cloud Computing Security Workshop*, pp. 45–50, 2017.

[20] National Vulnerability Database, https://nvd.nist.gov/.

[21] CWE-Common Weakness Enumeration. http://cwe.mitre.org/data/definitions/1194.html.

[22] J. A. Roy, F. Koushanfar, and I. L. Markov, "EPIC: Ending piracy of integrated circuits," in *Proceedings of the conference on Design, automation and test in Europe*, pp. 1069–1074, 2008.

[23] K. Vaidyanathan, B. P. Das, and L. Pileggi, "Detecting reliability attacks during split fabrication using test-only BEOL stack," in *Design Automation Conference (DAC)*, pp. 1–6, 2014.

[24] E. Charbon, "Hierarchical watermarking in IC design," in *Proc. of the Custom Integrated Circuits*, pp. 295–298, 1998.

[25] Z. Zhou, U. Guin, and V. D. Agrawal, "Modeling and Test Generation for Combinational Hardware Trojans," in *VLSI Test Symp. (VTS)*, pp. 1–6, 2018.

[26] A. Stern, D. Mehta, S. Tajik, U. Guin, F. Farahmandi, and M. Tehranipoor, "SPARTA-COTS: A Laser Probing Approach for Sequential Trojan Detection in COTS Integrated Circuits," in *IEEE Physical Assurance and Inspection of Electronics (PAINE)*, pp. 1–6, 2020.

[27] S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, "A survey on chip to system reverse engineering," *ACM journal on emerging technologies in computing systems (JETC)*, vol. 13, no. 1, pp. 1–34, 2016.

[28] H. Salmani, M. Tehranipoor, and J. Plusquellic, "A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time," *Trans. Very Large Scale Integration Sys.*, pp. 112–125, 2012.

[29] X. Xu, F. Rahman, B. Shakya, A. Vassilev, D. Forte, and M. Tehranipoor, "Electronics supply chain integrity enabled by blockchain," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 24, no. 3, pp. 1–25, 2019.

[30] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, *et al.*, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.

[31] M. Pilkington, "11 blockchain technology: principles and applications," *Research handbook on digital transformations*, vol. 225, 2016.

[32] U. Guin, P. Cui, and A. Skjellum, "Ensuring Proof-of-Authenticity of IoT Edge Devices using Blockchain Technology," in *IEEE Int. Conf. on IoTs (iThings) and IEEE GreenCom and IEEE CPSCo) and IEEE SmartDat)*, pp. 1042–1049, 2018.

[33] M. N. Islam and S. Kundu, "Enabling ic traceability via blockchain pegged to embedded puf," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 24, no. 3, p. 36, 2019.

[34] B. Tukamuhabwa, M. Stevenson, and J. Busby, "Supply chain resilience in a developing country context: a case study on the interconnectedness of threats, strategies and outcomes," *Supply Chain Management: An International Journal*, vol. 22, no. 6, pp. 486–505, 2017.

[35] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf," 2008.

[36] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, no. 1, 2012.

[37] M. Castro, B. Liskov, *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, pp. 173–186, 1999.

[38] P. Cui, U. Guin, A. Skjellum, and D. Umphress, "Blockchain in IoT: Current Trends, Challenges, and Future Roadmap," *Journal of Hardware and Systems Security*, vol. 3, no. 4, pp. 338–364, 2019.

[39] Y. Zhang and U. Guin, "End-to-End Traceability of ICs in Component Supply Chain for Fighting Against Recycling," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 767–775, 2019.

[40] Age Yeh, "Trends in the global IC design service market." DIGITIMES Research, 2012.

[41] ECID - Electronic Chip ID, IEEE, https://grouper.ieee.org/groups/1149/1/ECID_Electronic_Chip_ID.html.

[42] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of ACM Conf. on Computer and Communications Sec. (CCS)*, ACM, 2002.

[43] G. Suh and S. Devadas, "Physical Unclonable Functions for device authentication and secret key generation," in *Proc. of ACM/IEEE on Design Automation Conference*, 2007.

[44] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," in *International workshop on Cryptographic Hardware and Embedded Systems*, Springer, 2007.

[45] W. Wang, A. Singh, U. Guin, and A. Chatterjee, "Exploiting power supply ramp rate for calibrating cell strength in SRAM PUFs," in *IEEE Latin-American Test Symposium*, 2018.

[46] T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "Aro-puf: An aging-resistant ring oscillator puf design," in *Proceedings of the conference on Design, Automation & Test in Europe*, p. 69, 2014.

[47] Fusion design platform, Synopsys. https://www.synopsys.com/implementation-and-signoff/fusion-design-platform.html.

[48] cryptogen, https://hyperledger-fabric.readthedocs.io/en/latest/commands/cryptogen.html, Date accessed: 07.24.2023.