A Dissertation

entitled

An Assured and Zero Trust Semiconductor Supply Chain enabled by Blockchain Technology and Hardware Oriented Security

by

Akshay Raghavendra Kulkarni

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the Doctor of Philosophy Degree in Engineering

Dr. Mohammed Niamat, Committee Chair

Dr. Devinder Kaur, Committee Member

Dr. Weiqing Sun, Committee Member

Dr. Ahmad Javaid, Committee Member

Dr. Noor Ahmad Hazari, Committee Member

Dr. Scott Molitor, Acting Dean
College of Graduate Studies

The University of Toledo
August 2023

© 2023 Akshay Raghavendra Kulkarni

This document is copyrighted material. Under copyright law, no parts of this document may be reproduced without the expressed permission of the author.

An Abstract of

An Assured and Zero Trust Semiconductor Supply Chain enabled by Blockchain Technology and Hardware Oriented Security

by

Akshay Raghavendra Kulkarni

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the Doctor of Philosophy Degree in Engineering

The University of Toledo
August 2023

The microelectronics industry is facing significant security challenges, leading to extensive research in the field of assured and trusted microelectronics. Due to economic reasons, this challenge is further compounded by the involvement of various global entities in the semiconductor supply chain [1]. However, an unreliable or untrustworthy supply chain can compromise the quality of integrated circuits (ICs) [2]. The IC supply chain, including Field Programmable Gate Arrays (FPGAs), encounters numerous challenges, including Intellectual Property (IP) theft, hardware Trojan intrusion, reverse engineering, and overproduction [3]. Additionally, ensuring the genuine ownership of an IC as it progresses through different stages of the supply chain and conducting provenance checks are of paramount importance [4].

There have been well-documented cases of counterfeit chips and chips implanted with Trojans infiltrating the supply chain. According to a report published by the 'Alliance for Gray Market and Counterfeit Abatement (AGMA) in December 2020, there has been a 254% increase in counterfeit chips [5], [6]. It is also reported that 15% of the spare and replacement parts purchased by the Pentagon for the U.S. Department of Defense (DoD) turn out to be counterfeits [7].

This research aims to enhance the security of the semiconductor supply chain by implementing zero trust principles using blockchain technology and hardware-oriented security primitives such as Physical Unclonable Functions (PUFs). The main pillar of a zero-trust architecture involves satisfying the seven tenets established by NIST [8]. In this investigation, these tenets are fulfilled through the use of PUFs and blockchain technology. The efficient implementation of the proposed technique is demonstrated through simulated case studies, showcasing the successful assurance and zero-trust implementation in the semiconductor supply chain. The blockchain network is built on the Ethereum platform, utilizing the Solidity language for smart contract development. It is simulated using personal blockchain Ganache, provided by Truffle suite, which emulates the Ethereum Mainnet without using actual Ethers. The supply chain network is simulated using Xilinx Artix-7 FPGAs mounted on Nexys 4 Digilent boards. The case study simulations utilize ROPUFs for validating the authenticity of the FPGA chips. The results of the case studies demonstrate that the developed blockchain network ensures secure transfer of authentic FPGA chips between parties in the supply chain network and can identify the guilty party in the event of a breach. The performance of the blockchain network is computed on the basis of transactions per second (TPS) and latency for three different block times – 60, 120 and 180 seconds. The TPS recorded are 0.017, 0.0152 and 0.0158 for 60, 120 and 180 seconds respectively, while the average latency of the blockchain is calculated to be 0.66 seconds, with registration of participant requiring the most time with 1.36 seconds. The case studies confirm the successful fulfillment of the zero-trust tenets.

Finally, the work done in this dissertation explores Non-Fungible Tokens (NFTs) as an application of blockchain technology for assured and trusted microelectronics.

Anna, my late grandfather, Mr. M. N. Kulkarni, I know your blessings are always with me. I miss you. I wish you were with me today. This is for you from your *Ghodoba!*.

Acknowledgements

This journey would have been difficult without the support of my family, my advisor, professors, and friends.

Firstly, I would like to thank my advisor Dr. Mohammed Niamat for providing me an opportunity to conduct my graduate research under him and for continued support and guidance. My sincere thanks to Dr. Devinder Kaur, Dr. Weiqing Sun, Dr. Ahmad Javaid and Dr. Noor Ahmad Hazari for being a part of my dissertation committee.

A major part of this Ph.D. was financially supported by the Assured Digital Microelectronics Training and Education Ecosystem (ADMETE) grant awarded by the U.S Air Force Research Laboratory (AFRL). Financial support from the EECS, and Physics and Astronomy departments is also greatly acknowledged.

I would like to thank my lab mates, Dr. Noor Ahmad Hazari, Dr. Ahmed Oun, Dr. Faris Alsulami, Amrit Niraula, Muskan Saraf, Hrishav Bhattrai, and Talha Syed Hussain for spending their precious time to help me out in my research. Very importantly I would like to thank my parents Mr. R.V. Kulkarni and Mrs. Parimal Kulkarni, my wife Shraddha Ghotkar, and my in-laws, Mr. Dilip Ghotkar and Mrs. Dipti Ghotkar and my entire family for their constant love, support, understanding, encouragement, and motivation that made this work possible. Big thanks to my friends who made living away from home feel like home.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

3P	Third Party
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BIST	Built-in-Self-Test
BEOL	Back End of Line
CRPs	Challenge response Pairs
ECID	Electronic Component Identification
EDA	Electronic Design Automation
FEOL	Front End of Line
FPGA	Field Programmable Gate Array
GDSII	Graphic Design System Information Interchange
HT	Hardware Trojan
IC	Integrated Circuit
ID	Identification
IoT	Internet of Things
IP	Intellectual Property
IPFS	InterPlanetary File System
MPV	Manufacturing Process Variation
NFT	Non-Fungible Tokens
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OSAT	Outsourced Semiconductor and Testing
PoA	Proof of Authority
PUF	Physical Unclonable Function
RO	Ring Oscillator

RoT	Root of Trust
TPS	Transactions per Second
ZTA	Zero Trust Architecture

Chapter 1

Introduction

1.1 Background

In an effort to reduce fabrication costs, the semiconductor supply chain has become global [9]. The modern Integrated Circuit (IC) supply chain involves participants from different parts of the world collaborating to ensure its success [2]. For instance, Third Party IP vendors (3PIP vendors) provide the Intellectual Property (IP) [10], while chip design is carried out in a design house using EDA tools sold by Third Party EDA Vendors [12]. It is worth noting that the design house encompasses various steps that integrate different IP cores and generate a chip blueprint in the form of a Graphical Design System (GDSII) file [13], [14]. The blueprint is then physically created at the foundry, which involves several steps [15], [16]. Once the chip is manufactured, it is sent to the Outsourced Semiconductor Assembly and Testing (OSAT) for testing and packaging [17]. After verification and packaging, the OSAT sends the chip either back to the design house for further testing or directly to the Original Equipment Manufacturer (OEM), who combines all the chips received from the OSAT to create a final electronic product [18]. This final product is then distributed to end customers through distributors and/or retailers. In summary, an IC supply chain involves various entities, both trusted and untrusted, which raises concerns about the security of the chip and the final electronic product, especially when it may be used in critical infrastructure, including military applications [19].

1.2 Research Motivation

Every step in an IC supply chain is vulnerable to attacks from malicious actors who can tamper with the ICs, introduce compromised chips, or pose a threat to the security and integrity of the entire supply chain [14], [20]. The growing complexity of the IC supply chain, involving various players from different parts of the world, makes it challenging to monitor and address these issues [21].

The contemporary semiconductor supply chain, with its diverse participants from across the globe, faces several challenges that can compromise its security and integrity. These challenges include a rogue 3PIP vendor tampering with the actual IP core [22], a malicious actor at the design house manipulating the IC design, or stealing and leaking the IP [23], [24]. Additionally, there are risks such as the intrusion of hardware Trojans at the foundry or the issue of overproduction of ICs [25]. Another concern arises from internal adversaries at the OSAT leaking sensitive test data. A visual representation of the threat model for an IC supply chain is presented in Figure 1-1.

A concerning incident related to hardware security involves a well-known consumer electronic company discovering that a recycler in Canada was illegally reselling over 100,000 of their products, with an estimated value of USD $23 million [8]. This highlights not only the presence of external adversaries but also the challenges posed by insider threats within the IC supply chain. Another notable example is the indictment of four employees from a semiconductor giant in October 2022, accused of stealing valuable semiconductor technologies and leaking them to rival overseas firms [9]. Given these prominent challenges, the US Government took action by issuing an executive order in February 2021 to enhance the resilience of America's supply chain, including the semiconductor industry [29]. Furthermore, another executive order in May 2021 emphasized the importance of zero-trust architecture in bolstering national cybersecurity [30]. Building upon this context, this dissertation proposes a zero-trust architecture for the semiconductor supply chain, leveraging blockchain technology and hardware security primitives such as physical unclonable functions (PUFs).

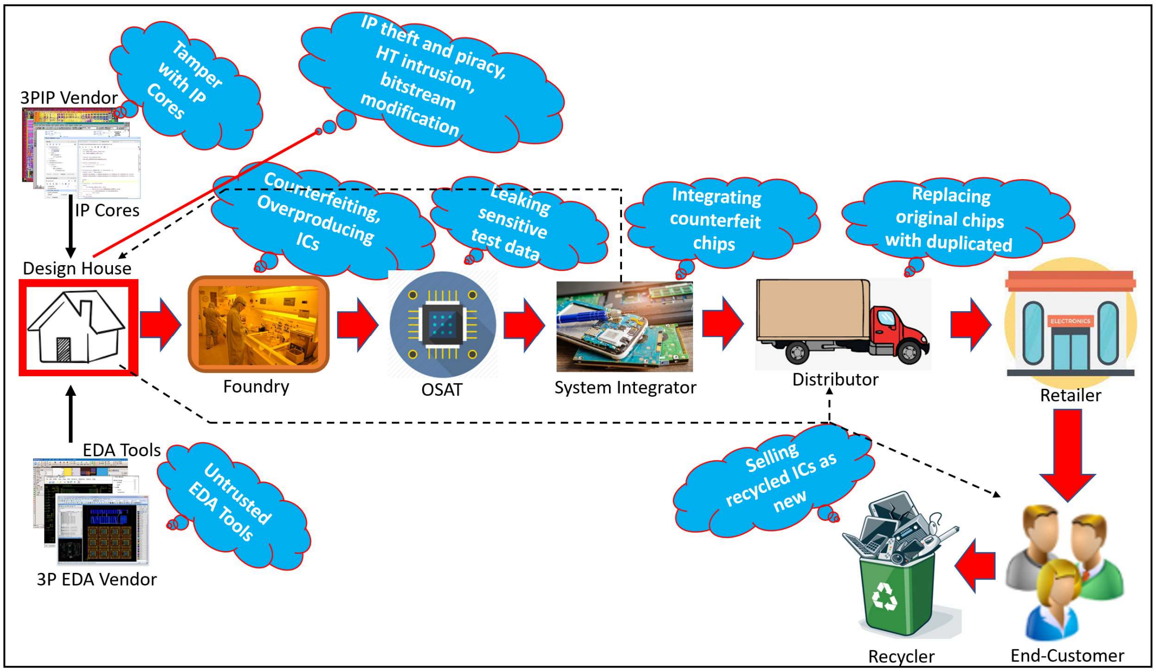

Tamper with IP Cores
IP theft and piracy, HT intrusion, bitstream modification
3PIP Vendor
IP Cores
Design House
Counterfeiting, Overproducing ICs
Leaking sensitive test data
Integrating counterfeit chips
Replacing original chips with duplicated
Foundry
OSAT
System Integrator
Distributor
Retailer
EDA Tools
Untrusted EDA Tools
3P EDA Vendor
Selling recycled ICs as new
Recycler
End-Customer

Figure 1-1: Modern semiconductor supply chain depicting possible security vulnerabilities at each stage

1.3 Relevant Concepts

This section explores the key concepts proposed to achieve the objectives of the dissertation. It begins by discussing zero trust, which establishes a security layer to safeguard the supply chain network. Next, the blockchain is explained, along with its application in the context of the supply chain. This is followed by an overview of smart contracts, which house the transaction logic. Finally, the Ring Oscillator Physical Unclonable Function (ROPUF) is discussed. Acting as a fingerprint, the ROPUF establishes a Root-of-Trust (RoT) for the ICs. Both blockchain technology and ROPUF are utilized to align with the policies outlined by the Zero Trust Architecture (ZTA).

1.3.1 Zero Trust Architecture

The term zero trust was coined in 2010 by the analyst firm Forrester Research as a response to modern attacks in the field of information security [30], [31]. The traditional security model operated under the assumption that anything within the security boundaries could be trusted. However, this assumption is now outdated, and there is a growing recognition that the notion of trusted networks needs to be discarded [32]. Zero trust is a cybersecurity paradigm that focuses on protecting resources and acknowledges that trust cannot be assumed but must be continuously evaluated [8], [30], [31]. It is based on the principle that organizations should not automatically trust anything, whether inside or outside their perimeter. Before granting access, everything attempting to connect to their systems should undergo verification. This approach leads to the micro segmentation of the network, which serves as the foundation for building a zero-trust network.

In practical terms, zero trust implies that access to any resource within the network should be subject to specific trust dimensions or parameters. If these parameters are not met, the result should be denial or revocation of access to that particular resource [33]. Zero trust encompasses a range of concepts and ideas aimed at minimizing uncertainty when enforcing accurate, least-privilege, per-request access decisions in information systems and services, ultimately leading to a micro segmented network [34]. Recognizing the significance of zero trust, the National Institute of Standards and Technology (NIST) outlined seven tenets to define zero trust in a special publication [8]. These tenets have been empathized and then mapped to the semiconductor supply chain domain in this work, as demonstrated in Table 1.1.

Table 1.1: Zero trust tenets and their description

Tenets	Description
Data and computation are considered as resources	Managing resources and providing user access only after verification
Information is secured regardless of location	Least-Privilege, Role Based and Time Based Access
Access to resources on a per-session basis	Keeping a record of who accessed the resources
Access is determined by a dynamic policy	Tracking who accessed the resources
Device and assets are held in the most secure state possible	Critical information should be known only to a set of participants
Authentication and authorization are strictly enforced	Ensuring that people supposed to be doing things are doing them.
Collection of information on current state to improve security	Collection of information and doing persistent and rapid analysis.

All of these policies have been developed based on the principles set forth by NIST. Blockchain features and PUFs have been employed to achieve these policies, thereby establishing a secure perimeter around the supply chain.

1.3.2 Blockchain Technology

Blockchain is a decentralized database and a peer-to-peer network that maintains a registry of transactions [35]. Each block in a blockchain functions like a folder on a computer that contains data, and the collective set of these folders forms the blockchain itself [9]. Blockchain offers several features such as decentralization, immutability, traceability, trust, and transparency [36], [37]. These features have contributed to the widespread adoption of blockchain technology in various fields, including online voting, banking, and the Internet of Things (IoT) [38]. Blockchain can be categorized into different types based on ownership and participant access, namely public, private, and consortium blockchains [39], [40]. For the purpose of this investigation, a consortium blockchain has been utilized [41].

The smart contract serves as the core of the blockchain network and plays a vital role in establishing trust [42]. Despite the term "contract," a smart contract does not possess a legal context but rather functions as a computer program [43]. This code is stored on the blockchain and is assigned a unique address [44]. The involved parties collectively agree upon the terms of the contract. Adhering to the stipulations of the smart contract, any updates made within the blockchain network are considered valid only when a majority of the participating parties reach an agreement. If a consensus is not achieved, the update is deemed invalid and subsequently rejected [45].

Within a blockchain, mathematical algorithms known as consensus algorithms or mechanisms are employed to verify transactions and establish trust among participating parties [46]. Various consensus mechanisms are utilized by different blockchains. However, the proposed blockchain in this work utilizes Proof-of-Authority (PoA) as its consensus mechanism [48].

Leveraging the diverse features provided by blockchain, the proposed work aims to utilize it as a means to achieve a portion of the formulated zero trust policies, specifically in securing the IC supply chain. In this model, all transactions are recorded on the blockchain, ensuring comprehensive tracking of actions and fostering accountability within the network.

1.3.3 Physical Unclonable Functions (PUFs)

A Physical Unclonable Function (PUF) is a hardware security primitive that generates a device-specific digital output based on the unique characteristics of the device [48]. The output, often referred to as a "response," is obtained from the inherent variations in the manufacturing process (MPV). These variations, which occur randomly and remain static, contribute to the uniqueness of the PUF response from one device to another. As a result, the PUF response is highly unpredictable and presents significant obstacles for adversaries attempting to replicate or tamper with the device [49]. As stated by Bhunia et al. in [50], a PUF generates digital fingerprints based on the intrinsic characteristics of a device. It produces distinct digital outputs, known as responses, for a given input or challenge, without revealing any information about their relationship [51], [52]. This implies that a PUF is a function whose output depends not only on the input but also on the specific device executing it [53]. Consequently, even if the same challenge is presented to different devices, the generated responses will be unique to each device, as illustrated in Figure 1-2.

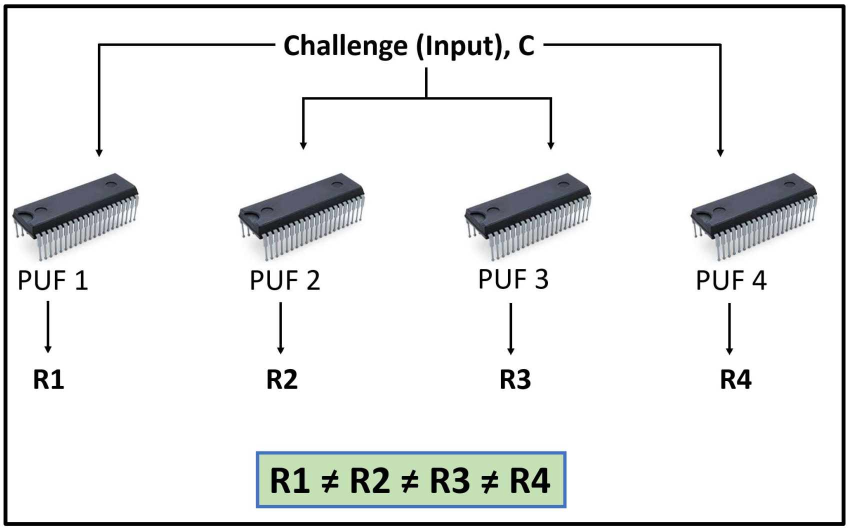


Figure 2-2: PUFs embedded on different devices generating unique responses.

PUFs can be categorized into two groups based on the type of randomness they employ: explicitly introduced randomness and implicitly introduced randomness. This research focuses on utilizing a type of PUF from the latter category known as silicon PUFs to address and fulfill the authentication policies defined for ICs. Further information regarding explicitly introduced PUFs can be found in [54], [55], [56], [48], [52]. Implicitly introduced PUFs, including Arbiter PUFs (APUFs) [57], [58], Butterfly PUFs [59], and Ring Oscillator PUFs, primarily rely on the intrinsic variations in the manufacturing process to generate secret keys. These PUFs leverage the inherent process characteristics of ICs to produce random responses. In this research, a Ring Oscillator PUF is proposed as the chosen PUF type. As part of the initial investigation for the proposed work, a Ring Oscillator PUF has been designed and implemented on an FPGA, which has been utilized for the purpose of authentication.

1.3.3.1 Ring Oscillator Physical Unclonable Function (ROPUF)

The Ring Oscillator PUF, commonly known as ROPUF, is a type of delay-based Physical Unclonable Function (PUF). The fundamental design of the ROPUF relies on delay loops created using an odd number of inverters. In an ROPUF circuit, n- identical Ring Oscillators (ROs) ($\boldsymbol{RO_1\ to\ R0_n}$) are utilized to generate oscillator frequencies within a delay loop. These ROs exhibit unique oscillation behavior, producing distinct frequencies due to variations in the manufacturing process . As a result, when pairs of ROs are mapped to different chip locations, they generate different frequencies, denoted as ($\boldsymbol{f_a\ and\ f_b}$). To select these frequency pairs, a pair of multiplexers is employed, with the PUF challenge serving as the select bits for the multiplexers. By quantitatively comparing these real-valued frequencies ($\boldsymbol{f_a\ and\ f_b}$) using a simple comparison method, a response bit ($\boldsymbol{r_{ab}}$) is generated. The comparison method is as follows:

$$r_{ab} = \begin{cases} 1, & if\ f_a\ >\ f_b\ , \\ 0, & otherwise. \end{cases} \ldots\ldots\ldots\ldots\ldots.(1.1)$$

The architecture proposed in this work for the Ring Oscillator PUF (ROPUF) is a 5-stage ROPUF, consisting of 256 Ring Oscillators (ROs), as depicted in Figure 1-3. Each stage of the ROPUF is determined by the number of inverters within its circuitry. The placement of the 256 ROs within the FPGA is manually mapped using the FPGA Editor tool, ensuring that identical ROs are placed at different spatial locations. Demultiplexers control the selection of these ROs, with the select lines of the demultiplexers also serving as the select lines for the multiplexers. The role of the multiplexers is to choose specific ring oscillators for frequency comparison. Counters connected to the multiplexers measure the frequencies of the selected ring oscillators. The frequency comparison is performed to derive a response bit based on Equation (1.1).

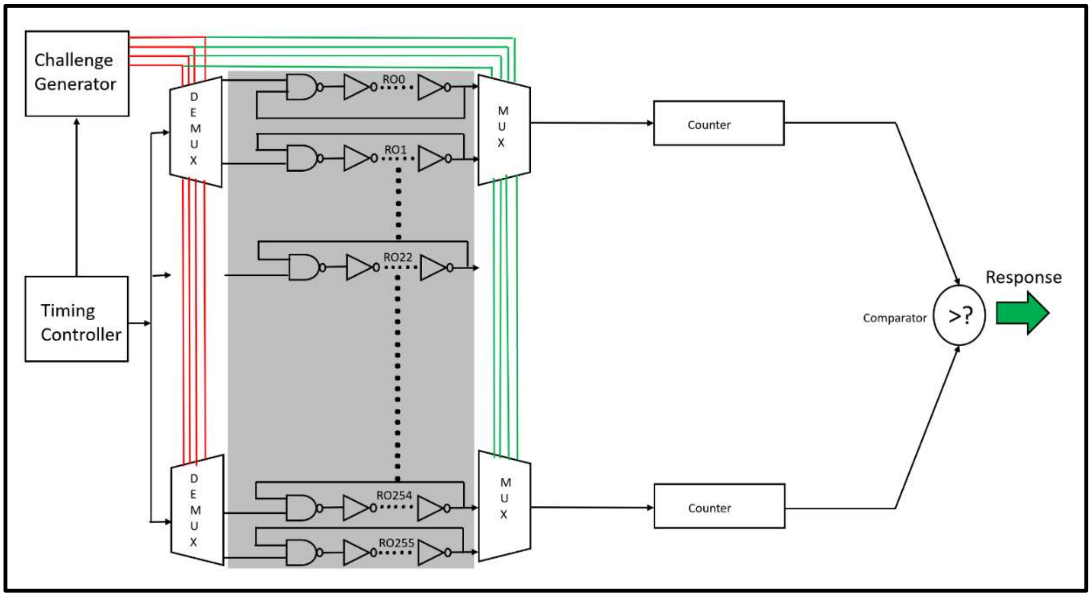


Figure 3-3: Proposed ROPUF architecture.

Figure 1-4 illustrates the floorplan layout of the Ring Oscillator hard macros, taken from the Xilinx FPGA Editor, on four different Configurable Logic Blocks (CLBs). The four ROs are depicted in green, red, purple, and blue colors, with small circles inscribed on them. It is worth noting that the accurate placement of the ROs within the FPGA is crucial for obtaining precise results. In the proposed design, challenges for selecting the ROs are generated by a 10-bit challenge generator. After applying the challenge, the frequency counter is activated for 0.4 ms to measure the frequency response. A 0.1 ms delay is introduced between challenges to select the next RO.

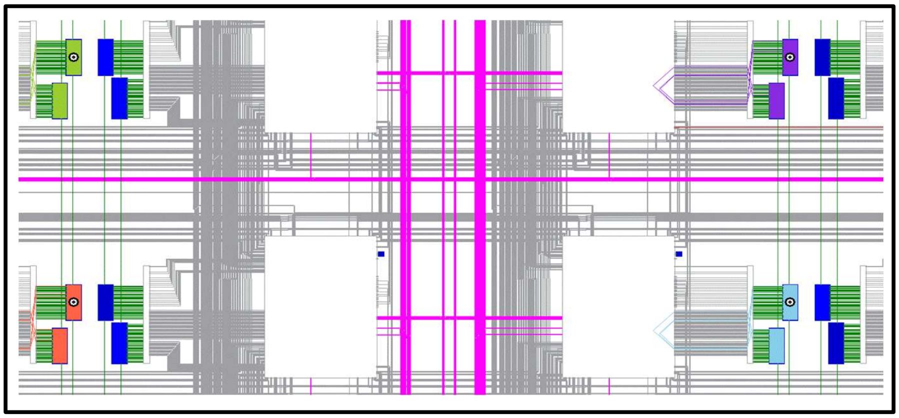


Figure 4-4: Floorplan layout of the RO hard macros on four different CLBs.

1.4 Research Goals

This section discusses the various goals of the dissertation, which encompass designing a zero-trust architecture, developing a blockchain network, and implementing a PUF. These objectives aim to ensure a secure and streamlined process for the IC supply chain, covering all stages from design to fabrication and post-fabrication phases. Furthermore, the dissertation explores the implementation of a foundry-level blockchain through the use of smart contracts for the mask writing process. The application of blockchain technology to enhance the security of hardware IP is also elaborated upon. The research goals of this dissertation are as follows:

- ✓ Design a blockchain network that encompasses the various participants of the semiconductor supply chain, with the aim of enhancing the security of the overall supply chain process.
- ✓ Design and develop smart contracts to ensure the seamless operation of the blockchain network to enhance the efficiency and effectiveness of the blockchain network's functionalities.
- ✓ Design and develop an AI attack-resilient Ring Oscillator Physical Unclonable Function (ROPUF) for robust authenticating the ICs at every stage of the supply chain.
- ✓ Develop a blockchain-enabled network for the post-fabrication supply chain of FPGA to enhance the security and integrity of the FPGA supply chain.
- ✓ Design a blockchain-enabled file storage and transfer system to ensure secure propagation of the design layout file for mitigating the risk of unauthorized access, tampering, or data leakage during the transmission process.
- ✓ Design and develop a Ring Oscillator Physical Unclonable Function (ROPUF) and generate challenge-response pairs for the authentication and validation of integrated circuits (ICs), aligning with the Zero Trust Architecture (ZTA) model.
- ✓ Design and develop a blockchain-enabled Multi-Factor Authentication (MFA) and validation scheme to enhance authentication and validation processes while enforcing access control for users within the supply chain network.
- ✓ Create a blockchain that serves as a shared and distributed ledger for recording transactions within the zero-trust enabled supply chain network to provide a secure and transparent record of all the transactions taking place within the network, ensuring integrity and immutability.

- ✓ Develop a smart contract capable of fetching external data from a distributed file storage system to interact with the distributed file storage system and retrieve specific data as required for seamless access to external data within the blockchain network, enhancing the functionality and versatility of the system.
- ✓ Create a smart contract capable of interacting with external APIs to directly fetch the GDSII layout file in the mask making machine, thereby reducing human interference.
- ✓ Develop and create a smart contract that facilitates the conversion of hardware IPs (Intellectual Property) into Non-Fungible Tokens (NFTs) and assists in their transmission to enable secure and traceable transformation of hardware IPs into unique NFTs, ensuring the authenticity and ownership rights of the IPs.

This dissertation integrates the principles of blockchain technology and Physical Unclonable Functions (PUFs) to fulfill the requirements of a zero trust architecture. Furthermore, it extends the scope to secure hardware IP by utilizing blockchain technology in the form of non-fungible tokens (NFTs), thereby mitigating threats such as theft and piracy. The dissertation not only applies blockchain to enhance the security of the supply chain externally but also focuses on securing the chip from Trojan intrusions by implementing blockchain at the mask writing step of the fabrication process.

Chapter 2

Literature Survey

The use of blockchain technology in the field of assured and trusted microelectronics is currently being widely explored, particularly to uphold and secure the integrity of the IC supply chain. Extensive research has been conducted in various aspects of assured and trusted microelectronics, encompassing the protection of hardware IPs and ensuring supply chain security across design, fabrication, and post-fabrication phases.

Significant research has been conducted to address the threats and protect hardware IP from various risks. In [60], a method is described that utilizes a graph neural network to compare circuit similarities, thereby safeguarding hardware intellectual property. Authors in [61] present a technique for hardware metering that leverages manufacturing variations in integrated circuits. This approach involves locking and disabling the IC through boosted finite state machines (BFSM). The work in [62] proposes a framework utilizing a neural network trained with a confidential key to conceal intellectual property by leveraging the hardware root of trust. Another method described in [63] is the 3D split method, which divides a design into two separate chips, manufactured independently, and then connected through face-to-face integration by vertically stacking them. Authors in [64], review the different IP protection techniques and provide the state-of-the-art advancements in them.

In recent times, there have been attempts to use Non-Fungible Tokens (NFTs) for security purposes [65], [66], [67]. Registering IP patents can be a time-consuming process, often taking up to a year for the application to be processed and the patent details to be publicly disclosed, making them vulnerable to theft. NFTs can help secure the IPs during this period and establish ownership details [65], [66]. Investigation in [67] presents an NFT framework where IoT devices and their users are registered on the blockchain through respective blockchain accounts, which are verified using unique responses from Physical Unclonable Functions (PUFs).

Notable research efforts have been dedicated to the detection and prevention of Trojan-intruded ICs. Various techniques, such as functional verification and side-signal analysis, have been developed to address the issue of Trojan insertion. However, functional verification techniques may not detect all types of Trojans, and side-signal analysis faces challenges in achieving high coverage and extracting abnormal signals from hardware Trojans [68]. In [69], authors present a statistical approach that achieves approximately 85% Trojan detection coverage. However, the risk of Trojan insertion going unnoticed still persists. Another technique for hardware Trojan detection is proposed in [70], but it is effective only for explicit payload Trojans and not for implicit payload Trojans. While there is extensive literature on Trojan detection, prevention of Trojan intrusion remains an unexplored domain. A novel approach to prevent Trojan intrusion is proposed in [68], where the unused spaces in the integrated circuit design are filled to prevent Trojan intrusion. A similar technique is presented in [71], where the empty spaces in the layout are filled with functional cells instead of filler cells. These functional cells are testable to prevent attackers from replacing them with Trojans.

While these methods provide strong defenses against hardware Trojans, new techniques are required to cope with intelligent adversaries and their attacks. In [20], researchers utilize blockchain technology to propose a secure framework for the IC supply chain. However, security against hardware Trojan intrusion is not addressed in this work. The work in [21] offers a solution for using blockchain to improve and secure the integrity of the electronic supply chain. In [9], a smart contract-enabled approach is proposed; however, hardware Trojan intrusion is not explored. Although the use of blockchain technology in hardware security has been extensively investigated, its implementation at the mask writing step remains unexplored.

To mitigate these threats, the concept of zero trust is being explored as a potential solution. The use of blockchain for implementing zero trust is being actively researched and applied in various domains, including healthcare, internet-of-things, and cybersecurity. In the context of the IC supply chain, significant research has been conducted to combat the entry of counterfeit chips. The work presented in [2] highlights the extensive research dedicated to detecting and preventing counterfeit chips using physical techniques. However, these methods may not offer a high level of confidence in addressing the challenges posed by sophisticated counterfeits, as their detection through simple external physical inspection processes can be difficult. In [72], authors conduct a systematic survey of risks associated with the VLSI (Very Large Scale Integration) supply chain, along with corresponding mitigation techniques. This survey provides valuable insights into the risks inherent in the VLSI supply chain and explores potential methods to address them.

Earlier studies focusing on detecting recycled and counterfeit FPGAs are documented in references [73] and [74]. In [73], the authors introduce a novel FPGA reverse engineering toolchain capable of accurately converting FPGA bitstreams into RTL code. This toolchain aids in the detection of hardware Trojans. Authors in [74] present a method specifically designed for detecting recycled FPGAs. However, despite these security techniques, several significant challenges, such as tracking and tracing FPGA chips throughout the supply chain, remain unanswered, and essential solutions are lacking.

To address these challenges and provide solutions, extensive research has been conducted on the integration of blockchain technology. Blockchain has gained significant attention and has been investigated in conjunction with various technologies, including Internet-of-Things (IoT), Zero Trust, and hardware security, to enhance security levels. In [62], authors introduce a blockchain-based architecture specifically designed for IoT, which offers lightweight and decentralized security and privacy features. This architecture leverages the capabilities of blockchain to enhance the security and trustworthiness of IoT systems. In [63], researchers present a comprehensive survey that focuses on the characteristics necessary for successful integration of blockchain with IoT. The survey also discusses the challenges faced during this integration process. Furthermore, the authors propose research questions that have the potential to provide solutions to these challenges. These works highlight the increasing interest in utilizing blockchain technology to enhance security in various domains and provide insights into the potential benefits and challenges of integrating blockchain with IoT systems.

Researchers are actively investigating the application of zero trust in securing supply chains, making it a prominent area of research. In [77], researchers map the zero trust concept to a generic supply chain and outline a research agenda for integrating zero trust with blockchain technology. This fusion has garnered significant attention, and its application has been explored in domains such as healthcare, as demonstrated by researchers in [78]. In [79], authors propose a framework for securing Internet-of-Things (IoT) systems using the principles of zero trust and blockchain. This framework highlights the potential of combining zero trust and blockchain to enhance IoT security. Additionally, [80] discusses the utilization of zero trust and blockchain in the domain of information security, showcasing their applicability and benefits. These works emphasize the ongoing investigation and exploration of zero trust and blockchain in various fields, showcasing their potential to enhance security and resilience in supply chains, healthcare, IoT, and information security.

The research presented in [14] introduces a novel framework aimed at ensuring the confidentiality of electronic designs in a zero trust environment, specifically targeting insider threats. While the framework does not implement the zero trust architecture or model as a complete solution, it proposes various solutions within a zero trust environment at the design and fabrication stages of an IC. Furthermore, in [14], a cloud-based infrastructure is utilized for access control and action logging. However, it is important to note that a cloud-based infrastructure has certain limitations and drawbacks, including centralization and potential vulnerabilities. To overcome these limitations, the use of blockchain technology is suggested as an alternative. Blockchain offers a decentralized storage solution that can enhance security and mitigate the drawbacks associated with centralized storage systems.

Previous literature highlights the potential of blockchain technology in assured and trusted microelectronics. However, its implementation in IP protection and specific steps like mask writing remains unexplored. In this work, a technique is proposed for securing hardware intellectual property, including IP cores and layout files, by utilizing blockchain-enabled non-fungible tokens (NFTs). This technique offers protection against various threats and introduces accountability by recording IP ownership in a decentralized manner facilitated by blockchain technology. Additionally, this work introduces the application of blockchain in the mask writing process to prevent the insertion of Trojan circuits in the layout file, assuming the layout is free from Trojans. By leveraging blockchain technology, this approach aims to enhance security and integrity in the field of microelectronics.

The previous research demonstrates the influential combination of zero trust and blockchain. However, this powerful combination has not yet been extensively explored in the field of assured and trusted microelectronics, leading to prevailing security threats in the IC supply chain that require attention. In addition to blockchain, the proposed work incorporates the use of physical unclonable functions (PUFs) to implement the zero trust architecture (ZTA) for the microelectronics supply chain. This novel approach leverages the convergence of blockchain technology and PUFs to establish a zero trust architecture for securing the semiconductor supply chain. By combining these concepts, the proposed approach aims to enhance the security of the supply chain network by creating a secure boundary around the network. This approach fosters a trustless environment where anything outside the network is not automatically trusted but is verified before entering the network. Similarly, transactions within the network are also subject to verification before being executed. This framework aligns with the principles of zero trust and aims to bolster the security and integrity of the microelectronics supply chain.

Chapter 3

Introducing Blockchain in Semiconductor Supply Chain

In order to reduce the costs of integrated circuit (IC) fabrication, the IC supply chain has expanded globally. However, this globalization introduces risks if the foundry or supply chain involved in the fabrication process is not reliable or trustworthy, potentially compromising the quality of ICs. Instances of counterfeit chips and ICs implanted with Trojans entering the supply chain have been well-documented. To address these challenges, this chapter of the dissertation focuses on strengthening the supply chain process by leveraging blockchain technology, which is widely recognized for its security benefits in various fields. Initially introduced for the security and mining of bitcoins, blockchain has emerged as a trusted security technique in today's world. This chapter proposes an approach that utilizes blockchain technology to ensure the security and trustworthiness of ICs by tracking the potential stage of alteration in the IC supply chain where the chip may have been compromised. By implementing blockchain, the goal is to enhance transparency and traceability throughout the supply chain, allowing for the identification of any potential compromises.

In order to stay competitive in the market, chip manufacturing has increasingly shifted to third-party foundries offshore, leading to reduced fabrication costs [1]. However, this outsourcing of the IC supply chain has also brought about significant concerns regarding the proliferation of counterfeit ICs, thereby raising apprehensions about hardware security [2]. In the modern landscape of IC production, every aspect of the supply chain is outsourced to different entities. For instance, IP cores are sourced from one vendor, while EDA tools are provided by another. The actual fabrication of the IC takes place at a foundry, followed by testing and assembly at an OSAT (Outsourced Semiconductor Assembly and Testing) facility, among other steps. Unfortunately, each step within the supply chain is susceptible to potential attacks or Trojan intrusions. Numerous techniques have been developed to safeguard hardware from such attacks. Ideally, the IC design should undergo thorough simulation and verification before entering the fabrication process. However, obtaining the necessary IP-based designs from third-party vendors can be challenging [5]. Traditional methods of ensuring chip authenticity, such as reverse engineering, are time-consuming and impractical in many scenarios. As a result, novel approaches are needed to address these challenges and enhance the security of the IC supply chain.

3.1 Traditional mitigation techniques

To address the rise in hardware attacks, various techniques have been developed to verify the authenticity of a chip after fabrication. One such method is destructive reverse engineering, as mentioned previously. However, it is important to note that not all chips are tampered with, which limits the practicality of using destructive reverse engineering on a large scale. Testing every single chip using this method is neither feasible nor practical. Another traditional approach involves comparing the functionality of manufactured chips.

However, this technique has its own limitations. Some intruded Trojans may not be constantly active, only triggering under specific pre-defined conditions set by the attacker. Additionally, Trojans can be strategically hidden to evade detection by relatively small sets of testing patterns. Therefore, relying solely on functionality comparison may not be sufficient to identify all types of Trojans [81]. These challenges highlight the need for more sophisticated and comprehensive methods to detect and mitigate hardware attacks, considering the evolving nature of threats in the IC supply chain.

In response to the growing challenges of IC counterfeiting, modern techniques for detecting counterfeit chips have emerged. In the field of hardware security, cryptographic algorithms based on public and private key concepts, as well as specialized structures like Built-in-Self-Test (BIST), have been developed to enhance the security of manufactured chips [82]. Researchers have conducted extensive studies to keep pace with increasingly sophisticated and advanced attacks. However, many of these security-enhancing techniques do not provide a clear indication of the source of the attack or compromise within the supply chain. This creates a need for a robust and secure method to accurately locate the point of compromise or attack. Blockchain technology, with its unique features and advantages, has the potential to address the limitations of traditional techniques and effectively track down the source of attacks. By leveraging blockchain, it becomes possible to establish a transparent and tamper-proof system that can fill the gaps left by conventional approaches and provide valuable insights into the origins of attacks within the IC supply chain.

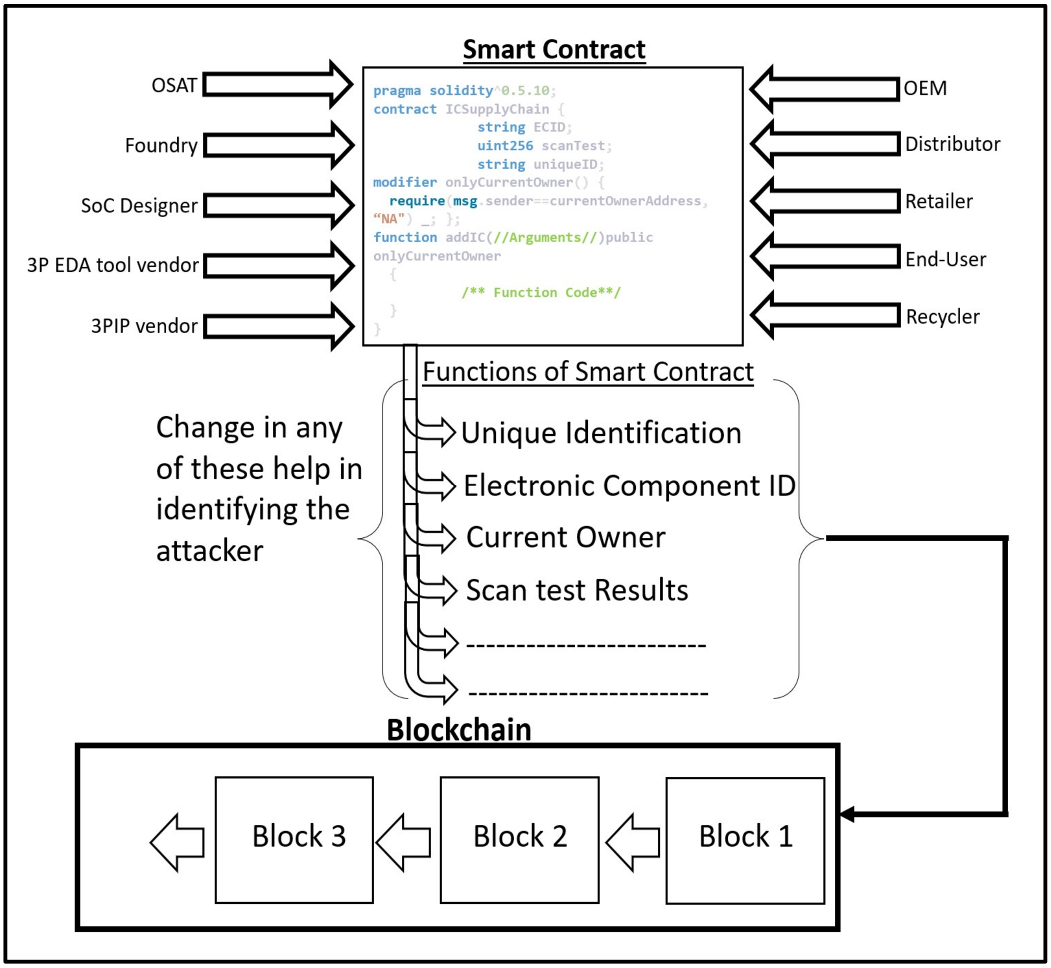
3.2 Proposed Approach

Blockchain technology has gained significant traction and found applications in various domains, including online voting, banking, and supply chain management. In this research, the focus is specifically on leveraging blockchain for the IC supply chain process. The IC supply chain involves multiple entities and stages, and currently, there is a lack of a robust method to track the specific stage in the supply chain where the IC may have been compromised. This gap in traceability poses significant challenges in identifying the source of compromises or attacks within the supply chain. By integrating blockchain technology into the IC supply chain process, it becomes possible to establish a transparent and immutable ledger that records every transaction and event at each stage of the supply chain. This enables better traceability and accountability, allowing for the identification of potential points of compromise. The utilization of blockchain in the IC supply chain aims to enhance the security and integrity of the process by providing a reliable and decentralized system for tracking and monitoring the movement and handling of ICs throughout their lifecycle.

A smart contract is a program that operates on the blockchain, encompassing both program code and a storage file [43]. When all parties or entities involved in the supply chain agree to the terms of the contract, the program code and data are embedded within the smart contract. It is important to note that once recorded, the program code and data stored in the smart contract are immutable, meaning they cannot be modified by anyone at any time. In the event of a typing error, the erroneous record must be re-entered. The entire supply chain operates based on this smart contract, ensuring the integrity of the chip. Each entity updates the smart contract upon successfully completing their assigned tasks. The update is then communicated to all other entities, who must approve the update according to the terms of the contract. Once all entities agree, the update is uploaded onto the blockchain. Every update is timestamped, providing a clear record of the time of the update. In the event that an entity attempts to tamper with the chip's manufacturing process, an error is triggered by the smart contract, notifying the entire network. Furthermore, this alteration attempt is timestamped and stored on the shared ledger, enabling the identification of the responsible party. Smart contracts are interactive in nature, as they can communicate with users and other smart contracts. They execute the code in response to messages received from users or other smart contracts [44].

In this research, the design and requirements of the chip are recorded on the blockchain network. Each entity involved in the supply chain updates the ledger once they have completed their respective tasks. Once updated, the ledger becomes immutable and cannot be modified. Every entity in the supply chain has "read-only" access to the ledger unless they are authorized to make updates or granted special permissions. All parties in the supply chain are responsible for updating the ledger after completing their tasks. This ensures that every participant, from the designer to the end user, is aware of the changes recorded in the ledger. By maintaining a transparent and immutable ledger, the research aims to track and safeguard the chip throughout the manufacturing process and subsequent stages, ensuring its security and authenticity.

The program is developed to conduct chip testing at different stages, evaluating various parameters such as chip components, size, and test results. Several scan tests, including stuck-at tests, at-speed tests, path delay tests, and small-delay defect tests, are performed. It is important to note that the design and outcome of the code are kept confidential, accessible only to the trusted party, which in this case is the design house. Smart contracts play a crucial role in the execution of functions at each stage of the supply chain. Entities involved in the process update the shared ledger with the execution outcomes, which are then uploaded onto the connected blockchain. The proposed approach is illustrated in Figure 3-1, providing a visual representation of the workflow. In summary, the program conducts chip testing, maintains the confidentiality of the design and test outcomes, and uses smart contracts to execute functions and update the shared ledger on the blockchain, ensuring transparency and security throughout the supply chain process.



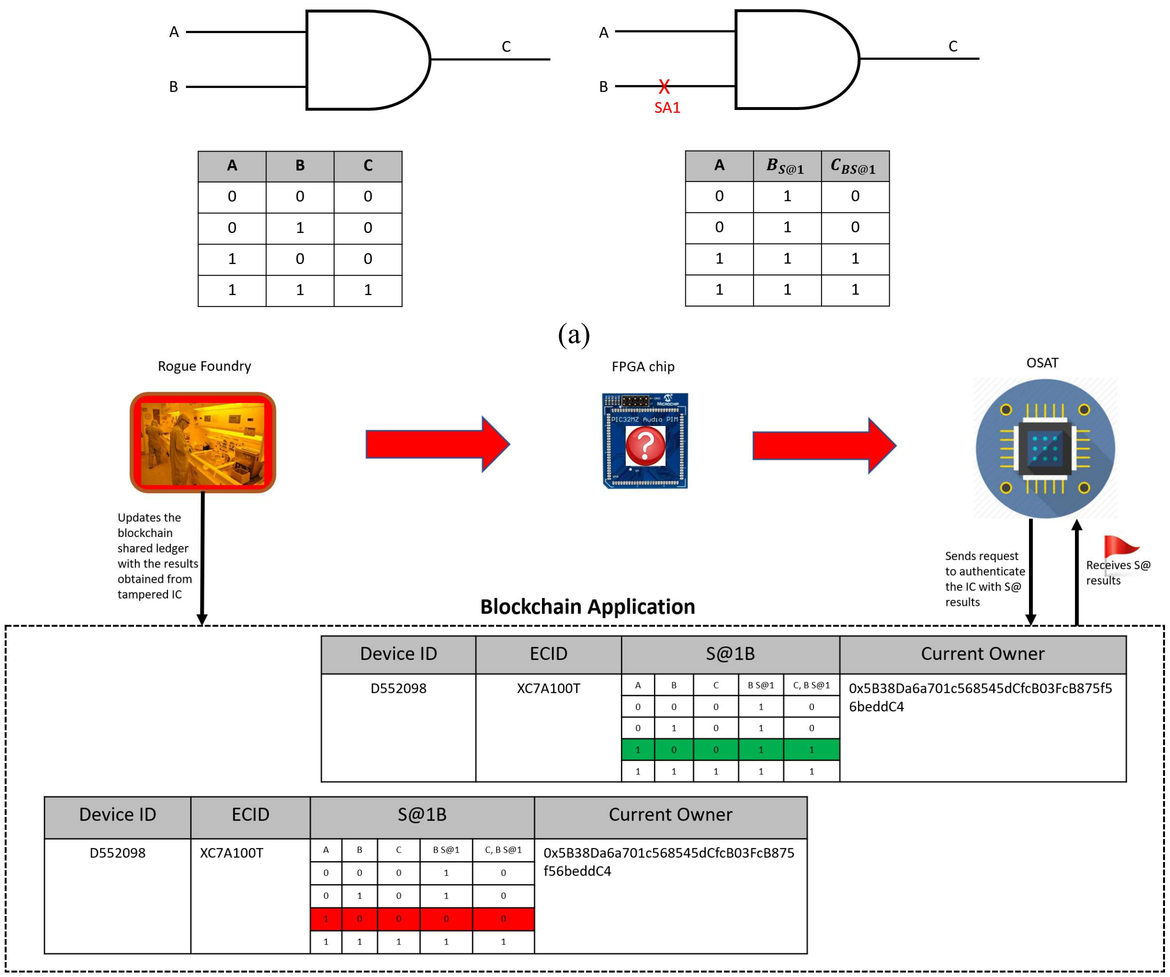
```
pragma solidity^0.5.10;
contract ICSupplyChain {
              string ECID;
              uint256 scanTest;
              string uniqueID;
modifier onlyCurrentOwner() {
  require(msg.sender==currentOwnerAddress,
“NA") _; };
function addIC(//Arguments//)public
onlyCurrentOwner
  {
           /** Function Code**/
  }
}
```

Figure 3-1: Blockchain approach to detect the attacker and the attack

After the execution of the smart contract, any change in the outcome of the program execution is closely monitored and tracked. The pre-defined nature of the program execution allows for the identification and tracking of attacks and attackers. Whenever an entity in the supply chain updates the ledger, all other entities are promptly notified about the change. However, for these changes to be considered valid, they require the agreement of the majority of the parties involved. Once the change has been verified and approved, it becomes immutable and is uploaded onto the blockchain, which is connected to the smart contract. The uploaded updates remain permanently stored on the blockchain and can be accessed and referenced at any point in the future. This capability makes it convenient to trace modifications in the results, facilitating the identification of the exact source of alteration. Furthermore, the timestamp attached to each update or modification provides not only information about the source but also the precise time of the alteration, enhancing transparency and accountability within the supply chain.

3.3 Case Study: detection of guilty party

The proposed model has been implemented through the creation and simulation of a supply chain network, blockchain network, and smart contracts. The supply chain network consists of various participants such as vendors, 3P EDA tool vendor, SoC designer, foundry, OSAT, OEM, distributor, retailer, end-user, and recycler. Each participant is assigned a blockchain address, which serves as their digital identity within the network. The simulation of the network has been conducted and the results indicate smooth functioning of the system, with the ability to detect the guilty party in case of any wrongdoing. A demonstration of the simulation run is presented in Figure 3-2, illustrating the effective operation of the proposed model. To further validate the efficiency of the smart contracts, deliberate forged stuck-at results were recorded by a user with a foundry address. When queried by the OSAT, these forged results raised a red flag, confirming the effectiveness of the proposed technique in detecting and flagging fraudulent activities. Overall, the implementation and simulation of the model have demonstrated its potential to enhance security and accountability within the supply chain network, providing assurance and trust in the IC manufacturing process.


A
B
C
A
B
SA1
C
Rogue Foundry
FPGA chip
OSAT
Updates the blockchain shared ledger with the results obtained from tampered IC
Sends request to authenticate the IC with S@ results
Receives S@ results
Blockchain Application

A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

A	$B_{S@1}$	$C_{BS@1}$
0	1	0
0	1	0
1	1	1
1	1	1

(a)

Device ID	ECID	S@1B					Current Owner
D552098	XC7A100T	A	B	C	B S@1	C, B S@1	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
		0	0	0	1	0	
		0	1	0	1	0	
		1	0	0	1	1	
		1	1	1	1	1	

Device ID	ECID	S@1B					Current Owner
D552098	XC7A100T	A	B	C	B S@1	C, B S@1	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
		0	0	0	1	0	
		0	1	0	1	0	
		1	0	0	0	0	
		1	1	1	1	1	

(b)

Figure 3-2: (a) Stuck-at fault representation. (b) Pictorial representation of the simulated results

3.4 Summary

The chapter focuses on addressing the critical concerns of hardware security and trust in the IC supply chain. To achieve this, the utilization of blockchain technology is proposed, leveraging its robust security features that have been successfully implemented in various domains like online voting, banking, and IoT. The chapter presents an approach that applies blockchain technology to enhance the security and trust in the semiconductor manufacturing supply chain process. A key component of this approach is the development of a smart contract that outlines the chip's design specifications to be manufactured. This smart contract is deployed and shared among all participants in the supply chain. When interacting with the smart contract, each participant inputs the results obtained from their specific task, which are then recorded and uploaded onto a shared ledger. This enables the tracking of any compromises or malicious activities introduced by third parties in the supply chain. By examining the recorded data and timestamps, the identity of the guilty party can be determined, along with the exact time of the intrusion. By incorporating blockchain technology and the use of smart contracts, this approach aims to establish a more secure and trustworthy environment within the IC supply chain. It provides a mechanism for detecting and identifying potential compromises in the chip's design, ensuring accountability and enhancing overall security measures.

Chapter 4

ROPUF & Blockchain: A way to secure FPGA supply chain

Due to the growing demand for Field Programmable Gate Arrays (FPGAs) in various applications, the issue of counterfeit and recycled FPGAs infiltrating the FPGA supply chain has become more prevalent. This problem has been exacerbated by recent disruptions in the global semiconductor chip supply chain. Counterfeit and recycled FPGAs are unreliable and can lead to failures in critical infrastructures where they are deployed. Additionally, they are susceptible to security threats such as hardware Trojan insertion and aging, further compromising their integrity. This chapter introduces a technique that utilizes physical unclonable functions (PUFs) and blockchain technology to secure the post-fabrication FPGA supply chain and mitigate these challenges. A detailed case study with simulation results is provided to illustrate the effectiveness of this technique. The simulations were conducted using Ganache, a personal blockchain provided by the Truffle framework. While the primary focus of this chapter is on protecting the post-fabrication supply chain, it is worth noting that this technique can be extended to encompass both the pre and post-fabrication stages. By implementing this approach, users can not only verify the authenticity of FPGAs but also identify the responsible party within the supply chain for any untrustworthy actions or compromises. Overall, the proposed technique offers a reliable solution to enhance the security and trustworthiness of the FPGA supply chain, ensuring the integrity of the FPGAs and safeguarding critical systems against potential threats.

4.1 Background: FPGAs, threats, and countermeasures

Field Programmable Gate Arrays (FPGAs) have gained widespread usage in various sectors, including rapid prototyping, aerospace systems, the military, artificial intelligence, and more [83], [84]. However, with the increasing demand and recent supply chain disruptions, the infiltration of counterfeit and recycled FPGAs has become a concerning issue in the industry [85], [86]. Counterfeit FPGAs have particularly emerged as one of the top counterfeited electronic components due to the presence of recycled FPGAs in the FPGA supply chain [2]. The use of such devices not only raises concerns about reliability but also introduces significant security threats to cyber-physical systems. The presence of counterfeit and recycled FPGAs in the supply chain poses several security risks, including hardware Trojan insertion, bitstream modification, fault injection, and more [87], [88], [89], [90], [91]. These malicious activities can have detrimental consequences, leading to compromised system security, financial losses for FPGA vendors, and negative impacts on the parties involved in the FPGA supply chain. It is crucial to address these issues and develop robust techniques to secure the FPGA supply chain, ensuring the authenticity and reliability of FPGAs.

To address hardware security threats in FPGA devices, Physical Unclonable Functions (PUFs) have emerged as a promising approach. While PUFs are typically embedded on Application Specific Integrated Circuits (ASICs) during fabrication, they can also be implemented on FPGAs after the fabrication process. During the manufacturing of integrated circuits, random variations occur due to factors such as imprecise control of oxide thickness, mask variations, and process temperature and pressure, leading to what is known as Manufacturing Process Variation (MPV) [92], [93]. This process variation is inherent to each individual IC, causing variations in chip characteristics even among chips of the same class and manufactured from the same wafer. By leveraging the process variation, PUFs can be designed to generate unique challenge-response pairs for each chip [94], [95]. Among the various PUF designs, the Ring Oscillator Physical Unclonable Function (ROPUF) is particularly suitable for FPGA implementation as it does not require mirror symmetry [96]. Since FPGAs are reprogrammable, ROPUFs can be easily designed and implemented on FPGAs to generate unique challenge-response pairs, further enhancing their security and authenticity.

In recent years, there have been attempts to leverage blockchain technology in the domain of hardware security [85], [97], [20], [21], [98], and [9]. Blockchain, known for its decentralized database and peer-to-peer network, has gained popularity through its use in the development of cryptocurrencies [35]. It offers various features such as decentralization, immutability, traceability, trust, and transparency [37], [38]. As a result, blockchain has found applications in diverse fields including online voting, banking, and the Internet of Things (IoT) [38]. Blockchain can be categorized into different types based on ownership and access, such as public, private, and consortium blockchains [99]. In this investigation, a consortium blockchain has been utilized [39], [40]. This chapter presents a technique that focuses on securing the post fabrication FPGA supply chain by combining consortium blockchain technology with Ring Oscillator Physical Unclonable Functions

(ROPUFs) [94], [40], [41]. The proposed technique not only enables the identification of counterfeit or recycled FPGAs but also introduces accountability by tracing the responsible party involved in the infiltration of such devices into the supply chain.

4.2 FPGA post-fabrication supply chain

It is important to note that the manufacturing cycle for FPGAs and ASICs differs, as the application design in FPGAs can be mapped post fabrication [100]. The supply chain model for FPGAs can be divided into two stages: pre-foundry fabrication and post-foundry fabrication, as shown in Figure 4-1. Among these stages, the Outsourced Semiconductor Assembly and Test (OSAT) stage is considered the most vulnerable [101]. However, in the proposed model, we assume the foundry to be trusted, as reputable FPGA manufacturers like Xilinx work with highly reliable and trusted foundries such as TSMC and Samsung. In the post-fabrication stage, FPGAs are received by the OSAT, where they undergo assembly, packaging, and testing before being sent to third-party integrators (3P Integrator). From there, the FPGAs may be received by distributors, either as individual units or assembled on printed circuit boards with other peripherals. Retailers purchase FPGAs from distributors and sell them to end users. In some cases, the original vendors may obtain FPGAs directly from 3P integrators or OSAT vendors and, after conducting their own testing procedures, ship them directly to the distributors. The CRPs and other device features are obtained by the original vendor from the trusted foundry and recorded in the blockchain. During the post-fabrication stage, there is a possibility that a party within the supply chain may introduce recycled or counterfeit FPGAs. For instance, a retailer might supply recycled or counterfeit FPGAs to customers. Therefore, maintaining the security of the supply chain is crucial to prevent the distribution of counterfeit or recycled FPGAs to end users.

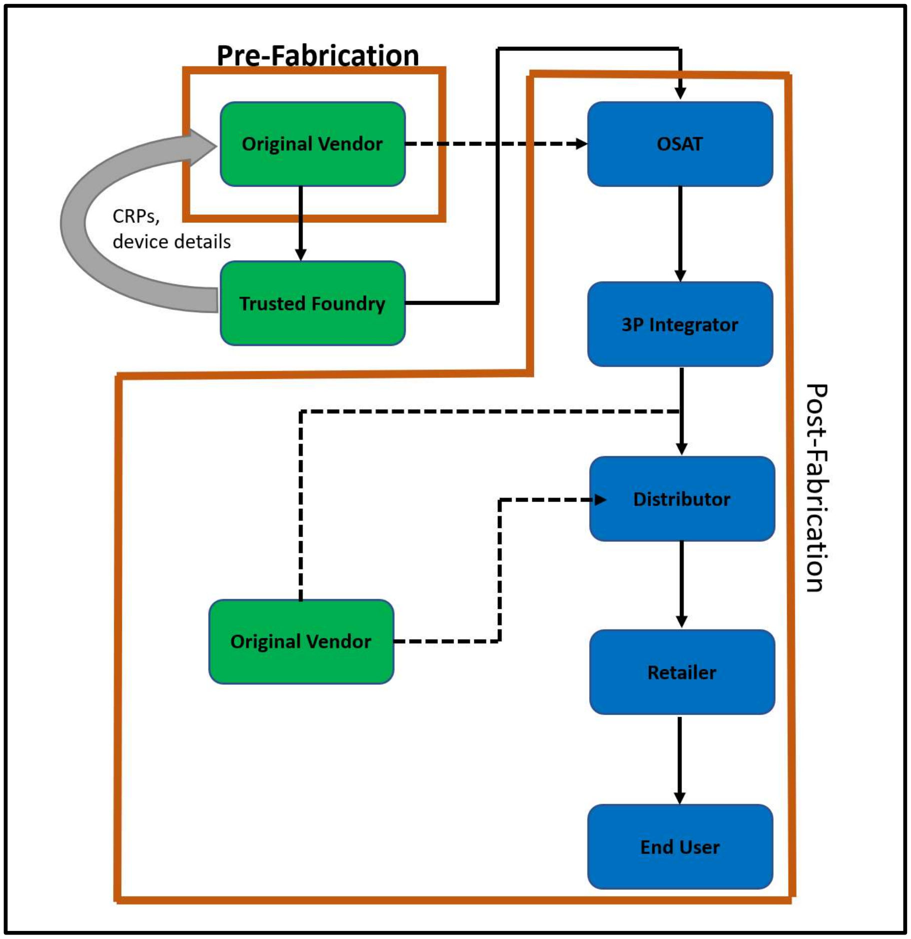


Figure 4-1: A typical FPGA post-fabrication supply chain

4.3 Countermeasure steps

To ensure the security of the transfer mechanism of the FPGAs to different parties, the following steps have been proposed:

4.3.1 ROPUF design and implementation

In this step, a Ring Oscillator Physical Unclonable Function (ROPUF) is specifically designed for the FPGA. The Challenge-Response Pairs (CRPs) obtained from the FPGA at the trusted foundry are provided to the original vendor and securely stored in the blockchain. Additionally, the bitstream file, which contains the programming information for the FPGA, is uploaded to a blockchain file storage system called the Interplanetary File System (IPFS) [102] by the original vendor.

4.3.2 Design and deployment of smart contract

After the implementation of the ROPUF, a smart contract is developed and deployed on the blockchain with the following features (functions)–

(i) Device Registration: *addFPGA()*

(ii) Device Status: *FPGAStatus()*

(iii) Transfer Ownership *transferOwnership()*

(iv) Accept Ownership: *acceptOwnership()*

(v) Authenticate FPGA: *authenticateFPGA()*

(vi) Check Provenance: *checkFPGAProvenance()*

4.3.3 Accessing the information from blockchain

To authenticate the FPGA, the configuration bit file for the device is downloaded, and the authentication scheme guides the process of providing challenges to the FPGA. The FPGA then generates responses corresponding to those challenges, and the user verifies these responses by comparing them with the pre-stored responses in the blockchain. This comparison ensures the authenticity and integrity of the FPGA.

4.3.4 Secure transfer of ownership

When a user wishes to transfer ownership of an FPGA to another party, this transaction is conducted on the blockchain. It involves providing the blockchain addresses of both parties involved and the secret key of the current owner. However, the ownership transfer is not finalized until the new owner accepts the ownership. Once the new owner accepts the ownership, the transaction is completed, and the FPGA is successfully transferred to the new owner, ensuring a secure and transparent transfer process.

4.3.5 Track and trace the FPGA

If an FPGA owner desires to access the historical information of the device, they can retrieve this data from the blockchain. This functionality allows the owner to obtain detailed information about all previous owners of the FPGA, as well as the provenance or origin of the device. By accessing this information from the blockchain, the owner can have a comprehensive understanding of the FPGA's ownership history, providing transparency and traceability to the supply chain process.

4.4 Case study: Design and implementation

This section discusses a case study to demonstrate the efficiency of the proposed approach:

4.4.1 Implementation of ROPUF

Figure 4-2 illustrates a higher-level schematic of the Ring Oscillator Physical Unclonable Function (ROPUF) design utilized in this specific case study. The ROPUF design exhibits exceptional performance metrics, as documented in [94], [103]. For this design, Xilinx Artix 7 FPGAs are employed and mounted on Digilent Nexys 4 boards. The ROPUF operates by taking a 16-bit challenge as input and generating a corresponding 16-bit response. To implement the ROPUF, the ring oscillators are strategically placed on the FPGA using the Xilinx Design Constraints (XDC) macro in the Vivado tool. The responses generated by the ROPUF are collected from the Logic Analyzer. Notably, a total of 256 oscillators are positioned on the FPGA to facilitate the ROPUF operation.

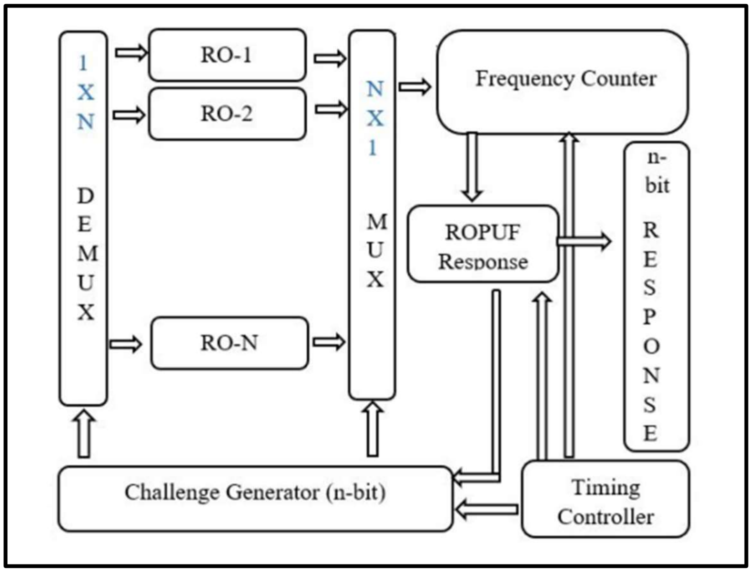


Figure 4-2: Block diagram of ROPUF to generate an n-bit response for an n-bit challenge

The ROPUF design remains consistent across all FPGA boards, with the only difference being the constraint file, which is specific to each board. The modification required involves changing the XDC constraint file according to the particular board. In this case study, the ROPUFs are implemented on four different Nexys 4 boards. For each FPGA board, a total of 30,000 Challenge-Response Pairs (CRPs) are generated by the ROPUF. Table 4.1 provides a few examples of the actual CRPs generated during the study.

Table 4.1: A sample CRP set from a data set of *30,000* CRPs

FPGA ID	Sample Challenges	Sample Responses
D552220	0111011101110001	1000000000110101
D552222	0101011101110001	1010111000000010
D552224	1101011101110001	1010011001010001
D552226	0001011101110001	0001001010101110
D552228	1011100010010000	1010111011111110
D552230	1010100111000010	1101111101100001
D552232	0101010101110101	0111111101100001
D552234	1111011101010000	0001000011110000
D552236	0010100000011110	1110111000011110
D552238	1010101000001010	0101010001111101

4.4.2 Design of smart contract – Pseudocodes

The smart contract developed for the proposed blockchain network includes several functions, which are presented as pseudocode in this subsection. These pseudocode snippets collectively form the complete smart contract, as depicted in Figure 4-3.

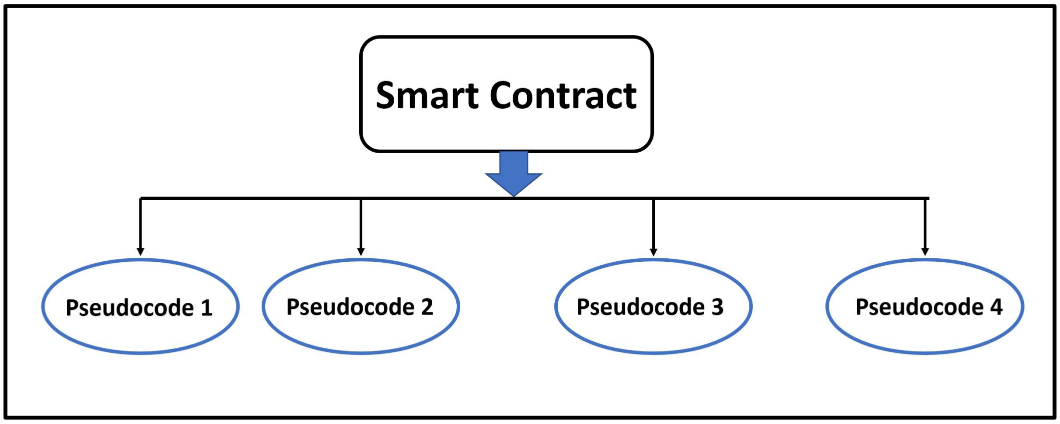


Figure 4-3: Representation of pseudocodes as part of the smart contract

4.4.2.1 Registration of the FPGA

For registering the FPGA in the blockchain, the following device features, as shown in Table 4.2, are entered. The registration process is shown in Pseudocode 4.1.

Table 4.2: FPGA specification as registered on the blockchain

Device ID	D552098	
FPGA Type	Artix 7	
ECID	XC7A100T	
CRP (Sample)	C	0111011101110001
	R	1000000000110101
Date Manufactured	11/02/2020	
Current Owner	0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db	
Vendor Name	Xilinx	
Bitstream File Hash	QmQJLbHi6yhd1nZTujgWhyiGWK3WSL4DE6BdBuN9puYQAf	

Pseudocode 4.1: Registration of FPGA

```
function addFPGA (registerAddress, key){
  if (registererAddress()=vendorAddress()) then
    if (key=vendorPrivateKey) then
    //add the FPGA to the blockchain
else - error message: "Private Key does not match"
    end if
else – error message: "User does not have permission"
  end if
```

4.4.2.2 Transfer of ownership of the FPGA

After the registration of the FPGA, it is transferred to the next party in the supply chain, by calling *transferFPGA()* function of the smart contract as shown in Pseudocode 4.2.

Pseudocode 4.2: Transfer of Ownership

```
function transferOwnership(currentAddress, newAddress){
  if (currentAddress = currentOwnerAddress) then
    if(newAddress()=newOwnerAddress()) then
      //Initiate FPGA Transfer
else -  error message : "New Owner does not exist"
    end if
else – error message : "Private Key does not match"
   end if
```

4.4.2.3 FPGA Authentication

For the new owner to authenticate the FPGA, the function *authenticateFPGA()* is executed as depicted in Pseudocode 4.3.

Pseudocode 4.3: FPGA Authentication

```
function authenticateFPGA(ECID, participantAddress, key, CRPs){
  if (ECID = ECID) then
    if(address()=participantAddress()) then
      if(key = participantPrivateKey()) then
        if(CRPs = challenge_response_pairs) then
```

```
            return authenticFPGA
else -  error message : "CRPs do not match"
        end if
else – error message : "Private Key does not match"
        end if
else -  error message : "User does not exist"
        end if
else -  error message : "No FPGA exist"
        end if
```

4.4.2.4 FPGA provenance

For any participant of the network, to check the provenance of the FPGA, the function *checkFPGAProvenance()* represented in Pseudocode 4.4 is executed.

Pseudocode 4.4: FPGA Provenance

```
function checkFPGAProvenance(ECID){
    if (enquirerAddress() = participantAddress()) then
        if(key = enquirerPrivateKey()) then
            if(ECID = ECID) then
                return FPGAProvenance
else -  error message : " No FPGA exist "
        end if
else – error message : "Private Key does not match"
        end if
else -  error message : "User does not have permission"
```

```
end if
```

Pseudocodes 3 and 4 assist in finding the guilty party as the authentication details and the ownership history are stored in the blockchain shared ledger.

4.5 Case study: security threat evaluation

In this section, the simulation results are presented, and the security threats are evaluated by comparing two scenarios: (a) a genuine OSAT and (b) an OSAT assumed to be an adversary. The proposed technique and algorithms have been simulated using the Ganache blockchain provided by the Truffle framework. The smart contract is implemented based on the pseudocodes discussed in Section 4.4. While any stage in the pipeline can be considered an untrusted entity, we begin the case study by initially determining the authenticity of the OSAT.

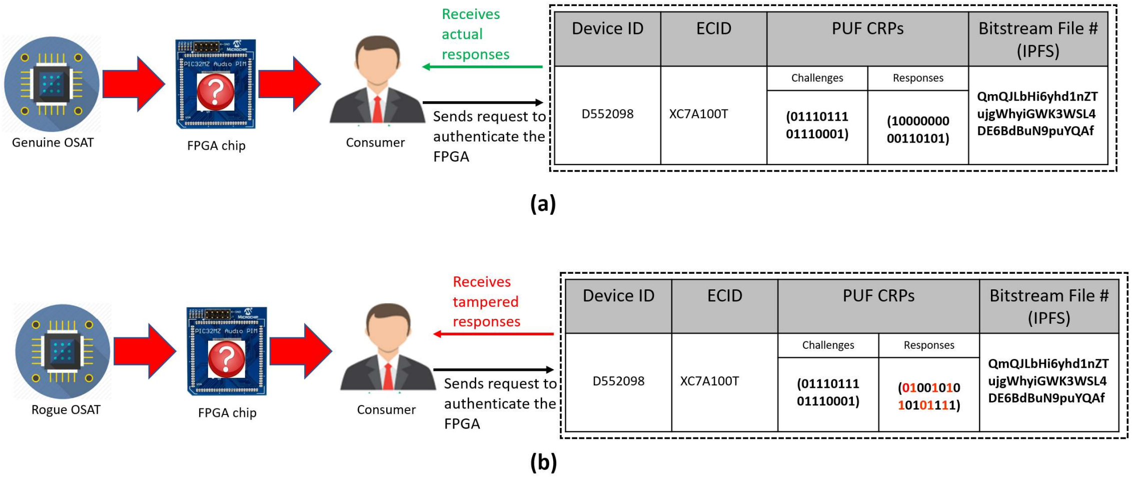
4.5.1 Genuine OSAT

Once the ownership of the FPGA is accepted, the OSAT assumes the responsibility of maintaining the authenticity of the device. In the case of a legitimate OSAT, there is no tampering with the FPGA or the bitstream file. The blockchain ledger is updated with genuine FPGA-specific information as per the blockchain application. Upon updating the blockchain ledger, the OSAT invokes the transferOwnership() function, providing the necessary arguments, and the FPGA is subsequently transferred to the consumer who is deemed genuine, after passing through various participants. To authenticate the FPGA, the genuine consumer interacts with the smart contract and calls the authenticateFPGA()

function. The smart contract retrieves the authentic FPGA data registered on the blockchain by the trusted original vendor and returns it to the consumer. The data retrieved from the OSAT shows no discrepancies in comparison to the data uploaded by the OSAT, thereby confirming the authenticity of the OSAT as a genuine participant. This scenario is illustrated in Figure 4-4 (a).

4.5.2 Rogue OSAT

In this scenario, similar to the previous one, the ownership of the FPGA is transferred from the original vendor to the OSAT. However, in this case, the OSAT is considered to be an adversary and an untrusted entity. The FPGA is assumed to be tampered with by the OSAT during the manufacturing process. After going through the various stages of the supply chain as depicted in Figure 4-1, the tampered FPGA reaches the consumer. The consumer interacts with the smart contract to verify the authenticity of the FPGA. The device specifications retrieved from the blockchain are compared with the original device specifications uploaded by the vendor. Due to the tampering carried out by the OSAT, the two sets of information do not match. In Figure 4-4 (b), some of the CRP response bits are highlighted in red to indicate the tampering performed by the OSAT. It is important to note that among all the device specifications shown in Figure 4-4, the CRPs are the most crucial as they cannot be forged. The CRPs are unique for each FPGA and must be physically generated by each owner to authenticate the device. In our case study, we were able to identify all genuine and tampered FPGAs by generating the actual 16-bit responses from the provided 16-bit challenges stored in the blockchain.


Genuine OSAT
FPGA chip
Consumer
Receives actual responses
Sends request to authenticate the FPGA

Device ID	ECID	PUF CRPs		Bitstream File # (IPFS)
		Challenges	Responses	
D552098	XC7A100T	**(01110111 01110001)**	**(10000000 00110101)**	**QmQJLbHi6yhd1nZTujgWhyiGWK3WSL4DE6BdBuN9puYQAf**

(a)

Rogue OSAT
FPGA chip
Consumer
Receives tampered responses
Sends request to authenticate the FPGA

Device ID	ECID	PUF CRPs		Bitstream File # (IPFS)
		Challenges	Responses	
D552098	XC7A100T	**(01110111 01110001)**	**(01001010 10101111)**	**QmQJLbHi6yhd1nZTujgWhyiGWK3WSL4DE6BdBuN9puYQAf**

(b)

Figure 4-4: Simulated security evaluation of the presented technique (a) genuine participant (b) adversary in the network

4.6 Summary

In this chapter, a technique that combines the use of ROPUFs and blockchain technology to enhance the security of the post-fabrication FPGA supply chain is introduced. By leveraging the unique CRPs generated by ROPUFs, along with the storage of ownership history and device features on the blockchain, a mechanism to verify the authenticity of FPGAs as they move through the supply chain is established. At each stage of the supply chain, the parties involved can verify the device information stored in the blockchain to ensure its integrity. This process allows for the detection of any malicious activities or tampering that may occur during the FPGA's journey from one owner to another. By tracing the ownership history and cross-referencing it with the stored information, any discrepancies or unauthorized modifications can be identified, enabling the identification of the guilty party. The effectiveness of this technique is demonstrated through a case study, which showcased the ability to detect tampered FPGAs by comparing the device specifications retrieved from the blockchain with the original specifications. The technique primarily focuses on the post-fabrication stage, where the supply chain is most vulnerable. However, it can be extended to cover the entire supply chain if necessary. It is worth noting that extending the technique to the entire supply chain may introduce additional steps and computational overhead and is typically warranted in cases where the trustworthiness of the foundry or the existence of internal threats is in question.

Chapter 5

Enabling blockchain in semiconductor supply chain

The FPGA supply chain has been plagued by various challenges, including IP theft, hardware Trojan intrusion, and bitstream modification. To address these issues and ensure the integrity of the supply chain, this work combines the use of blockchain technology and hardware-oriented security primitives such as physical unclonable functions (PUFs). Blockchain technology is employed to establish trust and enable the tracking and tracing of ownership for assets like IP cores, EDA tools, FPGAs, and bitstreams within the supply chain. By leveraging the decentralized and immutable nature of the blockchain, the integrity of these assets can be safeguarded. PUFs serve as the Root-of-Trust (RoT) for authenticating the FPGAs. These unique hardware-based primitives generate challenge-response pairs that are used to verify the authenticity of the devices. By incorporating PUFs into the supply chain, the risk of counterfeit or tampered FPGAs can be mitigated.

Furthermore, this chapter introduces a blockchain-powered file storage and transfer system that is integrated into the split manufacturing flow. This enables secure and tamper-proof storage and transfer of FPGA-related files throughout the supply chain process. Additionally, a remote chip activation technique is presented, which allows for the secure activation of FPGAs in a remote manner. This technique ensures that only authorized entities can activate the FPGAs, further enhancing the security of the supply chain.

To evaluate the performance of the blockchain network, a simulation is conducted using the Ganache user interface provided by the Truffle framework. The simulation considers different block times (60, 120, and 180 seconds) and measures the transactions per second (TPS) and latency of the blockchain. The simulation is performed on Xilinx Artix-7 FPGAs mounted on Nexys-4 Digilent boards, providing practical insights into the feasibility and effectiveness of the proposed approach in real-world scenarios.

5.1 Blockchain-enabled file storage and transfer system

To combat IP theft and piracy, as well as ensure the security of bitstream files, this research proposes a blockchain-enabled file storage and transfer system. The system aims to securely store and transfer layout files and bitstream files between participants. In this work, the Inter Planetary File Storage (IPFS) application of blockchain is utilized for storing the bitstream file [102]. IPFS operates as a blockchain-based peer-to-peer file storage system, assigning a unique hash to each uploaded file [104]. Notably, this hash changes with each modified version of the file [102].

This technique is an eleven step protocol represented in Figure 5-1. The steps are as follows:

1.) The sender uploads the file on to the IPFS application.

2.) The IPFS system generates a hash of the file and returns it to the sender.

3.) The sender registers the corresponding hash onto the blockchain shared ledger.

4.) The recipient requests the unique ID of the file.

5.) The sender sends the unique ID of the file to the recipient.

6.) The sender calls the *transferFile()* function from the smart contract.

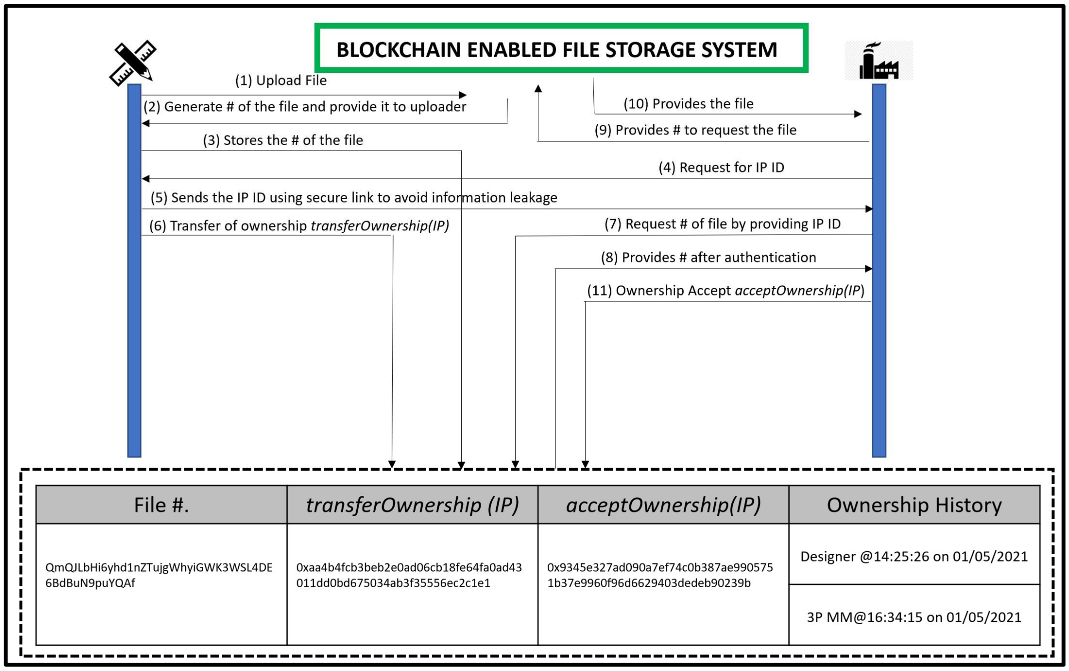
7.) Requests the blockchain the hash of the file using the corresponding unique ID.

8.) The blockchain application (after verification) provides the hash.

9.) Provides the hash to the IPFS application to fetch the file.

10.) The IPFS application (after verification) provides the file corresponding to the provided hash.

11.) The recipient calls the *acceptFile()* function from the smart contract.


BLOCKCHAIN ENABLED FILE STORAGE SYSTEM
(1) Upload File
(2) Generate # of the file and provide it to uploader
(3) Stores the # of the file
(4) Request for IP ID
(5) Sends the IP ID using secure link to avoid information leakage
(6) Transfer of ownership *transferOwnership(IP)*
(7) Request # of file by providing IP ID
(8) Provides # after authentication
(9) Provides # to request the file
(10) Provides the file
(11) Ownership Accept *acceptOwnership(IP)*

File #.	*transferOwnership (IP)*	*acceptOwnership(IP)*	Ownership History
QmQJLbHi6yhd1nZTujgWhyiGWK3WSL4DE6BdBuN9puYQAf	0xaa4b4fcb3beb2e0ad06cb18fe64fa0ad43011dd0bd675034ab3f35556ec2c1e1	0x9345e327ad090a7ef74c0b387ae9905751b37e9960f96d6629403dedeb90239b	Designer @14:25:26 on 01/05/2021
			3P MM@16:34:15 on 01/05/2021

Figure 5-1: Blockchain-enabled file storage and transfer system

All these eleven transactions are recorded on the blockchain shared ledger with timestamps in case any discrepancy is detected later.

5.2 Blockchain-enabled split manufacturing

Several techniques have been developed to address the issue of IC tampering during the untrusted foundry stage. One notable technique is split manufacturing, which has proven to be a crucial approach for minimizing IP risks and reducing production costs [105], [106].

In split manufacturing, the IC circuit is divided into two distinct parts prior to fabrication. The Front End of the Line (FEOL) comprises transistors and some routing wires, while the remaining routing wires are included in the Back End of the Line (BEOL) [24], [107]. As shown in Figure 5-2, the FEOL is fabricated at a high-end foundry that may not be trusted, while the BEOL is fabricated at a low-end trusted foundry [108].

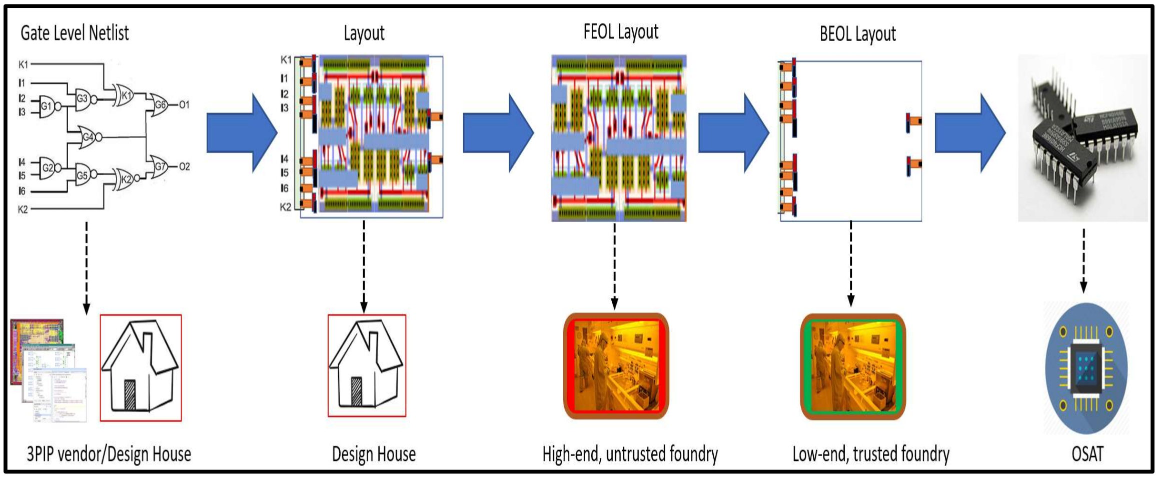
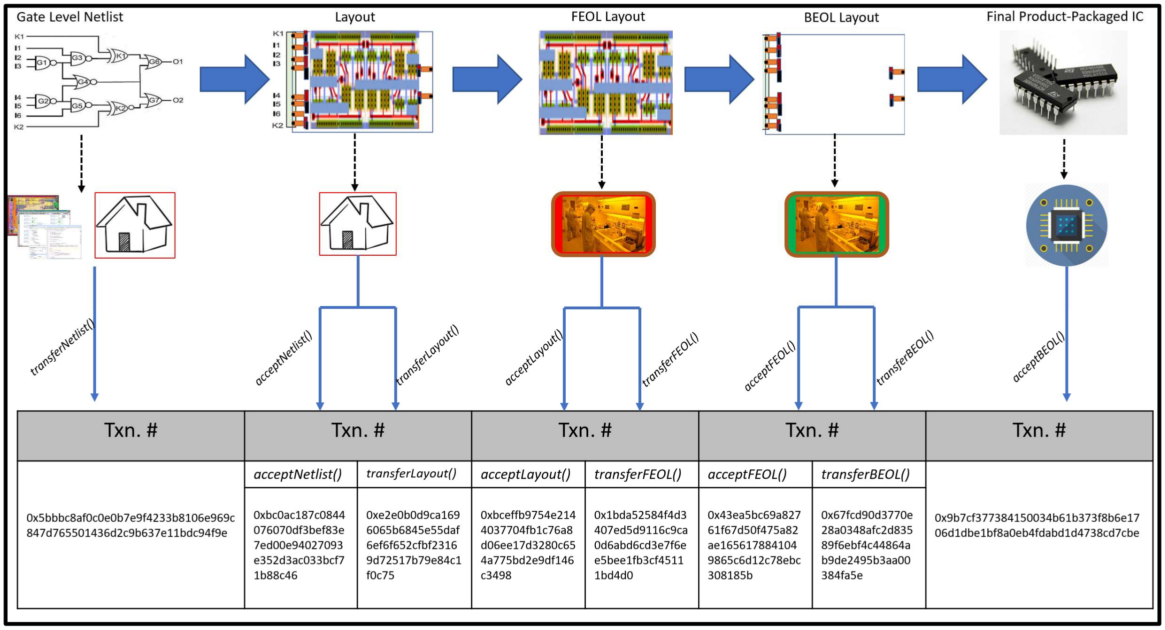


Figure 5-2: A split manufacturing process flow

In the context of split manufacturing, where two foundries are involved in the fabrication process (one for BEOL and the other for FEOL), this chapter introduces a blockchain-enabled split manufacturing technique. In the traditional approach, the design house sends parts of the layout file, typically in GDSII or OASIS format, to both foundries for their respective fabrication stages. In this work, the proposed framework suggests implementing a blockchain network at this stage of the process.

Each participant involved in the split manufacturing process, including the 3PIP vendor, design house, FEOL foundry, BEOL foundry, and OSAT, contributes to the shared blockchain ledger by uploading their respective assets (such as netlist, layout, FEOL fabricated part, BEOL fabricated part of the FPGA) and accepting the assets transferred to them. The smart contract is designed with functions to facilitate these transactions, such as *transferNetlist(), acceptNetlist(), transferLayout(), acceptLayout(), transferFEOL(), acceptFEOL(), transferBEOL(),* and *acceptBEOL()*. After the transfer and acceptance of assets, each participant invokes the corresponding function in the smart contract. The smart contract executes the function and returns transaction hashes containing all the relevant information about the transactions. The blockchain-enabled split manufacturing technique is illustrated in Figure 5-3.



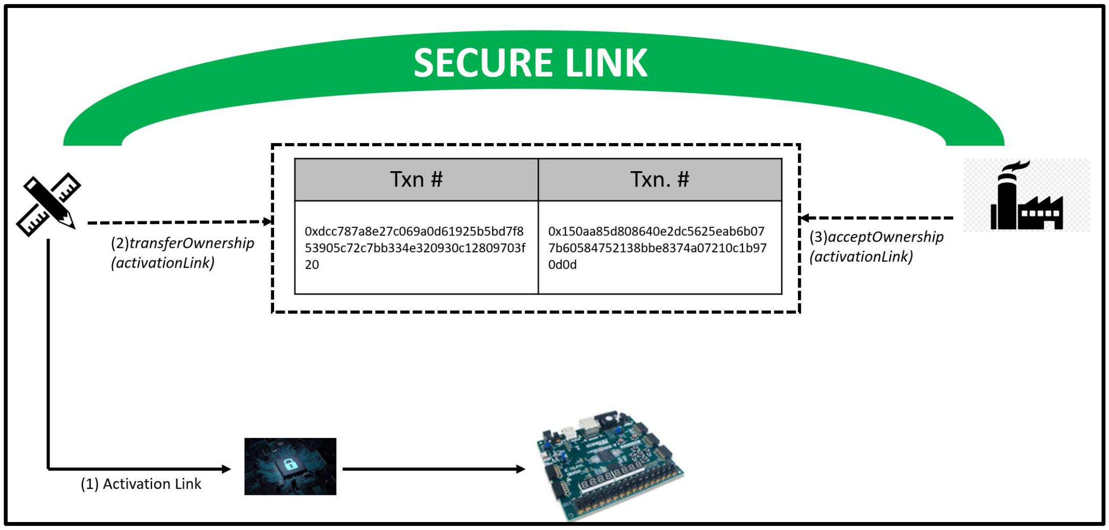
Txn. #	Txn. #		Txn. #		Txn. #		Txn. #
	acceptNetlist()	*transferLayout()*	*acceptLayout()*	*transferFEOL()*	*acceptFEOL()*	*transferBEOL()*	
0x5bbbc8af0c0e0b7e9f4233b8106e969c847d765501436d2c9b637e11bdc94f9e	0xbc0ac187c0844076070df3bef83e7ed00e94027093e352d3ac033bcf71b88c46	0xe2e0b0d9ca1696065b6845e55daf6ef6f652cfbf23169d72517b79e84c1f0c75	0xbceffb9754e2144037704fb1c76a8d06ee17d3280c654a775bd2e9df146c3498	0x1bda52584f4d3407ed5d9116c9ca0d6abd6cd3e7f6ee5bee1fb3cf45111bd4d0	0x43ea5bc69a82761f67d50f475a82ae1656178841049865c6d12c78ebc308185b	0x67fcd90d3770e28a0348afc2d83589f6ebf4c44864ab9de2495b3aa00384fa5e	0x9b7cf377384150034b61b373f8b6e1706d1dbe1bf8a0eb4fdabd1d4738cd7cbe

Figure 5-3: Blockchain-enabled split manufacturing

5.3 Blockchain-enabled remote FPGA activation

In the post-fabrication stage, this paper introduces a remote activation process for the manufactured FPGA. The purpose of this process is to prevent the offshore foundry from gaining control over the FPGA and to enhance its security against potential malicious activities. After the FPGA manufacturing is completed, the designer initiates the activation by sending an activation key to the FPGA using a secure connection established between the designer and the foundry. This connection is secure and authenticated through the use of public keys belonging to the designer and the foundry. To update the ownership of the activation link, the designer utilizes the smart contract and calls the transferOwnership(activationLink) function. This transfer is then recorded and updated on the blockchain ledger, notifying all the network participants about this ownership transfer.

Similarly, once the foundry receives and accepts the activation link, it updates the ledger by invoking the acceptOwnership(activationLink) function in the smart contract. Subsequently, the FPGA is activated using the provided activation link, while the foundry proceeds to update the ledger through the smart contract to reflect the chip activation. Through this process, the FPGA is successfully activated without granting activation control to the foundry, thus maintaining the control in the hands of the designer. The protocol for this activation process is depicted in Figure 5-4.



Txn #	Txn. #
0xdcc787a8e27c069a0d61925b5bd7f853905c72c7bb334e320930c12809703f20	0x150aa85d808640e2dc5625eab6b077b60584752138bbe8374a07210c1b970d0d

Figure 5-4: Blockchain-enabled remote FPGA activation

5.4 Blockchain-enabled supply chain network

After the FPGA is successfully activated, it is integrated into the supply chain network. This network consists of various participants, assets, and transactions, as summarized in Table 5.1. Throughout the supply chain process, the ownership of the FPGA is transferred and accepted as it moves from the foundry to the distributor, then to the retailer, and finally to the customer. The blockchain network plays a crucial role in tracking and tracing the FPGA at every stage of the supply chain, ensuring transparency and accountability. Additionally, the implemented PUFs provide an extra layer of authentication and verification for the FPGAs, enhancing their security and trustworthiness.

The smart contract implemented in this network incorporates a modifier function to ensure that each participant has access only to the specific asset required for their transaction. This prevents unauthorized access and ensures the integrity of the supply chain process. Table 5.1 provides a comprehensive overview of the participants, their respective assets, and the corresponding functions they are authorized to call within the smart contract. This ensures that the participants can interact with the blockchain network in a secure and controlled manner, contributing to the overall security and efficiency of the supply chain.

Table 5.1: Blockchain-enabled FPGA supply chain: Components

Sr. #	Participants	Assets	Transactions
1	3PIP vendor	IP Core	Registration of IP Cores, transfer of IP Cores
2	3P EDA vendor	EDA tools	Registration of EDA tools, transfer of EDA tools
3	Design House	IP Cores, EDA tools, GDSII layout file	Registration of layout, accept IP, EDA, transfer GDSII

4	FEOL Foundry	FEOL layout	Accept FEOL, transfer BEOL
5	BEOL Foundry	BEOL layout	Accept BEOL, transfer FPGA
6	OSAT	FPGA	Accept & transfer of FPGA
7	OEM	FPGA	Accept & transfer of FPGA
8	Distributor	FPGA	Accept & transfer of FPGA
9	Retailer	FPGA	Accept & transfer of FPGA
10	End-User	FPGA	Accept & transfer of FPGA
11	Recycler	FPGA	Accept & transfer of FPGA

5.5 Proposed Techniques: Implementation

A single smart contract has been developed to encompass the entire proposed work, serving as the foundation for the consortium blockchain. Only invited participants with proper access credentials are allowed to register themselves in the network, ensuring a secure and controlled environment. The designer, being the trusted party, has the authority to grant access to other participants. Upon registration, the smart contract validates the registration code generated by an external algorithm. Successful registration grants the participant a unique participant ID (address) generated by the smart contract, which is stored in the blockchain for future reference and validations. Once all participants are registered in the network, the supply chain process begins, following the flow discussed in Section 5.4. This comprehensive approach ensures the integrity and security of the supply chain network, with participants having authorized access and transparent interactions within the blockchain.

In addition to the smart contract, external applications have been developed to support specific functionalities linked to the contract. These applications generate unique registration codes for participant registration and retrieve file hashes from the file storage system. The smart contract is integrated with these applications, allowing them to be called when needed. During participant registration, the external application generates a unique registration code, similar to a one-time password. This code is then stored in the blockchain alongside the participant's information. The registration code provided during registration is compared with the stored code, and upon a match, a unique Participant Identification (address) is generated and assigned to the participant. This participant ID, along with the corresponding participant, is stored in the blockchain database for future verification purposes. A success message is displayed once the participant ID generation and storage are completed. Furthermore, a modifier function monitors the registration process, ensuring that the function is called by the participant whose address was provided during registration. This adds an additional layer of security and validation. Pseudocode 5.1 outlines the registration process in detail.

Pseudocode 5.1: Registration of Participant

```
function registerParticipant (name, companyName, role, regCode, participantAddress){
  if (msg.sender =participantAddress()) then
      //Register the participant with their corresponding role
else – error message: "User does not have permission"
  end if
```

Once the design house creates a new design layout or bitstream file, it needs to register the file in the blockchain network for further processes. This registration involves uploading the design file to the file storage system and obtaining the file's hash. To register the file, the participant (in this case, the designer) logs into the system using their Participant ID (designerAddress). With the use of a modifier, only the designer is allowed to upload the file specifications, including the IP ID or bitstream ID, and the hash of the uploaded file, into the blockchain system. After providing the necessary file specifications, the file is registered in the blockchain along with its corresponding hash. This process is similar to Pseudocode 1, with some changes in the input parameters. When requested by the foundry or the next owners, the design house securely sends the unique ID of the file using a designated link. The blockchain system provides the hash of the file exclusively to the next owner through a pre-defined modifier. Even though the unique ID of the file is known, the actual file cannot be accessed as it is hashed, and only the next owner has the authorization to access it. Upon downloading the file from the file storage system, the next owner accepts the ownership of the file, making them solely responsible for its handling. The transfer and acceptance of the file are outlined in Pseudocode 5.2, providing a step-by-step algorithm for the process.

Pseudocode 5.2: Transfer and accept of Asset

```
Input: unique ID, currentOwnerAddress, newOwnerAddress

if Message sender is currentOwnerAddress, then
    //Transfer the asset
else
    //Revert the transaction – "You are NOT Authorized"
end
if  Message sender is newOwnerAddress, then
    //Accept the asset
```

```
else
    //Revert the transaction – “You are NOT Authorized”
end
```

After the manufacturing of the IC, the foundry notifies the designer about the completion of the process. The designer then sends an activation link for the FPGA, and this information is updated on the blockchain ledger. The transfer of ownership for this activation link is also essential and follows a similar algorithm as the transfer of ownership for assets (Pseudocode 5.2). Once the FPGA is manufactured, it needs to be registered into the system. This registration process is solely performed by the designer to maintain control over the FPGA. The algorithm for registering the FPGA is similar to Pseudocode 5.1, with changes in the parameters. The parameters for this process include the IP ID, IC ID, ECID, and CRPs (challenge-response pairs). After the registration, the FPGA is incorporated into the supply chain for distribution. Throughout the supply chain, the ownership of the FPGA changes hands, necessitating the transfer and acceptance of ownership. This algorithm follows a similar approach as the transfer of ownership for assets, ensuring that ownership is properly transferred from one participant to another.

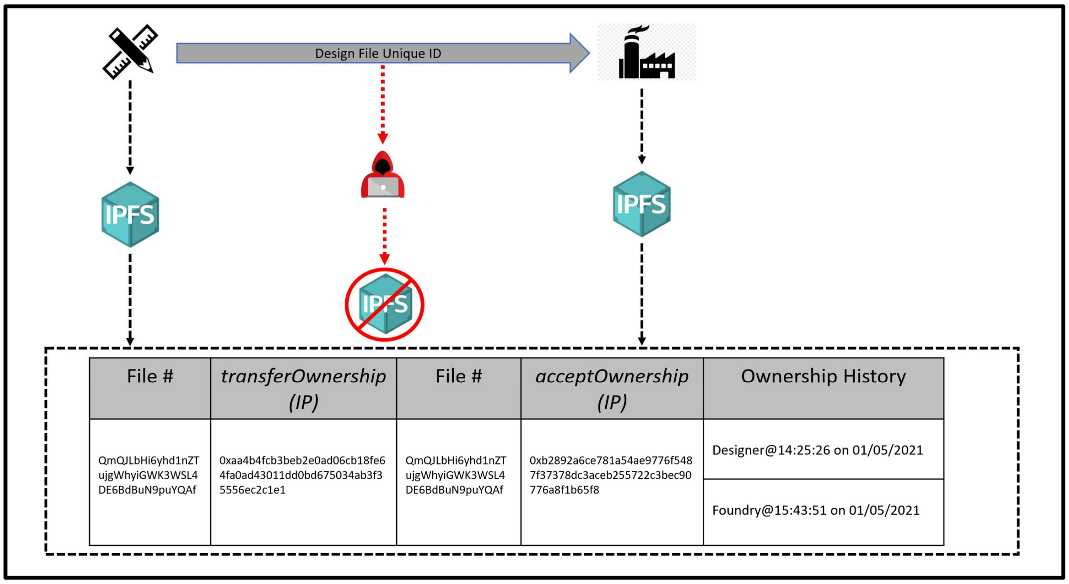
5.6 Case studies

The techniques discussed in Section 5.4 have been successfully simulated using the local Ganache UI provided by the Truffle framework. Smart contracts specifically designed for these techniques are developed and deployed on the Truffle framework, allowing them to be executed within the Ganache development environment. The simulations are conducted using Xilinx Artix-7 FPGAs mounted on Digilent Nexys 4 boards. These simulations effectively achieve the objective of securing the post-fabrication FPGA supply chain. Each technique developed addresses a specific security issue that is commonly faced by the FPGA supply chain. In this section, the conducted simulations are discussed, and an example scenario is presented to illustrate how these techniques mitigate specific threats within the supply chain.

5.6.1 Blockchain-enabled file storage and transfer system

An application for the file storage system has been developed to facilitate the acceptance of GDSII files and provide their corresponding hashes. This application is designed to be run on localhost port 3000 and features a user interface with upload and download buttons. To validate the functionality of this application, GDSII files for five different FPGAs are created using the GDSII layout software LayoutEditor. These GDSII files are then uploaded to the file storage system through the developed application, which subsequently fetched their respective hashes. The file storage system, integrated with the blockchain technology, returned hashes that start with 'Qm,' confirming the authenticity of the hashes and demonstrating that they are obtained from the designed blockchain-enabled file storage system application [104]. This confirms the successful operation of the file storage system application and its integration with the blockchain network.

In the traditional method of storing and transferring GDSII layout files, there is a risk of an adversary hacking the communication or transfer channel and stealing the layout file. However, by adopting the proposed blockchain-enabled system, the layout file is secured from such attacks as the adversary does not gain access to the file. In Figure 5-5, an adversary successfully hacks the transmission channel and obtains the unique ID of the design file (IP ID). However, simply possessing the unique ID is not sufficient, as the IPFS application requires the query to originate from the foundry in order to retrieve the hash of the file. Even if the attacker manages to acquire the hash through further attacks and modifies the file, the hash of the file will change. This change in hash raises a red flag among the participants in the network, alerting them to the tampering attempt. This demonstrates the effectiveness of the blockchain-enabled file storage and transfer system in protecting the FPGA supply chain from challenges such as IP theft, piracy, and bitstream modification. By leveraging the immutability and transparency of the blockchain, the system provides evidence of the file's integrity and safeguards against unauthorized modifications.



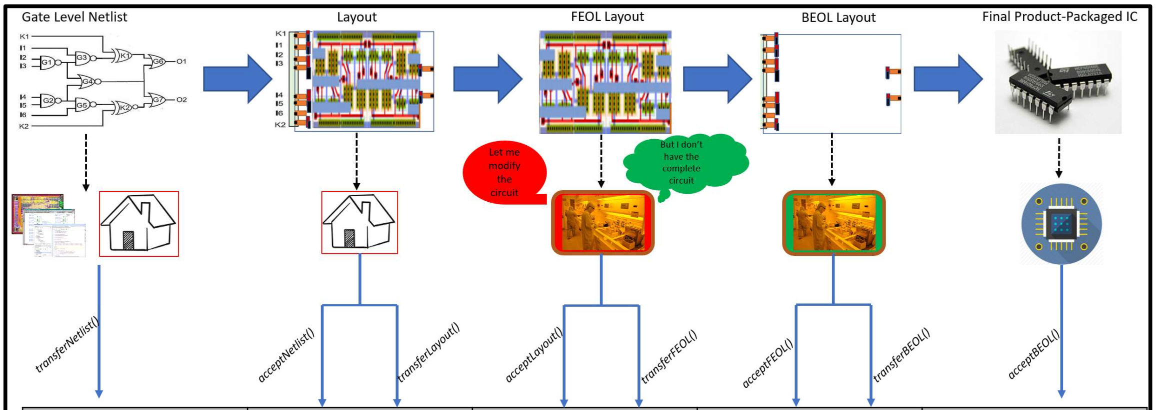
File #	*transferOwnership (IP)*	File #	*acceptOwnership (IP)*	Ownership History
QmQJLbHi6yhd1nZTujgWhyiGWK3WSL4DE6BdBuN9puYQAf	0xaa4b4fcb3beb2e0ad06cb18fe64fa0ad43011dd0bd675034ab3f35556ec2c1e1	QmQJLbHi6yhd1nZTujgWhyiGWK3WSL4DE6BdBuN9puYQAf	0xb2892a6ce781a54ae9776f5487f37378dc3aceb255722c3bec90776a8f1b65f8	Designer@14:25:26 on 01/05/2021
				Foundry@15:43:51 on 01/05/2021

Figure 5-5: Blockchain-enabled file storage system security evaluation

5.6.2 Blockchain-enabled split manufacturing

Initially, split manufacturing was introduced as a measure to mitigate the risks associated with reverse engineering. However, the conventional split manufacturing technique has proven to be inadequate in keeping up with the increasing sophistication of attacks and the intelligence of malicious actors. To address this limitation, there is a need to modernize the split manufacturing technique by incorporating blockchain technology, which can provide enhanced security measures to counter reverse engineering attempts. Consider a scenario where the high-end foundry, responsible for the FEOL layout of the FPGA, has malicious intentions and aims to tamper with the circuit by inserting a Trojan, as illustrated in Figure 5-6. By integrating blockchain technology into the split manufacturing process, the risks associated with such malicious activities can be effectively mitigated.

During the split manufacturing process, each stage of the supply chain, including the FEOL foundry, uploads the shared ledger to the blockchain. This ledger contains crucial information about the assets being transferred, such as the layout files. By maintaining a transparent and immutable record on the blockchain, any unauthorized modifications or tampering of the layout files can be readily detected. In this particular scenario, when the FEOL foundry attempts to insert the Trojan into the circuit, subsequent stages of the supply chain will identify this modification. Participants, including the designer, the BEOL foundry, and other stakeholders, can verify the authenticity and integrity of the layout files by comparing them with the information stored on the blockchain. Any inconsistencies or tampering will raise red flags, enabling prompt actions to address the malicious activity. By combining the split manufacturing technique with blockchain technology, the security of the supply chain is significantly bolstered, providing robust protection against reverse engineering attempts and ensuring the integrity of the FPGA's design.



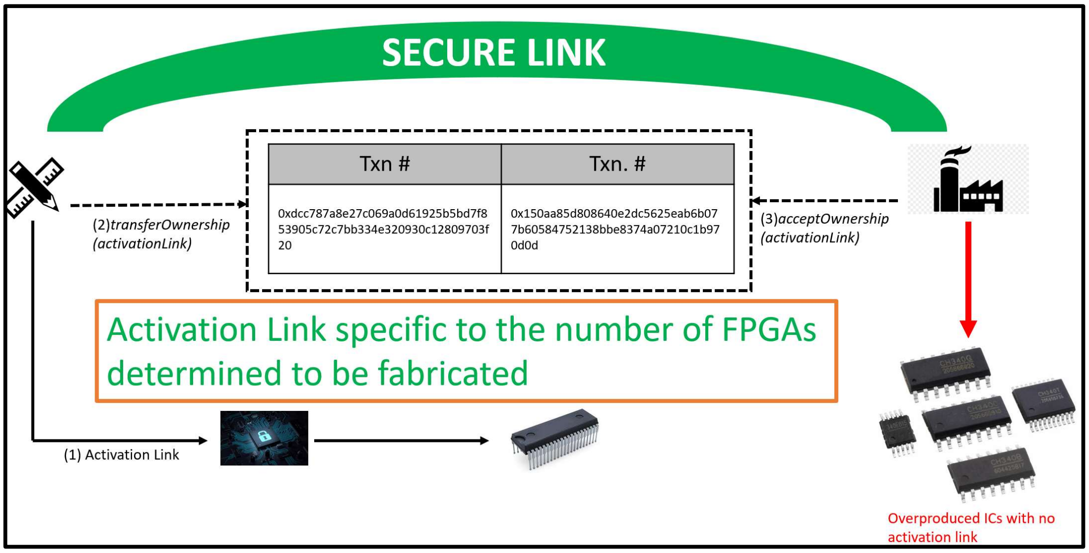
Txn. #	Txn. #		Txn. #		Txn. #		Txn. #
	acceptNetlist()	*transferLayout()*	*acceptLayout()*	*transferFEOL()*	*acceptFEOL()*	*transferBEOL()*	
0x5bbbc8af0c0e0b7e9f4233b8106e969c847d765501436d2c9b637e11bdc94f9e	0xbc0ac187c0844076070df3bef83e7ed00e94027093e352d3ac033bcf71b88c46	0xe2e0b0d9ca1696065b6845e55daf6ef6f652cfbf23169d72517b79e84c1f0c75	0xbceffb9754e2144037704fb1c76a8d06ee17d3280c654a775bd2e9df146c3498	0x1bda52584f4d3407ed5d9116c9ca0d6abd6cd3e7f6ee5bee1fb3cf45111bd4d0	0x43ea5bc69a82761f67d50f475a82ae1656178841049865c6d12c78ebc308185b	0x67fcd90d3770e28a0348afc2d83589f6ebf4c44864ab9de2495b3aa00384fa5e	0x9b7cf377384150034b61b373f8b6e1706d1dbe1bf8a0eb4fdabd1d4738cd7cbe

Figure 5-6: Blockchain-enabled split manufacturing security evaluation

5.6.3 Blockchain-enabled remote FPGA activation

One of the major challenges faced by design houses is the overproduction of microelectronics, which are then illicitly sold in the black market. This practice can result in significant financial losses for semiconductor companies. However, the proposed solution of blockchain-enabled remote FPGA activation aims to address this issue. In Figure 5-7, an untrusted foundry is depicted, fabricating an excessive number of FPGAs beyond the order placed by the design house. These surplus FPGAs are then sold in the black market, generating unethical monetary profits for the foundry.

To counter this practice, the blockchain-enabled remote FPGA activation technique plays a crucial role. With this technique, the designer maintains control over the activation process of the manufactured FPGAs. Once the manufacturing of the FPGAs is complete, the designer sends an activation link to the foundry through a secure connection. The ownership transfer of this activation link is recorded on the blockchain ledger. The foundry, upon receiving the activation link, updates the ledger to acknowledge the acceptance of ownership. This ensures that only the designated and authorized parties can activate the FPGAs.


SECURE LINK
(2)*transferOwnership* *(activationLink)*
(3)*acceptOwnership* *(activationLink)*
Activation Link specific to the number of FPGAs determined to be fabricated
(1) Activation Link
Overproduced ICs with no activation link

Txn #	Txn. #
0xdcc787a8e27c069a0d61925b5bd7f853905c72c7bb334e320930c12809703f20	0x150aa85d808640e2dc5625eab6b077b60584752138bbe8374a07210c1b970d0d

Figure 5-7: Blockchain-enabled remote FPGA activation evaluation

The implementation of the proposed technique results in locked FPGAs that can only be unlocked using the appropriate activation link, which acts as a key. These activation links are specific to each FPGA, ensuring that only FPGAs manufactured with the design house's consent have a valid activation link. On the other hand, the overproduced FPGAs remain inactive, without any functional application. The use of a shared blockchain ledger and the storage of activation link ownership with timestamps adds an additional layer of security. This prevents the untrusted foundry from engaging in any malicious activities related to the activation process. The blockchain ledger records and verifies the ownership of the activation links, ensuring transparency and accountability throughout the supply chain.

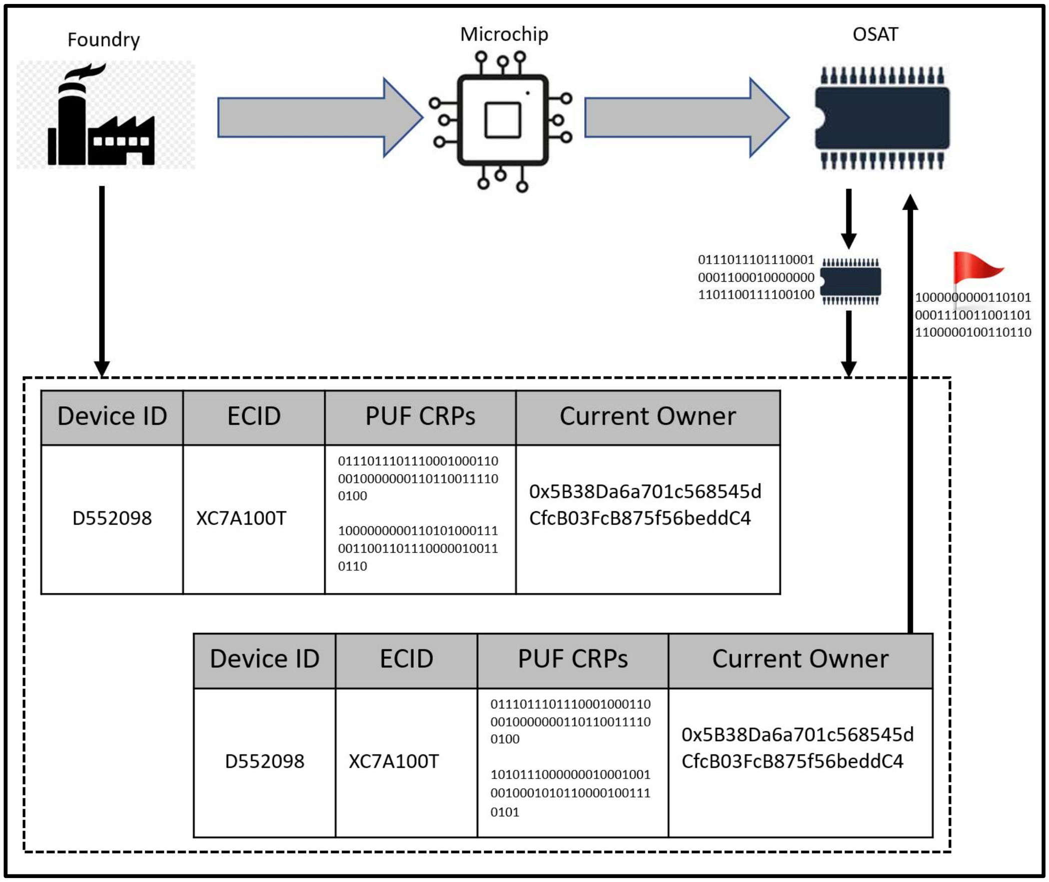
By employing this approach, the proposed technique effectively addresses the challenge of overproduction and unauthorized distribution of FPGAs. It ensures that only authorized FPGAs receive the appropriate activation links, enhancing the security and control over the FPGA supply chain. Additionally, the untrusted foundry is unable to gain unauthorized access or control over the activation of the FPGAs, preventing them from selling the surplus devices in the black market. This solution provides a robust mechanism for preventing the unauthorized distribution of FPGAs, safeguarding the financial interests of design houses and semiconductor companies.

5.6.4 Blockchain-enabled supply chain network

One significant threat faced by the FPGA supply chain is the presence of counterfeit FPGAs. To address this issue, the blockchain-enabled supply chain network proves to be beneficial. The blockchain network allows for the registration of FPGAs along with their descriptions onto the shared ledger. These registration details serve as a reference point for future comparisons. One important field included in the registration details, provided by the design house, is the challenge-response pairs of the ROPUF (Ring Oscillator Physical Unclonable Function). The response of the ROPUF is not only dependent on the challenge but also on the specific device on which it is implemented. Therefore, any alteration in the circuitry of the FPGA results in a change in the response of the ROPUF, as the PUF acts as a unique fingerprint for the device.

Let's consider a scenario where a rogue foundry produces a counterfeit FPGA that contains a hardware Trojan. Due to the changes made to the FPGA's circuitry, the response generated by the PUF when presented with a challenge will be different. During the testing procedure, the OSAT (Outsourced Semiconductor Assembly and Test) provides challenges to the FPGA. However, due to the alteration in the FPGA, the response generated by the PUF will not match the expected response. The OSAT then submits these parameters to the blockchain network for comparison with the reference values. As a result of the discrepancy in the response, the blockchain raises a red flag, alerting the OSAT about the presence of a counterfeit FPGA. This scenario is depicted in Figure 5-8, illustrating how the blockchain-enabled supply chain network can detect and identify counterfeit FPGAs based on the differences in the PUF responses.

The proposed work successfully addresses several challenges faced by the IC supply chain, including IP theft, hardware Trojan intrusions, over-production, and reverse engineering. These issues are significant threats to the integrity and security of the current supply chain. The chapter also focuses on achieving traceability of assets and tracking their provenance. By leveraging blockchain technology, the proposed system ensures the immutability and transparency of transaction records. This allows for the tracking and tracing of assets throughout the supply chain, providing a clear view of their origins and history. To address malicious activities and enhance security, various measures have been implemented. These include the use of physical unclonable functions (PUFs) for authentication and verification, the secure transfer of ownership through blockchain transactions, and the detection of counterfeit FPGAs through PUF responses. By integrating these security features into the proposed framework, the chapter demonstrates how the supply chain can be protected against malicious activities while providing a reliable and trustworthy system for asset tracking and provenance verification.



Device ID	ECID	PUF CRPs	Current Owner
D552098	XC7A100T	0111011101110001000110 0010000000110110011110 0100 1000000000110101000111 0011001101110000010011 0110	0x5B38Da6a701c568545d CfcB03FcB875f56beddC4

Device ID	ECID	PUF CRPs	Current Owner
D552098	XC7A100T	0111011101110001000110 0010000000110110011110 0100 1010111000000010001001 0010001010110000100111 0101	0x5B38Da6a701c568545d CfcB03FcB875f56beddC4

Figure 5-8: Blockchain-enabled supply chain network evaluation

The work presented in this chapter focuses on leveraging blockchain technology to enhance the security and integrity of the supply chain. A key aspect of the research is the development of a file storage system that facilitates the secure upload and hashing of design files onto the blockchain network as depicted in Figure 5-5. This system incorporates an additional security layer by allowing only the designer to upload the hash, ensuring accountability in case of any modifications to the intellectual property (IP) being shared. By utilizing a blockchain-powered split manufacturing approach, where different foundries have limited access to specific parts of the fabrication process, the risk of reverse engineering is significantly reduced. This makes it challenging for malicious actors to gain full knowledge of the IC's design, as illustrated in Figure 5-6. The registration of each IC in the blockchain network enables continuous monitoring, making it possible to identify any instances of overproduction and hold the responsible party accountable, as shown in Figure 5-7. To address the threat of hardware Trojan intrusion, the implementation of Ring Oscillator Physical Unclonable Functions (ROPUFs) on the ICs plays a crucial role. The stored Challenge-Response Pairs (CRPs) are compared with the obtained CRPs, and any discrepancies raise a red flag, indicating a potential Trojan intrusion, as depicted in Figure 5-8.

5.7 Blockchain performance

This section discusses the performance of the developed blockchain. First the simulation platform is elaborated along with the information about the computer configuration used. Furthermore, the smart contract details and blockchain performance is discussed on two parameters.

5.7.1 Simulation platform : Ganache

Ganache, developed by the Truffle Framework, is a personal blockchain platform specifically designed for efficient and rapid development of Ethereum-based distributed applications (dApps) [109]. It offers developers a safe and deterministic environment for various stages of dApp development, including development, deployment, and testing. Ganache provides two user-friendly platforms: a graphical user interface (UI) and a command-line interface (CLI). The Ganache UI is a desktop application that supports Ethereum technology. Within Ganache, there are ten pre-configured accounts, each equipped with a balance of one hundred Ethers. It is important to note that these Ethers are intended solely for testing purposes and should not be used in real blockchain networks. These accounts can be utilized for executing transactions, running tests, and inspecting the state of the blockchain. Figure 5-9 provides a visual representation of the Ganache UI and its account configuration. One notable feature of Ganache is the ability to customize the block mining time. Unlike the real-world Ethereum blockchain, where the time between two blocks is determined by network consensus, Ganache allows users to pre-define the block interval. The block mining time can be set within a range of 1 to 200 seconds. In the case study described, the accounts are assigned to different users within the network, and the blockchain system is tested and simulated accordingly. Simulations are conducted using different block times, specifically 60, 120, and 180 seconds.

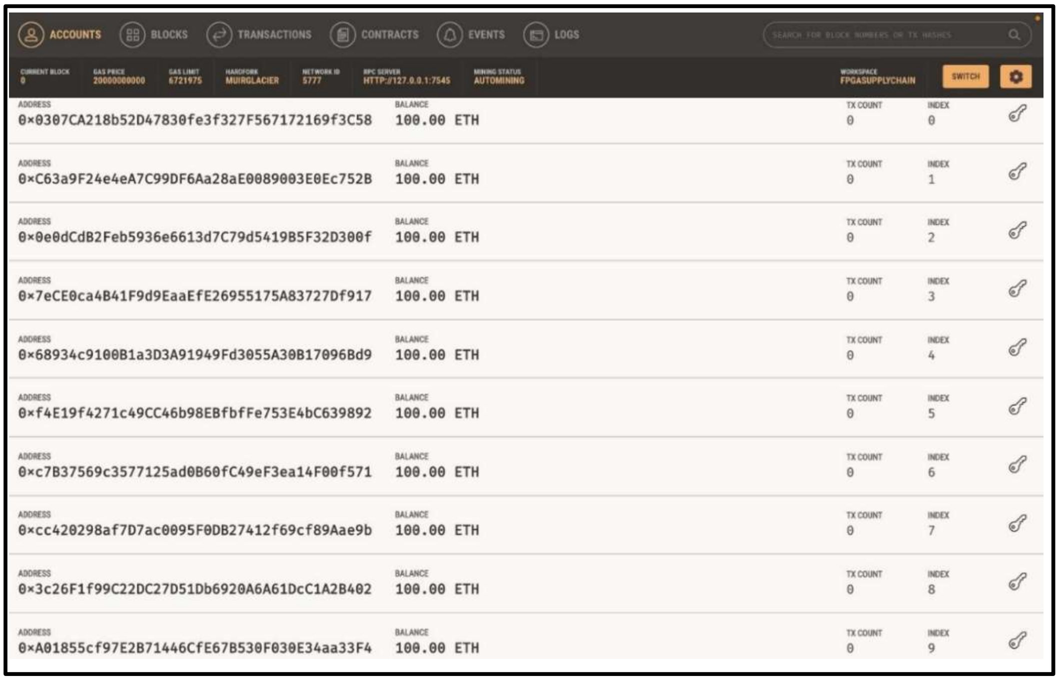
To assess the performance of the blockchain system, two key parameters are considered: transactions per second (TPS) and latency. These metrics provide insights into the efficiency and responsiveness of the blockchain network, allowing for an evaluation of its performance under varying conditions. By leveraging the capabilities of Ganache, the research is able to conduct simulations and measure the performance of the developed blockchain system, enabling a comprehensive analysis of its behavior and effectiveness.

5.7.2 Device Configuration

The network is simulated on Ganache blockchain run on an Apple MacBook (laptop). The system specifications are as follows:

- System Model – MacBook Air (Retina)
- Processor – 1.1 GHz Dual-Core Intel Core i3
- Memory – 8GB 3733 MHz LPDDR4X

- ❖ Graphics – Intel Iris Plus Graphics 1536 MB



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
0	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	FPGASUPPLYCHAIN

ADDRESS	BALANCE	TX COUNT	INDEX
0×0307CA218b52D47830fe3f327F567172169f3C58	100.00 ETH	0	0
0×C63a9F24e4eA7C99DF6Aa28aE0089003E0Ec752B	100.00 ETH	0	1
0×0e0dCdB2Feb5936e6613d7C79d5419B5F32D300f	100.00 ETH	0	2
0×7eCE0ca4B41F9d9EaaEfE26955175A83727Df917	100.00 ETH	0	3
0×68934c9100B1a3D3A91949Fd3055A30B17096Bd9	100.00 ETH	0	4
0×f4E19f4271c49CC46b98EBfbfFe753E4bC639892	100.00 ETH	0	5
0×c7B37569c3577125ad0B60fC49eF3ea14F00f571	100.00 ETH	0	6
0×cc420298af7D7ac0095F0DB27412f69cf89Aae9b	100.00 ETH	0	7
0×3c26F1f99C22DC27D51Db6920A6A61DcC1A2B402	100.00 ETH	0	8
0×A01855cf97E2B71446CfE67B530F030E34aa33F4	100.00 ETH	0	9

Figure 5-9: Representation of Ganache UI

5.7.3 Smart contract details

A single smart contract is developed for the research, with functions defined for every transaction. The details of the smart contract are tabulated in Table 5.2 below.

Table 5.2: Details of the smart contract

Function name	Caller	Execution
registerParticipant	3PIP Vendor, FPGA Vendor, EDA Vendor, Foundry, OSAT, OEM, Distributor, End Consumer	Registration of participants in the network
registerIPCore	3PIP Vendor	Registration of IP Core in the network
transferIP	3PIP Vendor	Transferring ownership of IP core
acceptIP	FPGA Vendor	Accepting ownership of IP Core
registerEDA	3P EDA Vendor	Registration of EDA in the network
transferEDA	3P EDA Vendor	Transferring ownership of EDA
acceptEDA	FPGA Vendor	Accepting ownership of EDA
registerGDSII	FPGA Vendor	Registration of layout file in network

transferGDSII	FPGA Vendor	Transferring ownership of layout
acceptGDSII	Foundry	Accepting ownership of layout
registerFPGA	FPGA Vendor	Registration of FPGA in the network
transferFPGA	FPGA Vendor	Transferring ownership of FPGA
acceptFPGA	New Owner	Accepting ownership of FPGA

Table 5.2 presents a comprehensive overview of the functions defined for each transaction, the corresponding user responsible for calling the function, and the action performed by the function. In the network, every user is assigned a unique account out of the ten accounts provided by Ganache. Furthermore, Ganache offers the flexibility to customize the block mining time, allowing users to specify the time interval between blocks within the range of 1 to 200 seconds. For the purpose of simulation, the blockchain network has been tested under three different block time scenarios: 60, 120, and 180 seconds. This variation in block times provides insights into the performance and behavior of the blockchain system under different temporal conditions.

The result for these different scenarios is tabulated below in Table 5.3 and represented graphically in Figure 5-10.

Table 5.3: Simulation results for different block times w.r.t transactions and blocks mined

Block Time (seconds)	Number of Transactions	Number of blocks mined
60	19	17
120	19	10
180	19	6

5.7.4 Performance Metrics

The performance of the blockchain network, which was developed for this investigation, was simulated using the Ganache blockchain platform provided by the

Truffle Framework. The simulations were conducted on the specified system configuration mentioned earlier. The performance of the blockchain network was evaluated based on two parameters:

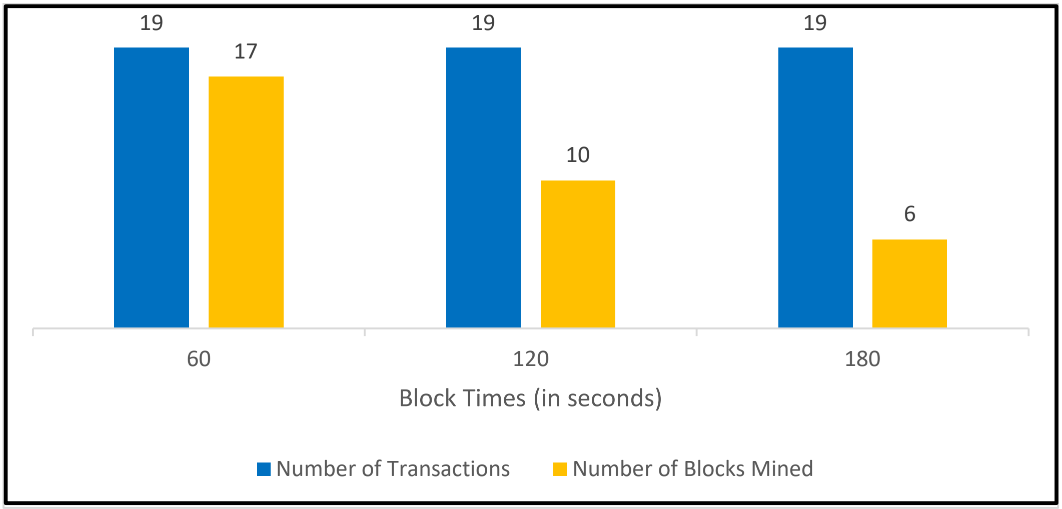


Figure 5-10: Simulation results for different block times

5.7.4.1 Transactions per Second (TPS)

TPS is a measure of the throughput of the blockchain, which refers to the number of successful transactions completed within a second by the blockchain platform [110], [111]. As provided in [111], we calculate TPS as follows:

TPS = (transaction per block) * (blocks per second)……………………… 1

Transaction per block=(number of transactions)/(blocks mined for entire process)..1.1

Block per second = (blocks mined in time ‘t’)/time ‘t’…………………………..1.2

As the blockchain network is simulated for three different time scenarios, the TPS for each timing is calculated.

⇨ <u>For t = 60 seconds:</u>

$$\left.\begin{array}{l}\text{Number of transactions: 19}\\ \text{Number of blocks mined: 17}\end{array}\right\}\text{From Table 5.3}$$

Substituting above values in eq. 1.1 –

TPS = (19/17)*(1/60) = (1.117)*(0.016) => $\boxed{\text{TPS = 0.017}}$

⇨ For t = 120 seconds:

$$\left.\begin{array}{l}\text{Number of transactions: 19}\\ \text{Number of blocks mined: 10}\end{array}\right\}\text{From Table 5.3}$$

Substituting above values in eq. 1.1 –

TPS = (19/10)*(1/120) = (1.9)*(0.008) => $\boxed{\text{TPS = 0.0152}}$

⇨ For t = 180 seconds:

$$\left.\begin{array}{l}\text{Number of transactions: 19}\\ \text{Number of blocks mined: 6}\end{array}\right\}\text{From Table 5.3}$$

Substituting above values in eq. 1.1 –

TPS = (19/6)*(1/180) = (3.167)*(0.005) => $\boxed{\text{TPS = 0.0158}}$

The above results are depicted by a bar graph in the Figure 5-11.

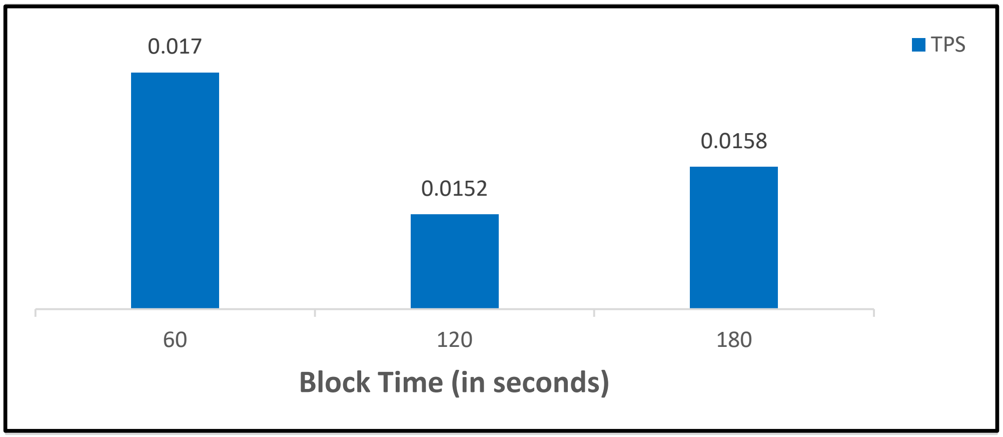


Figure 5-11: TPS for different block times

5.8.4.2 Latency

Latency, in the context of the blockchain platform, refers to the response time per transaction, indicating the time taken from transaction submission to its confirmation by the network [110]. It is an important performance metric that measures the efficiency and responsiveness of the network. In this investigation, the latency of the blockchain network was computed with the block time set at its default value provided by Ganache [112]. The latency of each function within the network was recorded, and the results were visualized in a bar graph shown in Figure 5-12. The latency values for each function are also tabulated in Table 5.5. he latency values were calculated in seconds and were averaged to obtain the overall latency of the entire network. By analyzing the latency of individual functions and the overall network latency, the performance and responsiveness of the blockchain platform can be assessed. It is worth noting that latency is independent of the block time, which means it is not affected by the time interval between blocks in the blockchain network. Instead, it focuses on the time taken for transaction processing and confirmation by the network. The latency information obtained from these calculations provides valuable insights into the performance and efficiency of the blockchain network in terms of transaction response time.

Table 5.4: Latency for different transactions and their average

Function name	Latency (in seconds)	Average Latency (in seconds)
registerParticipant	1.36	(1.36+0.83+0.5+0.5+1.06+0.51+0.48+0.78 +0.46+0.43+0.66+0.46+0.56)/13 = 0.66
registerIPCore	0.83	
transferIP	0.5	
acceptIP	0.5	
registerEDA	1.06	
transferEDA	0.51	
acceptEDA	0.48	
registerGDSII	0.78	
transferGDSII	0.46	
acceptGDSII	0.43	
registerFPGA	0.66	
transferFPGA	0.46	
acceptFPGA	0.56	

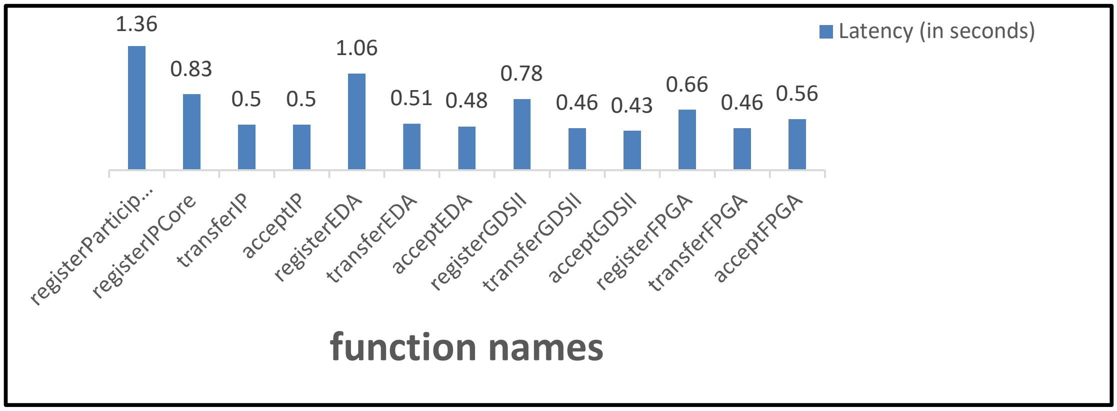


Figure 5-12: Latency recorded for every function

In order to achieve the research goal of simulating a prototype for a reliable and secure IC supply chain process, various security approaches were incorporated. These approaches are summarized in Table 5.5, highlighting the measures taken to ensure the security and integrity of the supply chain throughout the different stages. Overall, the combination of blockchain technology, secure file storage, split manufacturing, activation links, and PUF-based authentication contributes to the creation of a robust and trustworthy IC supply chain process.

Table 5.5: Comparison of presented work with previous work

Previous Work	IP Theft	Trojan Intrusion	Overproduction	Reverse Engineering	Traceability	Provenance
[20] - 2019	✗	✗	✓	✗	✓	✗
[21] – 2019	✓	✗	✓	✗	✗	✗
[97] – 2018	✗	✗	✗	✗	✓	✗
[124] - 2019	✗	✗	✗	✗	✗	✓
This work	✓	✓	✓	✓	✓	✓

5.8 Summary

This chapter introduces various blockchain-enabled techniques to enhance the security of the FPGA supply chain. It starts by presenting a file storage and transfer system that utilizes blockchain to secure files involved in the supply chain, such as IP cores and bitstream files. The traditional split manufacturing technique is then modernized by incorporating blockchain, which helps combat reverse engineering threats. To address overproduction issues, a blockchain-enabled remote FPGA activation method is proposed. Additionally, the entire supply chain is blockchain-enabled to detect and prevent counterfeited FPGAs by recording data on a shared distributed ledger.

The proposed techniques were evaluated through simulations conducted on the Ganache UI provided by the Truffle framework. The simulations demonstrated the effectiveness of the proposed work in addressing security threats faced by the FPGA supply chain, including IP theft, bitstream tampering, reverse engineering, hardware Trojan intrusion, and overproduction. The performance of the blockchain was also assessed in terms of transactions per second (TPS) and latency. Based on the simulations, the TPS values for the presented work were measured as 0.017, 0.0152, and 0.0158 for block times of 60, 120, and 180 seconds, respectively. The latency of each transaction was recorded, and the average latency for the entire system was calculated to be 0.66 seconds. Overall, the simulation-based evaluation confirms the effectiveness of the proposed techniques in addressing security threats and demonstrates the performance of the blockchain network in terms of TPS and latency.

Chapter 6

A Zero Trust FPGA Supply Chain Architecture

The semiconductor supply chain is vulnerable to security threats from untrusted participants involved in the network. These threats involve, but are not limited to hardware Trojan insertion, cloning, intellectual property (IP) theft and piracy, bitstream tampering etc. As a result, significant research is being conducted to secure the integrity of the semiconductor supply chain. Semiconductors are classified into two categories- application specific integrated circuits (ASICs), which are manufactured for specific applications, and field programmable gate arrays (FPGAs), which are general purpose and be programmed after fabrication. This paper aims to establish a secure zero-trust FPGA supply chain by leveraging blockchain and hardware security primitives like ring oscillator physical unclonable functions (ROPUFs). The proposed work capitalizes on blockchain's features like smart contracts, tracking and tracing capabilities, and immutability along with uniqueness offered by PUFs to formulate and implement zero trust policies. The policies draw inspiration from zero trust tenets outlined by NIST. The smart contract for the postulated work is developed using Solidity language. To evaluate the successful implementation of the proposed technique, simulations have been conducted in the author's research lab on Ganache framework provided by Truffle suite. Additionally, a corresponding case study of the same is presented. The experiment is performed on Artix 7 Xilinx FPGAs mounted on Nexys 4 Digilent boards. Finally, each tenet of the implemented zero trust architecture is evaluated by discussing an attack scenario, demonstrating how the proposed framework mitigates potential security risks.

6.1 Introduction & background

A field-programmable gate array (FPGA) is a versatile and reconfigurable logic device capable of being programmed with specific application designs after the manufacturing process [113], [114]. The desired application is defined by a binary file called a bitstream file [115]. FPGAs find extensive use in various cyber-physical systems, including aviation, medical, and military applications, owing to their reconfigurability, cost-effectiveness, and high performance [85], [116]. However, in order to manage financial constraints, the fabrication of FPGAs is often outsourced to offshore foundries, resulting in the establishment of a global supply chain [117], [118]. In the current FPGA supply chain, participants from different regions collaborate to ensure its success [2] as illustrated in Figure 1-1. This FPGA supply chain involves various entities, some trusted and others untrusted, raising concerns regarding the security of both the chip and the final electronic product [19]. The growing usage of semiconductor chips, coupled with recent disruptions in the global supply chain, has led to the infiltration of counterfeit and recycled FPGAs into various systems. This poses significant security threats to governments and industries [85]. Counterfeit FPGAs have become one of the top five counterfeited electronic components, accounting for approximately 8.3% of reported incidents [2], [119].

To address these significant challenges, the US Government acted by releasing an executive order in February 2021. The order aimed to improve the resilience of America's supply chain, particularly in relation to semiconductors [28]. Additionally, in May 2021, the Government issued another executive order that emphasized the importance of implementing zero trust architecture to enhance the nation's cybersecurity [29].

6.2 Roles of ZTA, blockchain & PUF

To achieve a successful implementation of a zero trust architecture, it is essential to adhere to the tenets outlined by NIST, which establish a secure perimeter around the supply chain network. These tenets focus on access control, authorization, supervision, and overall security. For user authorization, blockchain technology is primarily utilized, leveraging its features such as transparency and decentralized control. PUFs, on the other hand, play a crucial role in authenticating the FPGAs within the network. Monitoring and security are addressed through the traceability and immutability features offered by blockchain. These features enable the recording and tracking of transactions, ensuring that any tampering attempts or unauthorized changes can be identified and prevented. The combination of these features in the proposed architecture helps establish a secure and trustworthy supply chain network.

6.2.1 The zero trust approach

A zero trust architecture incorporates micro-segmentation within a network through authorization and verification policies. In this section, the policies necessary for the successful implementation of the zero trust architecture in the FPGA supply chain are discussed. These policies draw inspiration from the zero trust tenets defined by NIST [8].

The tenets are interpreted specifically for the FPGA supply chain domain and are presented in Table 6.1. The application of these tenets within the proposed research is discussed in detail, highlighting how they contribute to establishing a secure and trustworthy FPGA supply chain network.

Table 6.1: Zero trust tenets and their interpretation for FPGA supply chain

Tenets	Interpretation
Data and computation are considered as resources	Disparate resource set
Information is secured regardless of location	Independent security
Access to resources on a per-session basis	Traceability
Access is determined by a dynamic policy	Provenance
Device and assets are held in the most secure state possible	Confidentiality
Authentication and authorization are strictly enforced	Integrity
Collection of information on current state to improve security	Persistent Evaluation

6.2.2 The blockchain support

The development of smart contracts plays a crucial role in providing the key features of blockchain technology [120]. These features, in combination with smart contracts, contribute to the successful fulfillment of the zero trust tenets within the proposed work. Smart contracts enable the automation and enforcement of predefined rules and policies, ensuring transparency, accountability, and secure transactions within the FPGA supply chain network. In order to ensure authorization and verification of users in the system, the proposed research implements a blockchain-enabled multi-factor authentication application. It is important to note that the authors have developed this application, drawing inspiration from [122], and they do not claim original credit for it. The multi-factor authentication application is integrated into the system to enhance security. By leveraging blockchain technology, trust is established in the users, devices, applications, and traffic within the network. This is achieved through the recording and storage of all authentication and verification actions in the blockchain, along with corresponding timestamps. In addition to the users and FPGAs, this work also aims at securing the FPGA bitstream file from being tampered. An application of blockchain called Inter Planetary File Storage (IPFS) is utilized in this work to store the bitstream file [102]. IPFS is a blockchain based peer-to-peer file storage system, which allocates a unique hash for the stored file upon uploading [121]. This hash changes with every modified version of the uploaded file [102].

6.2.3 Authentication using ROPUFs

In conjunction with blockchain technology, the implementation and execution of the zero trust architecture are further reinforced by the utilization of ring oscillator physical unclonable functions (PUFs). PUFs serve as a Root-of-Trust (RoT) for the chips involved in the FPGA supply chain, focusing primarily on ensuring their security. The challenge and response pairs (CRPs) generated by the PUFs play a crucial role in authenticating and verifying the FPGAs. By leveraging the unique characteristics provided by the PUFs, the authentication process enhances the overall security of the supply chain, mitigating potential risks and ensuring the integrity of the FPGA devices.

6.3 Policy implementation

The individual roles of zero trust, blockchain, and ROPUFs in this research are elucidated in Section 6.2. This section delves into the functioning of blockchain and ROPUFs to fulfill the requirements of the zero trust tenets. While Table I provides an interpretation of the zero trust tenets, their practical implementation in this work is described as follows:

- Disparate resource set: This involves the management of different resources and granting user access only after verification. To achieve this, a multi-factor authentication scheme is integrated into the system.

- Independent security implementation across all resources: This ensures that only authorized individuals have access to the resources they should have access to. It involves providing the least privilege access or role-based access. This is accomplished through the use of modifier and event functions in the smart contract.

-Maintain traceability of access to all the resources: This involves maintaining a record and tracking of individuals who accessed the resources, along with the timestamp of their access and the actions they performed. This is accomplished through the traceability feature offered by the blockchain.

- Checking the provenance of the policy that determined the grant of access: This means that a record is maintained to track who accessed the resources, when they accessed them, and what actions they performed with the resources or the associated information. This level of tracking and accountability is enabled by the provenance feature provided by the blockchain.

- Preserve confidentiality: Critical information should be restricted to a specific set of participants and not accessible to others. The use of modifier functions in smart contracts helps in ensuring the confidentiality of such information, allowing access only to authorized participants.

-Maintain integrity of the process: Ensuring that individuals are carrying out their designated tasks is achieved through the use of a shared ledger, which is immutable. Every action or transaction occurring in the network is recorded and updated on the shared ledger, guaranteeing the integrity of the system.

-Persistent evaluation: This involves the collection of information and conducting persistent and rapid analysis. Constant monitoring of blockchain performance enables continuous evaluation and analysis of the system.

All of these policies have been developed in accordance with the principles established by NIST, as presented in Table 6.2. To enhance the effectiveness of these policies and create a secure perimeter around the supply chain, blockchain features and PUFs are employed. These technologies play a crucial role in verifying and authenticating every entity that attempts to access the network, thereby significantly reducing the possibility of unauthorized elements entering the system. By implementing these protocols, the FPGA supply chain establishes a robust and trustworthy environment for resource access.

Table 6.2: Zero trust tenets & their implementation

Policies	**Implementation**	**Feature utilized**
Disparate resource set	Multifactor Authentication	Blockchain/PUF
Independent security	Modifier function of smart contract	Blockchain/PUF
Traceability	Traceability feature of blockchain	Blockchain
Provenance	Provenance check feature of blockchain	Blockchain
Confidentiality	Modifiers in smart contract	Blockchain
Integrity	Immutability feature of blockchain	Blockchain
Persistent Evaluation	Monitoring the blockchain	Blockchain

The proposed zero trust architecture for the FPGA supply chain, as depicted in Figure 6-1, integrates various components and mechanisms to ensure authentication, access control, traceability, and security. The authentication and access control of the users is mainly done through the blockchain enabled MFA and FPGA is authenticated via CRPs obtained from ROPUF. The transactions performed in the network is updated on the shared blockchain ledger and hence are trackable and traceable. To maintain confidentiality and integrity of the assets, features offered by blockchain are utilized. Furthermore, this work enforces that all the devices used in the network are updated with latest security patches and all the computer codes are developed taking into consideration the concepts of secure coding, thus adhering to the ZT compliance. The zero trust policy engine evaluates and enforces all the policies formulated for the architecture. Upon enforcement of the protocols, access to the network resources is either allowed or blocked, depending upon the evaluation of the policies laid and their implementation. With these protocols in place, everything that enters the network to fetch access to the resources is verified and authenticated, with very less or no room for an untrusted element to enter the network.

6.4 Case Study: Pseudocodes and Simulation

The proposed approach is empirically tested in the authors' lab using Artix 7 Xilinx FPGAs mounted on a Nexys 4 Digilent board. The testing is conducted on the Ganache framework provided by the Truffle suite. Ganache is a personal blockchain designed for rapid development of Ethereum distributed applications. It offers both a UI and a CLI for development, deployment, and testing of dApps in a secure and deterministic environment. Ganache UI is a desktop application that supports Ethereum technology. It provides ten accounts, each with a hundred Ethers (for testing purposes only, not to be used in a real blockchain network), which can be used for transactions. These accounts allow for running tests, executing commands, and inspecting the blockchain state while controlling the operations on a personal Ethereum blockchain.

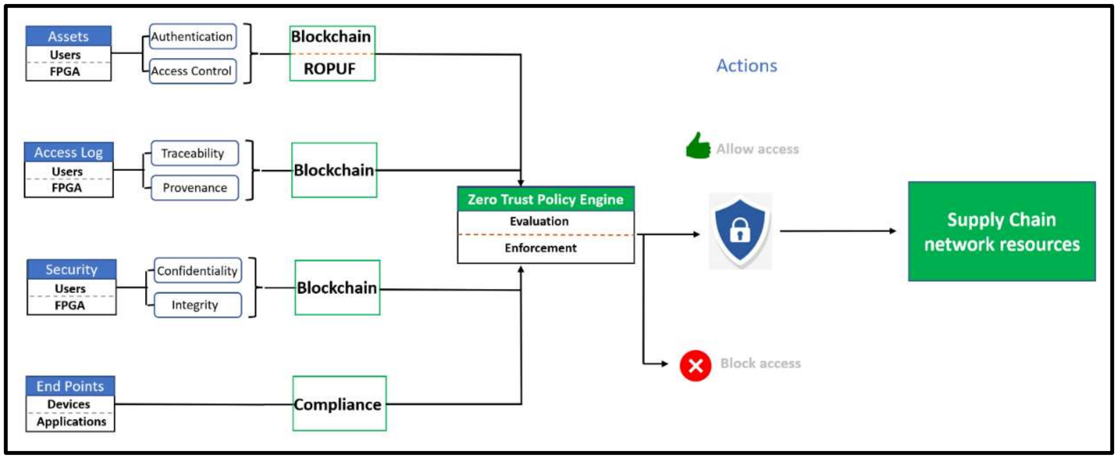


Figure 6-1: Zero trust architecture employed for the work

Firstly, the policies for the architecture are devised and the corresponding components required for their successful implementation are designed. These components include building a blockchain network (elaborated below), developing a smart contract and implementing ROPUFs on the FPGA boards to produce CRPs for authentication. The ROPUF has been designed as discussed in subsection C of Section III and the CRPs are generated using an Agilent 16801A logic analyzer as represented in Figure 6-2. These CRPs are stored in the blockchain for later authentication and validation.

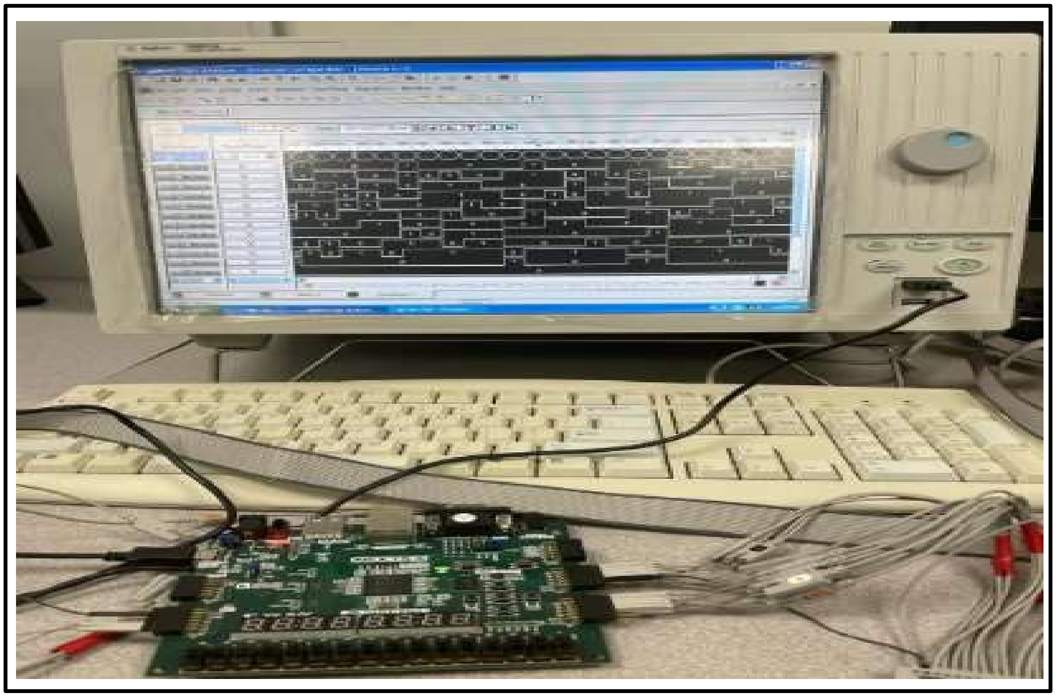


Figure 6-2: Lab set up to fetch CRPs from ROPUF

6.4.1 The blockchain network

The proposed model is centered around the FPGA supply chain network, which consists of participants, assets, and transactions. This forms the blockchain network that is established for the model, as outlined in Table 6.3. In the FPGA supply chain, the assets include the IP, bitstream file, and the FPGA itself. Ownership of these assets is transferred and accepted as they change hands between participants in the network. The participants in the network engage in the transactions such as registration, transfer, and acceptance of these assets.

Table 6.3: The blockchain network participants, assets and transactions

Sr. #	Participants	Assets	Access Controlled Transactions
1	3PIP vendor	IP	Registration of Participant, IP & Transfer of IP
2	Design House	IP/FPGA/Bitstream	Registration of Participant, FPGA & Accept of IP/Transfer of IP, Bitstream
3	Foundry	IP/FPGA	Accept and Transfer of IP and FPGA
4	OSAT	FPGA	Accept and Transfer of FPGA
5	OEM	FPGA	Accept of FPGA
6	Consumer	FPGA/Bitstream	Accept of FPGA, bitstream
7	Recycler	FPGA	Accept of FPGA

The developed application, which facilitates all transactions within the supply chain network, is blockchain-enabled. It incorporates smart contracts that provide role-based or least privilege access to users. The application also integrates a multi-factor authentication mechanism inspired by [122]. The smart contracts are not only responsible for access control but also for recording transactions within the network.

The first step involves creating and registering a user named 3PIP vendor in the blockchain network. The 3PIP vendor designs the IP cores for the FPGA using secure coding practices and ensuring the latest bug fixes. Once the IP cores are designed, they are sent to the design house. However, in order for the 3PIP vendor to access the device at the design house and complete its tasks, it must go through a role-based access process enforced by the function modifier in the smart contract. This ensures that the vendor is granted appropriate access privileges based on their role and responsibilities within the network.

After the IP cores are created, the 3PIP vendor follows a specific process before sending them to the design house. Instead of directly sending the IP cores, the 3PIP vendor uploads them onto the IPFS system. Once the IP cores are uploaded, the vendor registers them on the blockchain network. The smart contract includes a function modifier that ensures only the 3PIP vendor can perform these transactions, maintaining role-based and least-privilege access. After registration, the 3PIP vendor calls the transferIP() function in the smart contract, which is protected by the modifier only3PIP(). This initiates the transfer of the IP cores to the design house. Upon receiving the notification, the design house retrieves the IP cores from the IPFS system. The modifier function in the smart contract ensures that only the design house can request access to the IP cores. Once the IP cores are retrieved, the design house calls the acceptIP() function to signify their acceptance. Both the transfer and acceptance transactions are restricted by the modifier function, as depicted in Pseudocode 6.1. This ensures that only authorized participants can perform these actions in the FPGA supply chain network.

Pseudocode 6.1: Function Modifier

```
contract zeroTrustFPGA {
address authorizedParticipantAddress;
    //modifier to validate participant
modifier onlyAuthorizedParticipant() {
    require(msg.sender == authorizedParticipantAddress,
        “Only Authorized Participant can perform this Operation.”);
            _;
}}
```

Modifier functions are developed and implemented throughout the supply chain network to control access for all users, including the foundry, OSAT, OEM, and consumer. These modifier functions enforce role-based and least privilege access controls, ensuring that each participant can only perform authorized actions within their role. Once the design house initiates the transfer of the asset, in this case, the layout file for the FPGA IPs, the foundry is notified. However, the access granted to the foundry is not only role-based but also time-based. The foundry can only start accessing the network after the transfer event is successfully completed. This time-based access control is implemented using an event function in the smart contract, as shown in Pseudocode 6.2. The event function ensures that access is granted only after the specified event or task, in this case, the completion of the transfer, is successfully executed. By incorporating these modifier functions and event-based access controls, the proposed model ensures that participants in the FPGA supply chain network can only access the network and perform actions according to their roles and the successful completion of relevant events or tasks.

Pseudocode 6.2: Events Function

```
contract zeroTrustFPGA {
    //event to trigger an action
event transferInitiated(address currentOwner, address newOwner);
    //function to initiate transfer of an asset
function transferOwnership () ….. {
  //code to execute transfer of ownership of an asset
emit  transferInitiated (currentOwner, newOwner);
}}
```

By implementing event functions at each stage of the supply chain, time-based access control is enforced, preventing unauthorized access attempts by potential attackers. At the foundry stage, the FPGA undergoes fabrication and is embedded with a ROPUF, which generates unique CRPs (Challenge-Response Pairs). Starting from this stage, the FPGA goes through authentication at each step of the supply chain. During each transaction, the current owner of the FPGA verifies its authenticity by providing the CRPs as inputs. The blockchain then compares the input CRPs with the stored CRPs and declares the FPGA authentic if they match. The pseudocode for this FPGA validation process is presented in Pseudocode 6.3. This validation mechanism ensures that the authenticity of the FPGA can be verified at any point in the supply chain by utilizing the CRPs generated by the ROPUF. By integrating this process into the blockchain, the model establishes a secure and trusted environment for FPGA authentication and prevents the use of counterfeit or tampered FPGAs.

Pseudocode 6.3: IC Validation using PUFs

```
contract zeroTrustIC {
  //modifier function to validate current owner
  // similar to ALGORITHM 1
  //function to validate IC
function validateIC(challenges, responses) onlyCurrentOwner(){
  if (challenges && responses == stored CRPs){
      return true;
  }
else {
        return false; }}}
```

Continuing the authentication and verification process, the current owner of the FPGA is responsible for performing these actions at each stage of the supply chain. Pseudocode 6.3 illustrates how the current owner utilizes the CRPs generated by the ROPUF to authenticate and verify the FPGA. This process ensures that the FPGA's authenticity is confirmed by the owner at every step, maintaining the integrity and security of the supply chain. All the transactions taking place within the blockchain network are recorded on a shared ledger, ensuring transparency and accountability. The provenance of these transactions can be traced back, allowing for a comprehensive view of the entire supply chain. The immutability feature of the blockchain ensures that the recorded data cannot be tampered with, providing a high level of integrity. By implementing a blockchain monitor, the supply chain transactions can be consistently supervised, analyzed, and evaluated. This monitoring mechanism helps in detecting any anomalies or suspicious activities, contributing to the overall security of the network. Through this experiment, all the formulated policies were successfully implemented, resulting in the establishment of a secure perimeter around the network. The combination of blockchain, and ROPUFs contribute to the successful implementation of a zero trust model leading to the overall security and trustworthiness of the FPGA supply chain.

Note that this experiment, has been successfully implemented on Ganache in the research lab, and it can also be migrated on Ethereum Mainnet. However, deploying it and executing the transactions on the real network would cost real Ethers and hence was only tested on the test network and not on actual blockchain network.

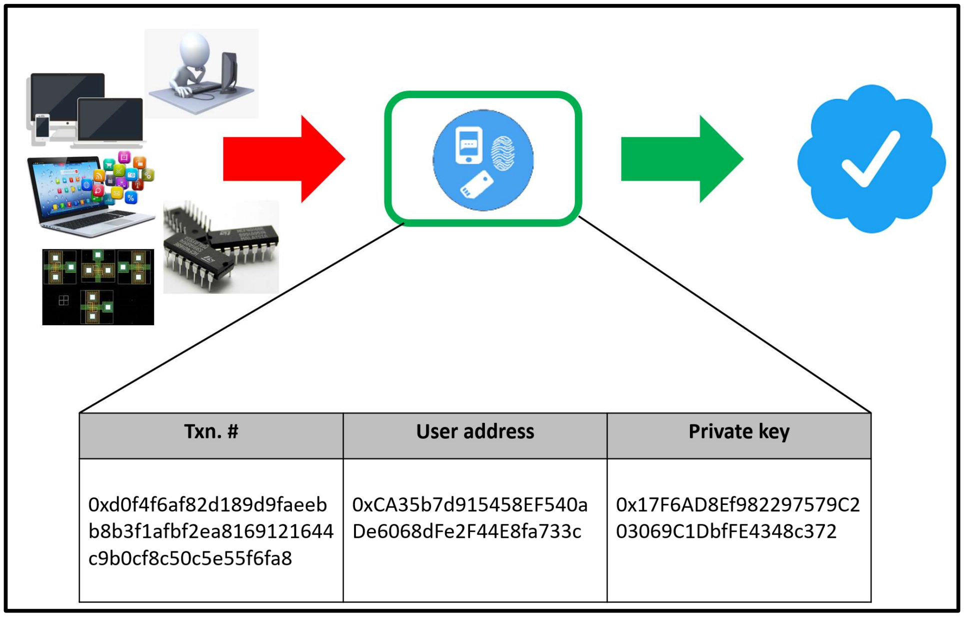
6.5 Tenet evaluation

The zero trust tenets laid down by NIST are successfully satisfied in this investigation. This section discusses each tenet and evaluates it with an attack scenario.

6.5.1 Tenet 1: Disparate resource set

To ensure that all users, traffic, data, assets, and applications attempting to access the network, or its components undergo a thorough verification process implementation of a multi-factor authentication (MFA) scheme is crucial. This MFA scheme is adopted from [122], with modifications as per the proposed work. For the authentication of the chips, the ROPUF is designed as elaborated in subsection 1 of C of Section III. Failure to validate itself, leads to rejection of access, keeping a check on unauthorized elements from entering the network.

For example, consider an employee at a third-party intellectual property (3PIP) vendor who wishes to access the system where the IP cores are stored or designed. The employee is required to undergo a verification process using the MFA scheme. The user's credentials are checked, and based on the authentication result, the MFA scheme either grants or denies access to the system. In genuine scenarios, if the user passes the verification, they are allowed to access the system. However, in this proposed work, an additional MFA protocol is also introduced for accessing the electronic design automation (EDA) tools. Upon successful verification, the user gains access to the system, EDA tools, and eventually the IP cores. Similarly, any other user or entity attempting to access the network, or its components must go through the MFA scheme for verification. This requirement makes it challenging for an adversary to gain unauthorized access to the network. In addition to the users, the FPGAs also require authentication provided by CRPs from the ROPUF. The implementation of this tenet is depicted in Figure 6-8, showcasing how the MFA scheme is employed to verify users and ensure authentication before granting access to the network or its components. The integration of the ROPUF for chip authentication is also illustrated.



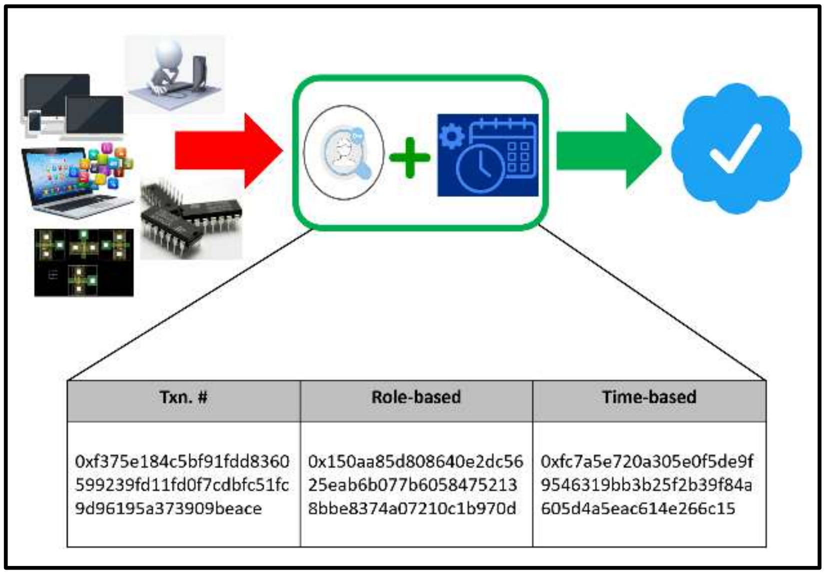
Txn. #	User address	Private key
0xd0f4f6af82d189d9faeebb8b3f1afbf2ea8169121644c9b0cf8c50c5e55f6fa8	0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c	0x17F6AD8Ef982297579C203069C1DbfFE4348c372

Figure 6-3: Representation of implementation of Tenet 1

6.5.2 Tenet 2: Independent security

Enforcing access control and least-privilege access is a critical policy in the FPGA supply chain network to ensure that only authorized entities with specific roles and scheduled access are granted entry. This policy limits the access sought by users, traffic, applications, data, or assets, restricting unauthorized and untimely access to the network. By implementing this policy, the network maintains a strict control over who can access specific elements or perform particular tasks based on their role and the designated time of access. If an entity is not required or scheduled to perform a specific task, their access to the network or element is denied.

Consider an employee in the design house who is assigned the duty of gate-level netlist synthesis. With this policy in place, the employee will only be granted access to the network if their role is verified as a gate-level netlist synthesis engineer and if the previous step, such as HDL coding and verification, has been completed. This ensures that the employee is restricted from accessing the RTL code and that only the necessary users are present in the network, facilitating easier monitoring. By implementing access control and least-privilege access, the network reduces the overall traffic and limits the number of users accessing the network at any given time. This restriction makes it easier to supervise and monitor the network activities, enhancing security and accountability. Furthermore, this policy helps in pinpointing any wrongdoing or malicious activity that may occur during a specific step or task. In the case of a wrongdoing during gate-level synthesis, the access logs and restricted access can help identify the culprit more easily. The implementation of this tenet is depicted in Figure 6-4, illustrating how access control and least-privilege access are enforced in the network, ensuring that only authorized entities with specific roles and scheduled access can gain entry to the network or its elements.



Txn. #	Role-based	Time-based
0xf375e184c5bf91fdd8360599239fd11fd0f7cdbfc51fc9d96195a373909beace	0x150aa85d808640e2dc5625eab6b077b60584752138bbe8374a07210c1b970d	0xfc7a5e720a305e0f5de9f9546319bb3b25f2b39f84a605d4a5eac614e266c15

Figure 6-4: Representation of implementation of Tenet 2

6.5.3 Tenet 3: Traceability

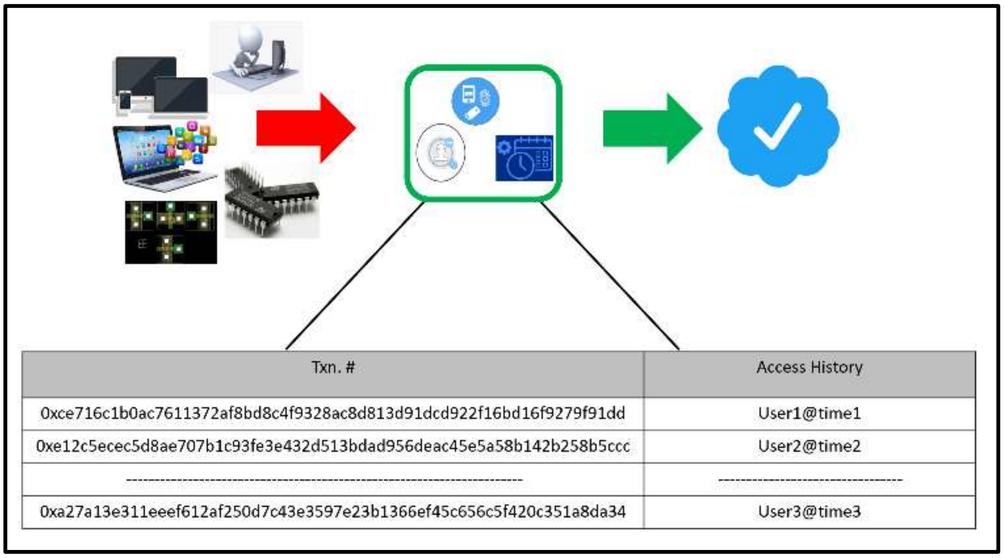
Tracking the activities and access of network elements is a crucial aspect of maintaining security and accountability within the FPGA supply chain network. The blockchain technology, with its shared ledger and timestamping feature, enables the tracking of transactions and access events [97]. Once an element within the network successfully passes the verification and access control process, their actions and access to specific resources are recorded on the shared ledger. This includes details such as the element's identity, the resource accessed, and the timestamp of the access event.

For example, consider the case of a mask writer in the fabrication stage who gains access to the layout file for converting it into a reticle. The authentication and access control processes are carried out, and the successful access by the mask writer is recorded on the blockchain ledger with a timestamp. By maintaining a log of these access events with timestamps, the network can effectively track and monitor the activities of each element. This provides visibility into who accessed which resources and at what time. In case of any suspicious activity or potential wrongdoing, the access logs can be analyzed to identify any adversaries or confirm any suspicions. The implementation of this tenet in the network is depicted in Figure 6-5, showcasing how the access events and transactions are recorded on the blockchain ledger with timestamps.

6.5.4 Tenet 4: Provenance

Tracking the transactions and maintaining their provenance is an important aspect of ensuring the integrity and accountability of the FPGA supply chain network. The blockchain technology provides a provenance feature, enabled by the timestamp associated with each transaction recorded on the shared ledger [124]. This tracking capability plays a crucial role in monitoring the network and ensuring that the processes within the supply chain are running as intended.

All the traffic that goes through the access control and verification, is stored on the shared ledger as described in the previous tenet. However, just storing the transactions does not satisfy the zero trust architecture. These transactions should be tracked back to their inception, making sure the process is running in the way it was determined. For instance, an FPGA is fabricated and sent to the OSAT for testing and packaging. If this transaction is not stored in the ledger and not able to be tracked, then any fraudulent activity happening in this phase, would be difficult to be investigated. Being able to track back the transactions, gives an upper edge in finding the guilty party, if one. Implementation of this tenet is similar to that of Tenet 3, hence represented in Figure 6-5.



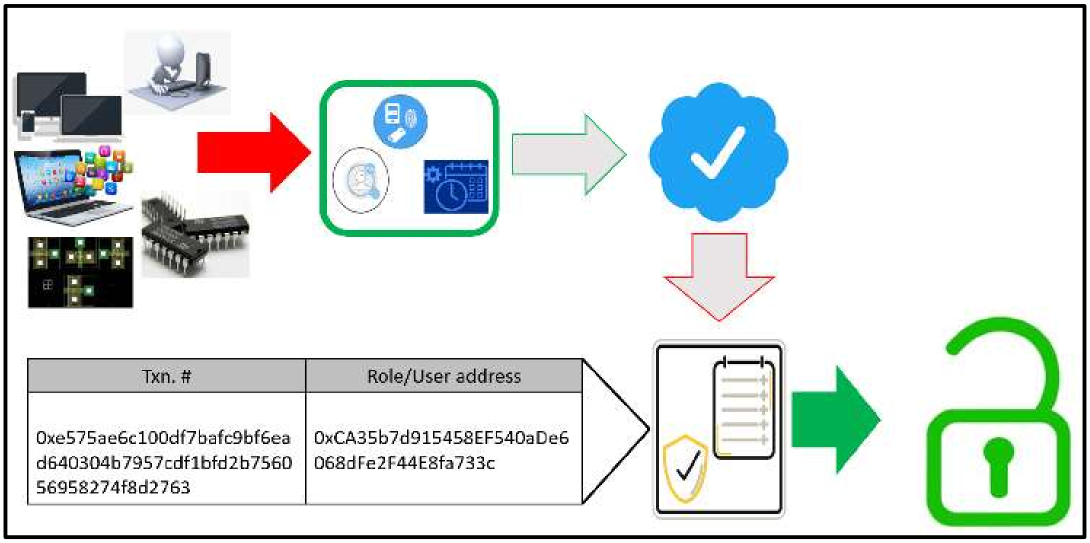
Txn. #	Access History
0xce716c1b0ac7611372af8bd8c4f9328ac8d813d91dcd922f16bd16f9279f91dd	User1@time1
0xe12c5ecec5d8ae707b1c93fe3e432d513bdad956deac45e5a58b142b258b5ccc	User2@time2
--	---------------------------------
0xa27a13e311eeef612af250d7c43e3597e23b1366ef45c656c5f420c351a8da34	User3@time3

Figure 6-5: Representation of implementation of Tenet 3 & 4

6.5.5 Tenet 5: Confidentiality

Confidentiality of sensitive information is a critical aspect of the FPGA supply chain, as the exposure of such data can lead to security concerns and the production of counterfeit chips. In the proposed architecture, the smart contract functionality is leveraged to enforce access control policies. Function modifiers within the smart contract allow for permission-based access to specific data or resources within the network. This means that only authorized users who require access to certain sensitive information will be granted the necessary permissions. To obtain permission to access specific data, users must go through the verification process implemented by the first two tenets of the proposed architecture. This verification process ensures that only authenticated and trusted users are granted access to sensitive information.

By implementing this policy, the risk of sensitive data leakage is mitigated. For example, in the case of the OSAT requiring predetermined results of FPGAs for testing, access to this information would be restricted to authorized personnel only. This prevents unauthorized individuals, such as a rogue employee in the foundry, from accessing and misusing the data. If sensitive data were to be leaked and reach a rogue employee, they could potentially manufacture counterfeit FPGAs and input matching verification results to hide any wrongdoing. However, with this tenet being satisfied, only authorized users with the necessary permissions can access and modify data on the blockchain. This ensures that any actions performed are attributed to the responsible and authorized parties, increasing accountability and maintaining the integrity of the supply chain. Figure 6-6 visually represents the implementation of this policy, illustrating how access to sensitive data is regulated and controlled, preventing unauthorized access and safeguarding the confidentiality of information within the FPGA supply chain network.



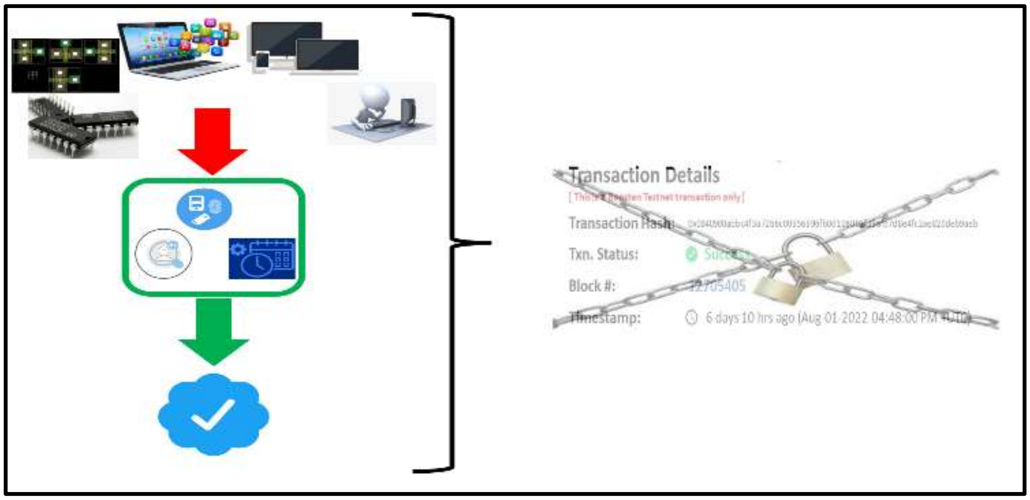
Txn. #	Role/User address
0xe575ae6c100df7bafc9bf6ead640304b7957cdf1bfd2b756056958274f8d2763	0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c

Figure 6-6: Representation of implementation of Tenet 5

6.5.6 Tenet 6: Integrity

Maintaining the integrity of the FPGA supply chain network and ensuring the accountability of each participant is crucial for its security. The use of blockchain technology, with its immutability feature, helps address these requirements [125]. By leveraging the immutability feature of blockchain, the proposed approach records every job or action performed by any party in the network on the shared blockchain ledger. This means that the responsibilities and activities of each participant are permanently recorded and cannot be modified retrospectively. This enables continuous monitoring and accountability within the supply chain.

For example, an OSAT is accountable for testing the manufactured semiconductor chip, but if the OSAT outsources this job to a third party tester, the sensitive testing data is leaked and in case of an untrusted third party tester, it may cause issues with the chips. Hence, it is significant that every job that is done by any party in the network is recorded on the blockchain network, which is immutable as shown in Figure 6-7. This results in monitoring the actions of every party involved, promoting transparency, accountability, and trust in the FPGA supply chain network.



Transaction Details

[This is a Ropsten Testnet transaction only]

Transaction Hash:

Txn. Status: Success

Block #: 12705405

Timestamp: 6 days 10 hrs ago (Aug 01 2022 04:48:00 PM +UTC)

Figure 6-7: Representation of implementation of Tenet 6

6.5.7 Tenet 7: Persistent Evaluation

Constant monitoring and auditing are vital for the proper functioning of the supply chain, particularly when it involves heavy traffic of users, data, applications, and assets from around the world. Monitoring helps in continuously evaluating and analyzing the activities within the supply chain, ensuring that everything is functioning as intended.

Persistent evaluation of the network helps in monitoring the network, which is very important for the successful implementation of a zero trust architecture. If the network experiences any disruption or malfunctions, it can potentially compromise the integrity and security of the transactions. Constant supervision of the blockchain network helps in identifying any potential vulnerabilities or attacks that could be exploited by adversaries. It allows for timely responses and mitigations to prevent unauthorized access or malicious activities that could compromise the security of the architecture and the FPGAs within the supply chain.

Implementation of a zero trust architecture, using blockchain and ROPUF, has been attempted for the first time in the FPGA supply chain domain, to the best of our knowledge. Zero trust inspired the policies to be formulated for securing the FPGA supply chain network, while implementing these policies was successfully achieved by blockchain technology, and ROPUFs. All the policies formulated and implemented helped in building a secure perimeter around the supply chain network by first eliminating the trust in all the elements and then verifying them. Many challenges faced by the FPGA supply chain network like IP theft, hardware trojan intrusion and others, were realized during this investigation. Table 6.4 provides a comparison of the proposed approach with some previous literature, on the concepts implemented to secure the FPGA supply chain.

Table 6.4: Comparison of presented work with previous work

Concepts/Prior work	[9] - 2019	[14]-2022	[20]-2019	[21]-2019	[97]-2018	This work
Hardware Oriented Security (PUFs)	✗	✗	✓	✓	✓	✓
Blockchain technology	✓	✗	✓	✓	✓	✓
Zero Trust	✗	✓	✗	✗	✗	✓

6.6 Summary

The presented chapter aims towards creating a novel zero trust FPGA supply chain by combining the concepts of blockchain, and ROPUF. The architecture is designed to eliminate blind trust and ensure that every user or element accessing the supply chain resources undergoes a thorough verification process. The smart contract, which forms the core of the blockchain component, is developed in Solidity on Remix IDE. A 5-stage ROPUF, with 256 ring oscillators, is also designed as part of the proposed architecture, which are used to generate unique CRPs for authenticating the FPGAs in the supply chain. A case study is simulated on Ganache framework to demonstrate the practical implementation and functionality of the architecture. To evaluate the effectiveness of the architecture, the tenets of zero trust are examined through various attack scenarios. This analysis helps to identify potential vulnerabilities and assess the robustness of the proposed framework against different security threats. Table 6.5 showcases the significance of this work by highlighting that the integration of blockchain, and ROPUFs for implementing a zero trust architecture to secure the FPGA supply chain is introduced for the first time. The proposed framework provides a higher level of trust and security, preventing malicious actors from infiltrating the FPGA supply chain.

Chapter 7

Supplementary Blockchain applications in Microelectronics Security

The globalization of integrated circuits (ICs) introduces challenges in maintaining the quality and integrity of the ICs due to potential involvement of untrusted entities in the supply chain. One prominent challenge is Intellectual Property (IP) piracy, which leads to significant revenue losses for third-party IP vendors (3PIP vendors) and design houses. The increasing trend of design re-use exacerbates this issue. Furthermore, malicious actors can engage in reverse-engineering of layout design files to obtain gate-level netlists and falsely claim ownership of designs. Extensive research has been conducted to protect IP from theft and piracy, but as attacks become more sophisticated, there is a pressing need for further research to combat these malicious activities targeting hardware IP. The challenges faced by the supply chain are not limited to the pre-fabrication phase; the fabrication phase also presents significant hurdles. Instances of chips infiltrating the supply chain with covertly implanted Trojans have been well-documented. Studies have identified tampering with lithographic masks, known as reticles, as one potential source of hardware Trojan intrusion.

To address these issues, this chapter presents a novel technique for hardware IP transfer by converting the layout file into a non-fungible token (NFT). Leveraging the blockchain-powered concept of NFTs, this investigation incorporates essential features such as decentralization and uniqueness. Additionally, a novel blockchain-enabled mask writing technique is introduced to mitigate alterations to the IC layout design during the mask-making step. The study explores a blockchain-enabled file storage and transfer system for secure transmission of the layout GDSII file from the design house to the mask-making machine. As part of this research, a smart contract is developed to interact with an external application programming interface (API) and retrieve the design layout file from the file storage system. The proposed smart contracts, implemented using Solidity language, can be integrated into existing Electronic Design Automation (EDA) tools for mask making, effectively limiting access sought by adversaries during the mask-making process. The development of these smart contracts is carried out using the Remix online integrated development environment (IDE). Finally, two case studies are presented to illustrate the application of the two techniques discussed in this chapter.

7.1 Relevant concepts

This section discusses the relevant concepts and background for the work in this chapter.

7.1.1 Hardware IP

In the modern semiconductor supply chain, participants from different regions collaborate to ensure its success [2]. Third Party IP vendors (3PIP vendors) play a crucial role by providing Intellectual Property (IP) [10]. In the semiconductor industry, IP refers to pre-defined blocks of a circuit that can be seen as standalone components of a complete System-on-Chip (SoC) design [126]. These IPs originate from the ideas of designers affiliated with 3PIP vendors or design houses. The growing complexity of SoC designs has led to a rise in the adoption of design reuse practices [127]. However, this trend has also brought about concerns regarding IP piracy within the IC design community [128]. In the field of assured and trusted microelectronics, the challenges related to IP can be categorized as follows and as shown in Figure 7-1:

- IPs being used without paying the requisite fees to the 3PIP vendors [129]
- Design houses illegally selling IPs obtained from 3PIP vendors to other parties [130]
- Design houses using more than the permitted instances of 3PIP [131].
- Companies performing post–silicon reverse-engineering to derive the design layout database of an IC to manufacture illegal "clones" [132].
- Insertion of hardware Trojan in the IP cores to infect the eventual integrated circuit (IC) [133].

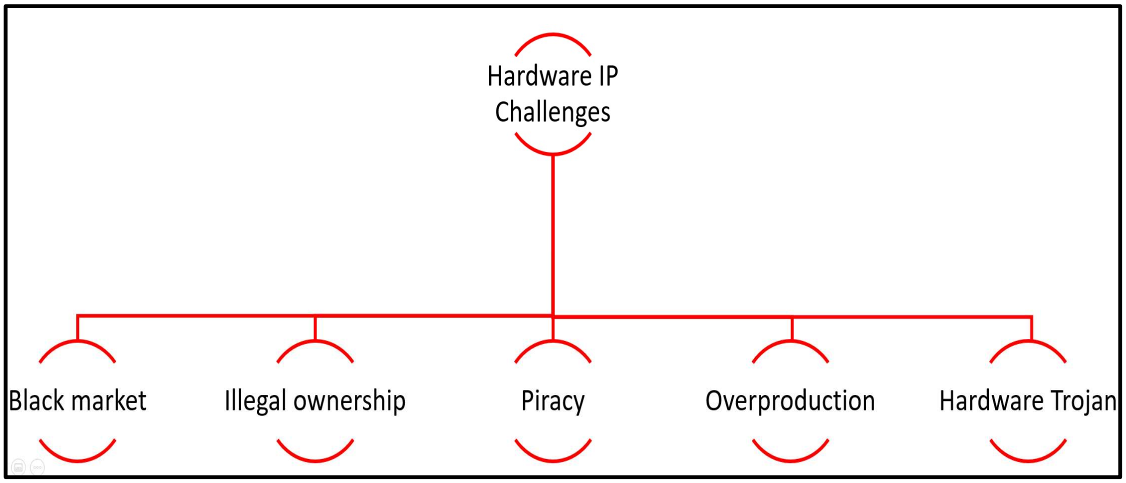


Figure 7-1: Types of challenges faced by hardware IP

These challenges have had a significant impact on the semiconductor industry. According to a study conducted by the U.S. Department of Commerce, IP-intensive industries account for 38% of the American economy, and they experience annual losses ranging from $225 billion to $600 billion due to IP theft by untrusted companies, particularly in the semiconductor sector [134], [135], [60], as reported by the U.S. Trade Representative. In light of these evident issues, the field of assured and trusted microelectronics has witnessed extensive and rapid research. This research encompasses various areas such as SoC design security, secure fabrication, supply chain integrity and security, protection against IP theft and piracy, and more.

As technology continues to advance at a rapid pace, potential adversaries are also becoming more capable of gaining unauthorized access to valuable intellectual property. The existing protection techniques may not be sufficient to deter these sophisticated attacks, as technology improves rapidly. Adversaries are actively seeking ways to gain an upper hand, putting third-party IP vendors and design houses at risk of significant financial losses and reputational damage. Therefore, there is a pressing need for a foolproof technique to protect intellectual property. To address this challenge, a part of the work presented in this chapter introduces the concept of Non-Fungible Tokens (NFTs) for securing hardware IP. NFTs are used to convert IP cores and design layout files into unique digital assets. The design layout files are commonly stored in GDSII or OASIS formats. For the sake of consistency, this paper will refer to them as layout files throughout.

7.1.2 Non-Fungible Tokens (NFTs)

An NFT, or Non-Fungible Token, represents a digital asset that is unique and cannot be replaced or replicated. By tokenizing an asset, it ensures that the ownership is securely established, and the asset's uniqueness is preserved. In the case of hardware IP, the ownership of NFTs is managed in a decentralized manner by the blockchain. The decentralized nature of blockchain technology allows for the automatic allocation of IP rights to the creator of the IP/NFT. This means that the rightful owner of the NFT retains the IP rights, and the new owner of the NFT is legally prohibited from modifying or creating copies of the asset without the explicit permission granted through the blockchain smart contract. Smart contracts play a crucial role in maintaining control over IP modifications. They provide a mechanism for monitoring and enforcing the rules and conditions set by the IP owner. By leveraging the features of uniqueness, decentralized ownership rights, and irreplaceability offered by NFTs, the proposed work aims to protect hardware IP from being stolen or pirated.

7.1.3 Mask-writing

Trusted integrated circuit design has become a significant area of research due to the globalization and outsourcing of IC fabrication to offshore foundries. This shift has resulted in the establishment of a global supply chain in the semiconductor industry. However, this outsourcing introduces the potential threat of tampering with the original IC design by third-party manufacturers. One such group of third-party manufacturers is the mask makers, who are responsible for producing the photomasks or reticles used in the fabrication process. The mask making process is vulnerable to circuit modification, which can result in the production of masks with maliciously inserted Trojans. This poses a significant risk to the overall integrity and security of the semiconductor supply chain. In a typical semiconductor supply chain setup, the mask making process can be conducted through various arrangements. It can be done in partnership with foundries, performed in-house by the foundry itself, or outsourced to specialized companies. Foundries often collaborate with companies such as ASML or utilize their machines for the mask writing process, ensuring the accuracy and quality of the masks.

Figure 7-2 illustrates the typical process that occurs after the tape out stage, leading up to the lithography process in IC fabrication. In this process, the SoC designer, also known as the design house, utilizes third-party Electronic Design Automation (EDA) tools to integrate all the IP cores and generate a layout file for the IC design. This layout file is commonly in the GDSII or OASIS format, but for consistency, it is referred to as GDSII throughout this paper. The design house then transfers the GDSII file to the foundry, which is responsible for converting the design into a physical IC. Depending on its manufacturing capabilities, the foundry may outsource the mask manufacturing process to a mask maker. The GDSII layout file is provided to the mask maker, who produces a mask that is utilized in the subsequent lithography process. The lithography process transfers the circuit pattern from the mask onto a wafer die, forming the basis of the IC. It is important to note that this paper does not delve into the intricacies of the mask manufacturing process. However, interested readers can refer to references [143] and [144] for more information. Additionally, Figure 7-2 includes the representation of a rogue mask maker to highlight the potential adversary model. For the purpose of this investigation, it is assumed that the GDSII layout file received from the design house is free of any hardware Trojans. However, it is worth noting that the manipulation of the GDSII layout file has become a significant source of concern, as it can lead to the production of counterfeit ICs and raise serious hardware security issues [9].

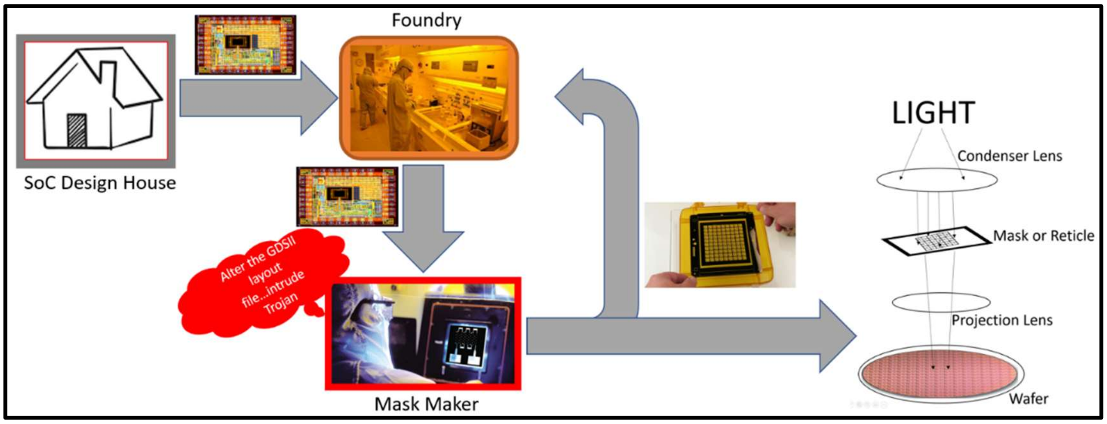


Figure 7-2: A typical post tape out setup and possible attack

It is estimated that the counterfeiting of ICs results in an annual loss of approximately $100 billion [2]. Furthermore, reports indicate that around 15% of spare and replacement parts in the U.S. Department of Defense (DoD) are counterfeit [98]. These alarming statistics highlight the significant challenges posed by counterfeiting in the semiconductor industry. To address these challenges, a novel mask writing process is presented in this chapter, leveraging the power of blockchain technology to minimize human intervention. The proposed approach involves the use of a smart contract that interacts with an external application programming interface (API) to directly retrieve the GDSII file from a blockchain-enabled file storage system. The retrieved file is then uploaded to the mask making machine. Additionally, the EDA tool is employed to automate the process of imprinting the GDSII layout onto a substrate made of fused silica or glass. The substrate is coated with an opaque film, resulting in the creation of a photomask. This automated process helps streamline the mask writing process and reduces the potential for human errors or unauthorized modifications. By incorporating blockchain technology and automation, this approach aims to enhance the security and integrity of the mask making process, mitigating the risks associated with counterfeit ICs.

7.2 NFTs for IP protection

The proposed work in this section suggests leveraging NFTs to enhance the security and ownership rights of hardware IP in the semiconductor industry. The process is depicted in Figure 7-3. The IP cores, developed by the Third-Party IP (3PIP) vendors, are converted into NFTs to create unique digital assets. Each IP core is assigned a corresponding tokenId, which serves as its unique identifier. The metadata of these NFTs, representing the IP cores, is stored in a blockchain-powered file storage system called the Interplanetary File System (IPFS). The 3PIP vendor shares the tokenId of the NFT-converted IP cores with the design house, which uses this tokenId to retrieve the IP cores from the IPFS. The design house integrates these IP cores and creates a layout file, which serves as a blueprint for the chip design. Similar to the 3PIP vendor, the design house converts the layout files into NFTs and obtains their corresponding tokenIds. The design house then shares the tokenId of the NFT-converted layout files with the foundry for the fabrication process. The foundry can fetch the layout file from the tokenId but only has restricted "view only" access to the NFT-converted layout files. This ensures that the foundry does not hold ownership or authority over the NFTs and the layout files. By converting IP cores and layout files into NFTs and managing their ownership on the blockchain, this approach provides a secure and traceable method for protecting hardware IP in the semiconductor supply chain.

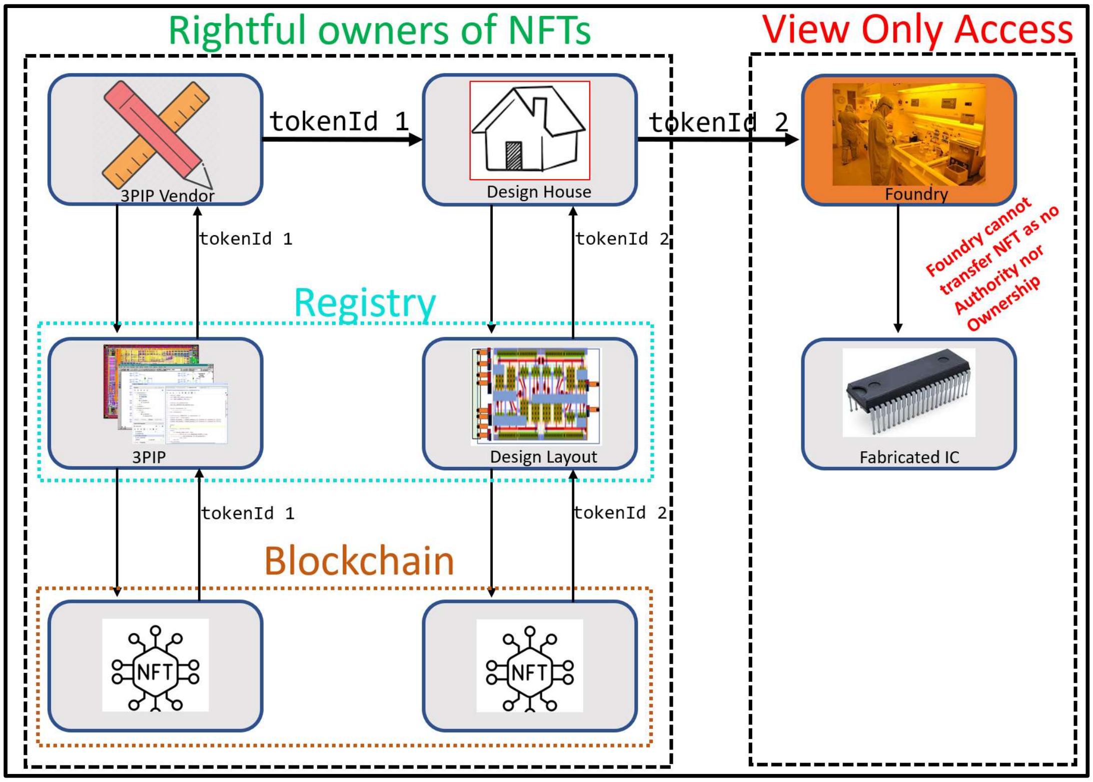


Figure 7-3: Employing NFTs for IP protection

In the proposed system, the ownership of the NFTs representing the IP cores and layout files is managed in a decentralized manner on the blockchain. The 3PIP vendor and design house are the rightful owners of their respective NFTs. The ownership of these NFTs cannot be transferred to any other party without the permission of the legal owners, ensuring that the IP remains protected and under the control of the authorized entities. This decentralized ownership model adds an additional layer of security and prevents unauthorized access or transfer of the NFTs and the underlying hardware IP.

7.2.1 Implementation of the technique

A single smart contract has been developed to achieve the objectives of the investigation. This smart contract encompasses eight functions that play essential roles in the successful implementation of the technique. The functions of the smart contract and their respective roles are presented in Table 7.1. The smart contract for NFT minting and transferring is designed in a way that does not grant any authority over the NFTs to the foundry. This is achieved by incorporating a function modifier [24]. Additionally, the design of the smart contracts restricts the transfer or modification of the NFTs to only the 3PIP vendor or the design house, who are the rightful owners of the NFTs. Consequently, the ownership of the NFTs remains with the designated owners, thereby ensuring protection against modification, piracy, and theft of the IP cores and layout files.

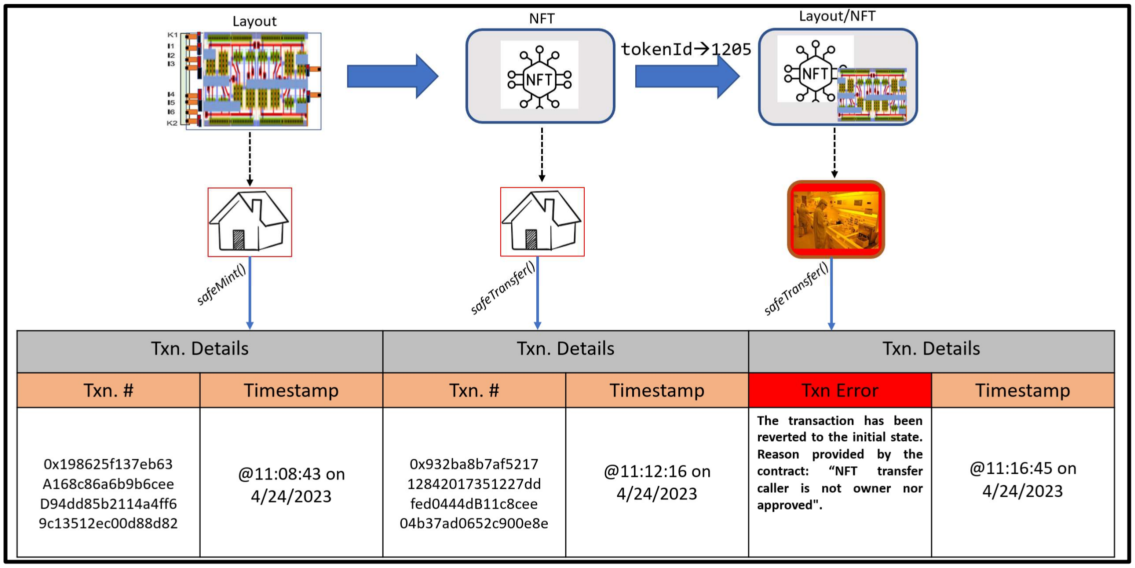
Table 7.1: Smart contract functions and their details

Sr. #	**Function**	**Role**	**Caller**
1	*safeMint()*	Mints the NFT	3PIP vendor/Design House
2	*safeTransfer()*	Transfer NFT	3PIP vendor/Design House
3	*grantRole()*	Grants authority to transfer NFT (if required)	3PIP vendor/Design House
4	*hasRole()*	Confirms role of a participant	Any Participant
5	*revokeRole()*	Revokes authority granted	3PIP vendor/Design House
6	*balanceOf()*	Returns number of NFTs with a participant	Any Participant
7	*name()*	Returns name of NFT	Any Participant
8	*ownerOf()*	Returns owner information of NFT	Any Participant

7.2.2 Case study: Security threat evaluation

This section presents a case study of the proposed technique simulated on Remix IDE. The simulation focuses on the interactions between the design house and the foundry, although the participation of the 3PIP vendor is assumed. In the simulation, after the design house combines the 3PIP cores and adds its own IPs, it prepares the layout file for tape out. However, before sending the layout file to the foundry, which is considered untrusted, the design house converts it into an NFT by invoking the safeMint() function from the smart contract. This transaction generates a unique tokenId for the minted NFT. The transaction details are stored on the blockchain shared ledger, associated with the transaction hash, while the layout file itself is stored on the IPFS registry, linked to the tokenId. It is important to note that the safeMint() function is implemented with a function modifier, ensuring that only the authorized user, in this case, the design house, can mint an NFT of the layout file. If any other user attempts to call this function, an error message will be displayed, indicating their lack of authority. By utilizing the function modifier and associating ownership information with the transaction hash and tokenId, the proposed technique establishes a secure and controlled process for minting NFTs, ensuring that only the rightful owner, in this case, the design house, has the authority to create NFTs of the layout files.

The tokenId of the NFT is then sent to the foundry by the design house using the safeTransfer() function in the smart contract. However, it is important to note that the legal ownership of the layout file remains with the design house. Similar to the safeMint() function, the safeTransfer() function also includes a function modifier that prevents unauthorized users, including the foundry, from transferring the NFT. In the presented scenario, the foundry is not authorized to transfer the NFT, so any attempt by the foundry to transfer the NFT would be deemed invalid and flagged by the network. Figure 7-4 illustrates a scenario where the foundry is considered an untrusted entity. However, it is worth mentioning that this technique is not only effective in identifying pirated IPs at different stages of the supply chain, but it also enables the identification of the responsible party by recording timestamps stored in the blockchain as the IP progresses through the supply chain. This provides a means to trace the IP's journey and detect any unauthorized modifications or ownership transfers along the way.



Txn. Details		Txn. Details		Txn. Details	
Txn. #	Timestamp	Txn. #	Timestamp	Txn Error	Timestamp
0x198625f137eb63 A168c86a6b9b6cee D94dd85b2114a4ff6 9c13512ec00d88d82	@11:08:43 on 4/24/2023	0x932ba8b7af5217 12842017351227dd fed0444dB11c8cee 04b37ad0652c900e8e	@11:12:16 on 4/24/2023	The transaction has been reverted to the initial state. Reason provided by the contract: “NFT transfer caller is not owner nor approved".	@11:16:45 on 4/24/2023

Figure 7-4: Security threat evaluation simulation result

7.3 Blockchain-enabled mask writing

There are various EDA tools available for mask making that streamline the process of imprinting layout patterns onto the chrome substrate with a simple click of a button. These tools prepare the necessary data from the GDSII files, which contain the IC design. During this step, there is a potential risk of a Trojan circuit being prepared and inserted into the design file. If this Trojan circuit goes unnoticed and gets imprinted onto the mask along with the rest of the design, it poses a significant security risk [141]. To address this issue, this section proposes a blockchain-enabled approach for mask writing, aiming to prevent unauthorized access to the GDSII file by potential adversaries. In this approach, only trusted and authorized users, such as the design house, are allowed to upload the GDSII file onto a secure blockchain-enabled file storage system. This is achieved through the use of a modifier function in the smart contract. The file storage system used in this work is developed externally using Inter Planetary File Storage (IPFS) [102], [104]. After uploading the GDSII file, the file storage system generates a hash for the uploaded file, which is then provided to the mask writer for further processing.

PSEUDOCODE 7. 1: File Storage System

```
contract maskWriting {
      //modifier to validate designer
    modifier onlyAuthorizedUser() {
     require(
       msg.sender == authorizedAddress,
       "Only Authorized user can perform this operation");
         _;
    }
      //function to upload test file to storage system
     function uploadFile(testFile) {
          /**Authorized User uploads the GDSII layout file**/
             return (ipHash)
          /** The file storage system returns the hash of the file **/

    }}
```

When the mask writer requires the GDSII file for mask writing, they provide the hash of the file as an argument to the fetchFile(ipHash) function in the smart contract. The smart contract then interacts with the file storage system to retrieve the GDSII file directly and uploads it to the mask making machine. This interaction with the external API is facilitated by another smart contract that is specifically designed for blockchain oracles [146]. Blockchain oracles are smart contracts that address the limitation of connecting smart contracts to the external world [147]. In this case, a blockchain oracle smart contract is created to enable the interaction between the smart contract and the file storage system. This allows the smart contract to access the GDSII file stored in the file storage system and retrieve it for further processing. Figure 7-5 illustrates the flow of interaction between the smart contract and the file storage system using the blockchain oracle smart contract.

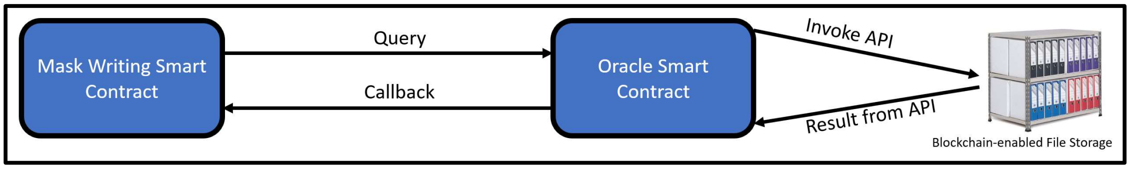


Figure 7-5: Interaction of smart contract with file storage system via blockchain oracle smart contract

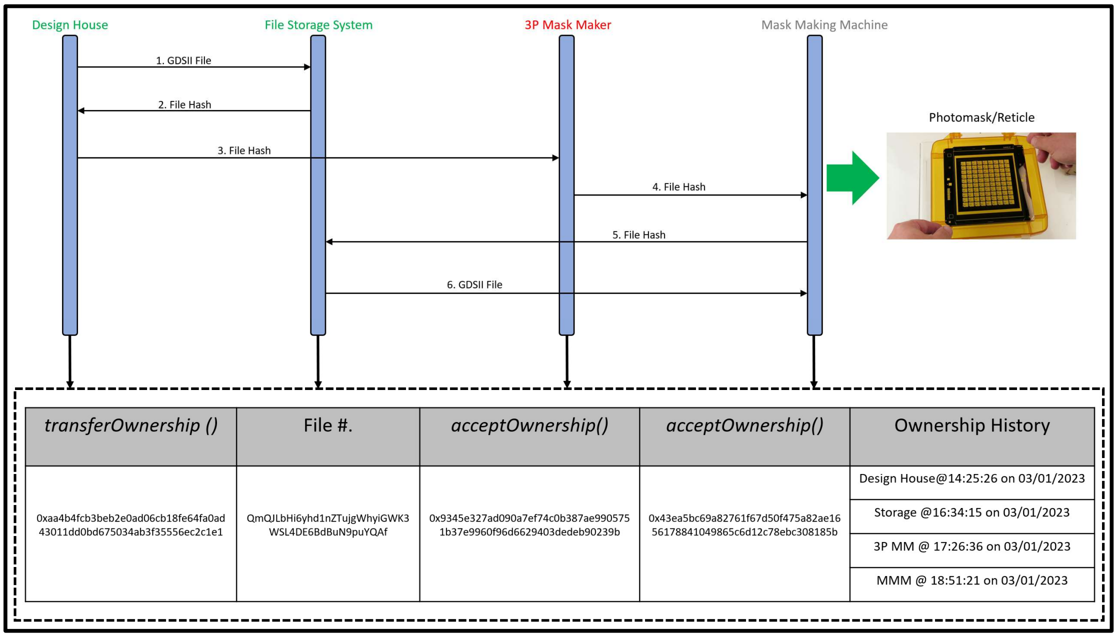
The file storage system validates the requester, which in this case is the mask writing machine, and provides the requested layout file directly to the machine. The file is uploaded onto the mask writing machine without any intervention from the foundry or mask writer. This ensures that the mask writing process can proceed without any risk of introducing a hardware Trojan. Pseudocode 7.2 illustrates the steps involved in fetching the GDSII file from the external API, which is the blockchain-enabled file storage system, using the blockchain oracle smart contract. The file storage system interacts with the smart contract and returns the GDSII file, which is then transferred directly to the mask writing machine. Figure 7-6 visually represents the entire process, showcasing the flow of the GDSII file from the blockchain-enabled file storage system to the mask writing machine, bypassing any potential intervention or tampering by unauthorized entities.

PSEUDOCODE 7.2: Blockchain Oracle

```
pragma solidity ^ 0.5.10;
    import fileHash.sol //infusing the oracle smart contract
    contract maskWriting {


      //modifier to validate designer
     modifier onlyMaskWriter() {
      /** Modifier definition – similar to ALGORITHM 1 **/
     }
        //function to fetch layout
     function fetchFile (ipHash) {
         /** API  string to fetch file – Querying file storage system**/
      }


         //function to return file
     function callBack () {
         /** fetches file from file storage system**/
     }
    }
```

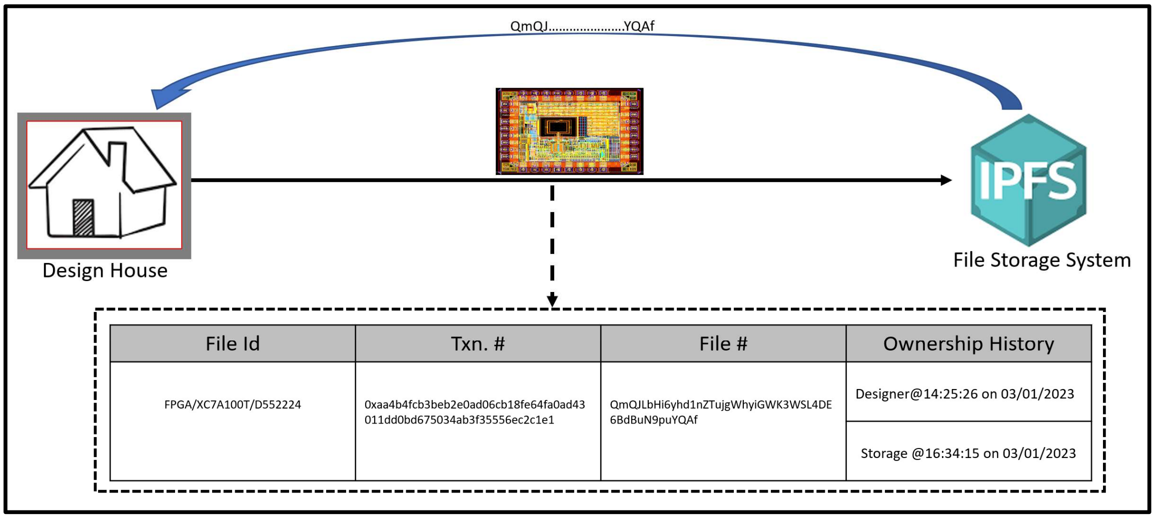


transferOwnership ()	File #.	*acceptOwnership()*	*acceptOwnership()*	Ownership History
0xaa4b4fcb3beb2e0ad06cb18fe64fa0ad43011dd0bd675034ab3f35556ec2c1e1	QmQJLbHi6yhd1nZTujgWhyiGWK3WSL4DE6BdBuN9puYQAf	0x9345e327ad090a7ef74c0b387ae9905751b37e9960f96d6629403dedeb90239b	0x43ea5bc69a82761f67d50f475a82ae1656178841049865c6d12c78ebc308185b	Design House@14:25:26 on 03/01/2023 Storage @16:34:15 on 03/01/2023 3P MM @ 17:26:36 on 03/01/2023 MMM @ 18:51:21 on 03/01/2023

Figure 7-6: Process flow of blockchain-enabled mask writing

7.3.1 Case study: security threat evaluation

The proposed technique and algorithms have been successfully simulated in a locally developed environment. The first step involved developing a file storage system that accepts a GDSII file and returns its hash. The application, running on localhost:3000, provides a user interface with 'upload' and 'download' buttons for file interaction. A GDSII test file was created using the design editing software 'LayoutEditor' and used in the application to generate the file hash. Figure 7-7 visually represents the simulation of this file storage system. Once the file storage system simulation yielded the desired results, the smart contract was simulated. This smart contract enables the mask writing machine to directly fetch the required layout files from the file storage system, without the need for human intervention. The simulations were repeated multiple times to ensure consistent results and better understanding of the system's behavior. In these simulations, all the transactions were performed by the mask writing machine, demonstrating its capability to interact autonomously with the file storage system.



File Id	Txn. #	File #	Ownership History
FPGA/XC7A100T/D552224	0xaa4b4fcb3beb2e0ad06cb18fe64fa0ad43011dd0bd675034ab3f35556ec2c1e1	QmQJLbHi6yhd1nZTujgWhyiGWK3WSL4DE6BdBuN9puYQAf	Designer@14:25:26 on 03/01/2023
			Storage @16:34:15 on 03/01/2023

Figure 7-7: Pictorial representation of simulation of file uploaded to file storage system and hash being returned

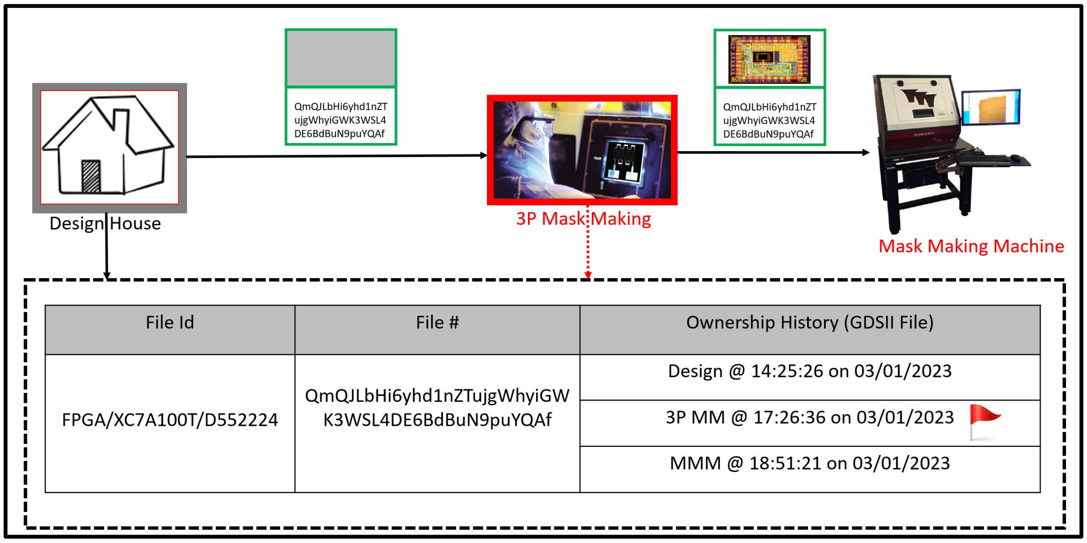
The simulations satisfy the objective of this investigation – security against hardware Trojan intrusion during the mask making process. The following section illustrates an example scenario as shown in Figure 7-8, using the technique and elaborates on it below.

7.3.1.1 Hardware Trojan intrusion

In the traditional mask making process, a third-party (3P) mask maker receives the GDSII file, granting them complete access to the IC design layout. This exposes a potential vulnerability wherein a rogue employee within the mask making team could manipulate the chip's circuitry or introduce a malicious circuit, resulting in a design layout compromised by a Trojan intrusion. When this compromised layout is used to generate a photomask on a chrome substrate, the resulting mask contains the altered or malicious circuitry. Subsequently, during the lithography process, these patterns are transferred onto a wafer, ultimately producing an integrated circuit that has been tampered with and infiltrated by a Trojan.

The incorporation of counterfeit chips into critical infrastructure can have severe repercussions, such as the potential leakage of sensitive data or malfunctions during critical operations. Furthermore, the reputation of the semiconductor company, particularly the design house responsible for the compromised chip, is adversely affected by the discovery of counterfeiting. To mitigate these risks, the semiconductor company can adopt the proposed blockchain-enabled technique and enforce the implementation of the developed smart contract by the foundry or third-party mask makers in their mask making machines. By integrating the postulated smart contract, the access permissions granted to individuals within the mask making team are restricted, thereby safeguarding against any unauthorized modifications or tampering.

To ensure the authenticity and ownership of the GDSII file, the design house registers it on the blockchain by providing relevant details such as the File ID and File Hash obtained from the storage system. Additionally, the smart contract includes functions like transferOwnership() and acceptOwnership(), which allow the user calling these functions to assert their ownership over the asset, in this case, the GDSII file. These ownership details are recorded on the shared ledger of the blockchain, providing a transparent and immutable record of ownership. The integration of the software with the blockchain oracle smart contract enables the automated loading of the layout onto the mask making machine. This automated process bypasses any human intervention, ensuring a secure and trustworthy transfer of the GDSII file. As a result, a clean and Trojan-free mask is generated, as the entire operation is controlled by the smart contract and the automated software, mitigating the risk of any unauthorized alterations or malicious insertions. By leveraging blockchain technology and smart contracts, the design house can establish a robust and auditable process for registering, transferring, and accepting ownership of the GDSII file. This enhances security, eliminates human error or manipulation, and guarantees the production of masks that are free from hardware Trojans, thereby ensuring the integrity of the IC design.



File Id	File #	Ownership History (GDSII File)
FPGA/XC7A100T/D552224	QmQJLbHi6yhd1nZTujgWhyiGWK3WSL4DE6BdBuN9puYQAf	Design @ 14:25:26 on 03/01/2023
		3P MM @ 17:26:36 on 03/01/2023 🚩
		MMM @ 18:51:21 on 03/01/2023

Figure 7-8: Security evaluation of blockchain-enabled mask writing technique

7.4 Summary

This chapter explores additional applications of blockchain, starting with an approach to protect hardware intellectual property (IP). The technique introduces the use of non-fungible tokens (NFTs) as a means to secure IP by converting it into a unique digital asset. NFTs are digital assets that are unique and cannot be replaced. The ownership of NFTs is managed in a decentralized manner by the blockchain, ensuring that IP rights are automatically granted to the creator of the IP/NFT. Once someone becomes the owner of an NFT, they are legally prohibited from modifying or making copies of it unless specific IP rights are granted in the blockchain smart contract. Smart contracts also play a crucial role in monitoring and enforcing IP modification restrictions. By leveraging the features of uniqueness, decentralized ownership rights, and irreplaceability provided by NFTs, the proposed technique aims to safeguard hardware IP from theft and piracy. Throughout the supply chain, the timestamps of transactions stored in the blockchain are carefully examined at each stage. This allows for the identification of any malicious acts and enables the pinpointing of the guilty party. The effectiveness of the technique is illustrated through a detailed case study, demonstrating its validity and practical application.

In addition to protecting hardware IP, this chapter introduces a blockchain-enabled mask making process to prevent Trojan intrusion during the mask writing stage of IC fabrication. To achieve this objective, a blockchain-enabled file storage system is developed to securely transmit the design file from the design house to the mask making machine. Furthermore, a smart contract is created to directly fetch the design file from the file storage system, eliminating the possibility of interference by any untrusted third-party. By implementing this blockchain-enabled approach, the access of potential attackers to the mask writing process is significantly attenuated. This ensures that the circuit imprinted on the mask and subsequently on the silicon wafer remains free from malicious modifications. The outcome is the production of desirable chips that are free from Trojans, enhancing the overall security and integrity of the IC fabrication process.

Chapter 8

Conclusion & Future Work

Assured and trusted microelectronics is a rapidly evolving field that has gained significant attention due to the presence of untrusted participants across the global semiconductor supply chain. This research focuses on analyzing the security threats associated with the FPGA supply chain and proposes novel frameworks to enhance its protection and integrity. By examining the vulnerabilities and risks present in the semiconductor supply chain, this research aims to develop comprehensive solutions that address these challenges. The implementation of these frameworks will contribute to creating a more secure and trustworthy environment for microelectronics production. Through the utilization of advanced technologies such as blockchain, and traditional techniques like physical unclonable functions (PUFs), this research seeks to establish robust security measures that safeguard against threats like IP theft, counterfeiting, hardware Trojan intrusions, and unauthorized modifications. By enhancing the traceability and transparency of the supply chain, these frameworks aim to mitigate risks and ensure the integrity of microelectronics throughout the entire production process. Overall, this dissertation strives to make significant contributions to the field of assured and trusted microelectronics by identifying security threats, proposing innovative solutions, and establishing frameworks that enhance the security and reliability of the semiconductor supply chain.

8.1 Summary

This dissertation presents a blockchain-based approach to enhance security and trust in the supply chain of integrated circuits. A smart contract, developed as part of this research, plays a crucial role by accepting chip parameters as input and comparing them against pre-defined standards. Any inconsistencies or discrepancies in the inputted arguments trigger a warning, highlighting potential issues or deviations from the expected specifications. To further strengthen the security measures, hardware security primitives such as Physical Unclonable Functions (PUFs) are integrated into the blockchain-enabled IC supply chain. Specifically, a Ring Oscillator PUF (ROPUF) is implemented on a Field-Programmable Gate Array (FPGA) to authenticate the FPGA device. This authentication is achieved by comparing the unique Challenge-Response Pairs (CRPs) generated by the ROPUF with the stored CRPs. The blockchain network developed in this research enables the participants of the supply chain to verify the ownership details of the FPGA as it transitions between different entities in the supply chain. Additionally, the blockchain facilitates the tracking of the FPGA's provenance, providing a transparent record of its journey. It should be noted that while this technique has been implemented for the post-fabrication supply chain of FPGAs, it can be readily extended to the Application-Specific Integrated Circuit (ASIC) supply chain as well.

In addition to the security measures discussed earlier, this work introduces a blockchain-enabled file storage and transfer system specifically designed for the secure exchange of intellectual property (IP), represented by the GDSII layout file. A blockchain-based split manufacturing technique, has also been presented, limiting the exposure of the layout file to untrusted foundries. This helps prevent IP theft and piracy, ensuring the integrity and confidentiality of the design. Furthermore, a comprehensive blockchain network has been designed and developed to encompass the entire supply chain, enabling secure asset transfers and maintaining a transparent record of transactions. The blockchain's shared ledger logs all transactions, providing a timestamp for each event. This allows for the precise recording of any malicious activity, aiding in the identification of the responsible party. The performance of the blockchain has been evaluated in terms of two key parameters: transactions per second (TPS) and latency. The simulations are conducted using the Ganache personal blockchain platform, with block times set at 60, 120, and 180 seconds. The blockchain demonstrates a TPS of 0.017, 0.0152, and 0.0158 for the respective block times. Latency, which measures the time taken from transaction submission to confirmation, was recorded for each transaction. The highest latency is observed during the registration of a participant, taking 1.36 seconds, while the lowest latency is observed during the acceptance of the layout file transaction, at 0.43 seconds. The overall average latency for the network was found to be 0.66 seconds.

Moreover, the proposed approach combines the use of blockchain technology and Physical Unclonable Functions (PUFs) to establish a zero trust semiconductor supply chain that adheres to the tenets outlined by the National Institute of Standards and Technology (NIST). By incorporating Ring Oscillator PUFs (ROPUFs) for authentication and blockchain for traceability, the scheme ensures a robust system that meets the principles of zero trust architecture (ZTA) while mitigating the impact of potential attacks on the FPGA supply chain. The presented scheme not only satisfies the requirements of ZTA but also leverages the transparency and immutability of blockchain technology. By making transaction data accessible to all nodes in the network, the integrity of the data is ensured, and it becomes resistant to tampering or unauthorized modifications. This enhances the security and trustworthiness of the supply chain. To evaluate the effectiveness of the proposed approach, each tenet of ZTA is examined through various attack scenarios, and the results are documented. By analyzing the performance of the system under these scenarios, the resilience and effectiveness of the solution are demonstrated.

In addition to the applications of blockchain technology for protecting the FPGA supply chain, this work also explores applications of blockchain technology in other related fields. Two specific applications are highlighted: the use of non-fungible tokens (NFTs) for securing hardware intellectual property (IP) and the implementation of a smart contract for the security of the mask writing process. In the first application, the IP files are transformed into NFTs, ensuring the uniqueness and ownership rights of the IP. This technique maintains the ownership with the original creator throughout the supply chain, preventing unauthorized modifications or copies of the IP. A case study is presented to demonstrate the effectiveness of this technique, showcasing how error messages are generated when a rogue foundry attempts to transfer the layout design file, thus highlighting the security measures in place. In the second application, a smart contract is developed to interact with external APIs, reducing human intervention in the mask making process. By automating the loading of the layout file onto the mask making machine, the risk of introducing trojans or malicious circuitry is mitigated. The smart contract is simulated and evaluated with an attack scenario, assessing its effectiveness in ensuring a

Trojan-free mask and chip production. Through these additional applications, the versatility and potential of blockchain technology in enhancing security and trust in the semiconductor industry are demonstrated. By leveraging NFTs and smart contracts, the integrity of hardware IP and the mask writing process can be safeguarded, contributing to a more secure and reliable supply chain.

Throughout this doctoral dissertation, several case studies have been simulated to validate the effectiveness of the proposed techniques in securing the semiconductor supply chain. These case studies encompass the implementation of blockchain technology, physical unclonable functions (PUFs), zero trust architecture, and non-fungible tokens (NFTs). By employing blockchain technology, the case studies demonstrate the ability to ensure the integrity and traceability of transactions and assets within the supply chain. The decentralized and immutable nature of the blockchain helps prevent IP theft, reverse engineering, and unauthorized modifications. It also enables the detection of Trojan intrusions and insider threats by recording and timestamping all transactions on the shared ledger. The integration of physical unclonable functions (PUFs) adds an extra layer of security to the semiconductor supply chain. PUFs generate unique and unclonable identifiers, such as CRPs (Challenge-Response Pairs), which can be used for authentication and verification purposes. The case studies showcase the successful implementation of PUFs in verifying the authenticity of FPGA devices and ensuring the trustworthiness of the supply chain. The adoption of a zero trust architecture (ZTA) further enhances the security of the semiconductor supply chain. The case studies illustrate how ZTA principles, such as micro-segmentation and continuous authentication, are applied to prevent unauthorized access and minimize the impact of potential attacks. By implementing ZTA, the supply chain becomes more resilient against security threats. Lastly, the use of non-fungible tokens (NFTs) provides a mechanism for securing hardware IP and ensuring ownership rights. The case studies demonstrate how IP files are converted into NFTs, maintaining their uniqueness and ownership throughout the supply chain. This helps protect against IP theft, piracy, and unauthorized modifications. Collectively, these case studies validate the effectiveness of the proposed techniques in safeguarding the semiconductor supply chain from various security threats. By leveraging blockchain, PUFs, ZTA, and NFTs, the integrity, authenticity, and trustworthiness of the supply chain are enhanced, providing greater security and peace of mind for all participants involved.

8.2 Contributions

This dissertation introduces a novel approach to mitigate threats in the FPGA supply chain, addressing both internal and external risks. The approach is based on the principles of zero trust and incorporates blockchain technology and hardware-oriented security mechanisms such as Physical Unclonable Functions (PUFs). The research makes the following key contributions:

- ✓ Development of a blockchain network as a distributed shared ledger to store transactions related to the semiconductor supply chain.
- ✓ Development of a blockchain network specifically designed for the secure transfer of fabricated semiconductors within the supply chain.
- ✓ Design and implementation of a ROPUF for generating CRPs utilized to authenticate the ICs in the supply chain.

- ✓ Development of a blockchain-enabled file storage and transfer system to ensure secure transfer of IP from designer to foundry minimizing the risk of unauthorized access and IP theft.
- ✓ Development of a blockchain-enabled split manufacturing technique to enhance the security and protection of intellectual property (IP) throughout the manufacturing process.
- ✓ Development of a blockchain-enabled, remote chip activation framework to ensure complete control of FPGAs in the hands of the designer, thereby mitigating the risk of unauthorized modifications or intrusions.
- ✓ Design of a supply chain process, enabled with blockchain technology to improve transparency, efficiency, and security throughout the entire supply chain journey.
- ✓ Design and development of a zero trust architecture for strict access control for the users, assets, traffic and application within the supply chain, established by blockchain and ROPUFs.
- ✓ Development of a smart contract to convert IP into NFTs for the security of the IPs from challenges such as IP theft and piracy.
- ✓ Development of a smart contract and blockchain network to secure the mask writing phase of fabrication, minimizing human interference in this process.

8.3 Future Work

The research work presented in this dissertation can be extended by pursuing the following:

- Developing a blockchain-enabled zero trust framework focusing on the pre-fabrication stage.
- Developing a blockchain based EDA tool, providing a secure mask writing solution.
- Developing a blockchain-enabled Computer-aided design (CAD) tool for secure designing of microelectronics chips.
- Developing a blockchain-enabled semiconductor supply chain powered by the concept of Zero knowledge proof (ZKP).
- Building a communication protocol for securing Advanced Metering Infrastructure (AMI) using zero trust architecture realized by blockchain and PUFs.

References

[1] D. Byrne, B. K. Kovak, and R. Michaels, “Offshoring and Price Measurement in the Semiconductor Industry,” presented at Measurement Issues Arising from the Growth of Globalization, Washington, DC, USA, 2009.

[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," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1207-1228, Aug. 2014, DOI: 10.1109/JPROC.2014.2332291.

[3] B. Halak, " CIST: A Threat Modelling Approach for Hardware Supply Chain Security," in Hardware Supply Chain Security, B. Halak (ed.), 2021, Springer, Cham, doi: 10.1007/978-3-030-62707-2_1.

[4] L. Aniello, B. Halak, P. Chai, R. Dhall, M. Mihalea, & A. Wilczynski, “Anti-BlUFf: towards counterfeit mitigation in IC supply chains using blockchain and PUF”, in International Journal of Information Security, vol. 20, pp. 445-460, June. 2021, doi: https://doi.org/10.1007/s10207-020-00513-8

[5] R. S. Chakraborty, S. Narasimhan and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," 2009 IEEE International High Level Design Validation and Test Workshop, 2009, pp. 166-171, doi: 10.1109/HLDVT.2009.5340158.

[6] S. Erickson and J. Solheim, “Brand protection insights from industry leaders in gray market, counterfeit and IP fraud mitigation,” Washington, DC, USA, AGMA Global, White Paper, Dec. 2020. [Online]. Available: https://agmaglobal.org/uploads/whitePapers/Whitepaper_Industry

[7] R. D. DeBobes et al., “The Committee’s Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain.” Accessed: May 5, 2021. [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG112shrg72702/html/CHRG-112shrg72702.htm

[8] S. W. Rose, O. Borchert, S. Mitchell, & S. Connelly, “Zero trust Architecture,” in NIST Special Publication 800-201, Aug. 2020. doi: https://doi.org/10.6028/NIST.SP.800-207. [Online].

[9] A. Kulkarni, N. A. Hazari and M. Niamat, "A Blockchain Technology Approach for the Security and Trust of the IC Supply Chain," 2019 IEEE National Aerospace and Electronics Conference (NAECON), Dayton, OH, USA, 2019, pp. 249-252, doi: 10.1109/NAECON46414.2019.9058027.

[10] A. Dhavlle, R. Hassan, M. Mittapalli and S. M. P. Dinakarrao, "Design of Hardware Trojans and its Impact on CPS Systems: A Comprehensive Survey," 2021 IEEE International Symposium on Circuits and Systems (ISCAS), 2021, pp. 1-5, doi: 10.1109/ISCAS51556.2021.9401254.

[11] M. Elshamy, G. Di Natale, A. Pavlidis, M. -M. Louërat and H. -G. Stratigopoulos, "Hardware Trojan Attacks in Analog/Mixed-Signal ICs via the

Test Access Mechanism," 2020 IEEE European Test Symposium (ETS), 2020, pp. 1-6, doi: 10.1109/ETS48528.2020.9131560

[12] J. P. Deschamps, G. Sutter, E. Canto, “Guide to FPGA Implementation of Arithmetic Functions”, Springer, Cham, doi: 10.1007/978-94-007-2987-2

[13] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, & M. Tehranipoor, “Hardware Trojans: Lessons after One Decade of Research,” in ACM Transaction on Design Automation of Electronic Systems, vol. 22, no. 1, May 2016. doi: 10.1145/2906147

[14] A. Stern, H. Wang, F. Rahman, F. Farahmandi and M. Tehranipoor, "ACED-IT: Assuring Confidential Electronic Design Against Insider Threats in a Zero-Trust Environment," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 41, no. 10, pp. 3202-3215, Oct. 2022, doi: 10.1109/TCAD.2021.3127864.

[15] S. Ray, A. Deb Nath, K. Raj, & S. Bhunia, “The Curious Case of Trusted IC Provisioning in Untrusted Testing Facilities,” in Proceedings of the 2021 on Grate Lakes Symposium on VLSI, June 2021, pp. 207-212, doi: 10.1145/3453688.3461758.

[16] Yon-Chun Chou and L-Hsuan Hong, "A methodology for product mix planning in semiconductor foundry manufacturing," in IEEE Transactions on Semiconductor Manufacturing, vol. 13, no. 3, pp. 278-285, Aug. 2000, doi: 10.1109/66.857936.

[17] S. Khan, A. Mann, & D. Peterson, “The semiconductor supply chain: Assessing national competitiveness,” Center for Security and Emerging Technology, vol. 8, no. 8, 2021.

[18] S. Bose, M. Raikwar, D. Mukhopadhyay, A. Chattopadhyay and K. -Y. Lam, "BLIC: A Blockchain Protocol for Manufacturing and Supply Chain Management of ICS," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1326-1335, doi: 10.1109/Cybermatics_2018.2018.00229.

[19] M. Tehranipoor, U. Guin, & D. Forte, “Counterfieted Integrated Circuits”, in Counterfeieted Integrated Circuits, Springer, Cham, doi: https://doi.org/10.1007/978-3-319-11824-6_2

[20] M. N. Islam, & S. Kundu, “Enabling IC traceability via blockchain pegged to embedded PUF,” in ACM Transactions on Design Automation of Electronics Systems (TODAES), vol. 24, no. 3, pp. 1-23, Apr. 2019, Art. No. 36. doi: 10.1145/3315669.

[21] X. Xu, F. Rahman, B. Shakya, A. Vaassilev, D. Forte, & M. Tehranipoor, “Electronics Supply Chain Integrity Enabled by Blockchain”, vol. 24, no. 3, May. 2019, Art No. 3, doi: 10.1145/3315571

[22] M. Rostami, F. Koushanfar and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1283-1295, Aug. 2014, doi: 10.1109/JPROC.2014.2335155.

[23] N. N. Anandakumar, M. S. Rahman, M. Rahman, R. Kibria, U. Das, F. Farahmandi, F. Rahman, & M. Tehranipoor, “Rethinking Watermarking:Providing Proof of IP Ownership in Modern SoCs,” in Cryptology ePrint Archive, 2022.

[24] T. D. Perez and S. Pagliarini, "A Survey on Split Manufacturing: Attacks, Defenses, and Challenges," in IEEE Access, vol. 8, pp. 184013-184035, 2020, doi: 10.1109/ACCESS.2020.3029339.

[25] M. Yasin, J. Rajendran, Ozgur Sinanoglu, “Trustworthy Hardware Design : Combinational Logic Locking Techniques”, Springer, Cham, doi: 10.1007/978-3-030-15334-2

[26] F. Carrique. “Apple Sues Recycling Partner for Reselling More Than 100,000 iPhones, iPads, and Watches it was Hired to Dismantle.” Oct. 2020. [Online]. Available: https://www.theverge.com/apple/2020/10/4/ 21499422/apple-sues-recycling-company-reselling-ipods-ipads-watches

[27] “4 current, former Samsung employees indicted on semiconductor technology theft charges,” *Yonhap news agency*, Oct. 27, 2022. [Online]. Available: https://en.yna.co.kr/view/AEN20221027007500315?input=rss&section=news

[28] “Execurtive Order on America’s Supply Chain,” Executive Order, The White House, Feb. 24, 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

[29] "Executive Order on Improving the Nation's Cybersecurity," Executive Order, The White House, May 12, 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[30] J. Kindervag, "No More Chewy Centers : Introducing The Zero Trust Model Of Information Security," in Forrester Research Inc., pp. 1–15, Sept. 2010.

[31] M. Samaniego and R. Deters, "Zero-Trust Hierarchical Management in IoT," 2018 IEEE International Congress on Internet of Things (ICIOT), 2018, pp. 88-95, doi: 10.1109/ICIOT.2018.00019.

[32] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," in Forrester Research Inc, pp. 1-26, Nov. 2010.

[33] A. Kerman, O. Borchert, S. Rose, & A. Tan, "Implementing a zero trust architecture," in The MITRE Corporation, Tech. Rep., pp. 1- 20, Mar. 2020.

[34] R. Vanickis, P. Jacob, S. Dehghanzadeh and B. Lee, "Access Control Policy Enforcement for Zero-Trust-Networking," 2018 29th Irish Signals and Systems Conference (ISSC), 2018, pp. 1-6, doi: 10.1109/ISSC.2018.8585365.

[35] S. Nakamoto., "Bitcoin: A Peer-to-Peer Electronic Cash System," Nov. 2008. [Online]. Available: https://assets.pubpub.org/d8wct41f/31611263538139.pdf

[36] A. R. Santhi, & P. Muthuswamy, " Influence of Blockchain Technology in Manufacturing Supply Chain and Logistics," in Logistics, vol. 2, no. 15, Feb. 2022. doi: 10.3390/logistics6010015.

[37] M. Wazid, A. K. Das, S. Shetty and M. Jo, "A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things," in IEEE Access, vol. 8, pp. 88700-88716, 2020, doi: 10.1109/ACCESS.2020.2992467.

[38] M. Iansiti, & K. Lakhani, “The Truth About Blockchain”, Harvard Business Review. Harvard University, pp. 118-127, Feb.2017. Available: https://hbr.org/2017/01/the-truth-about-blockchain

[39] A. Zhang, & X. Lin, “Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain,” in Journal of medical systems, vol. 42, no. 140, June 2018, doi: https://doi.org/10.1007/s10916-018-0995-5

[40] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," in IEEE Transactions on Industrial Informatics, vol. 13, no. 6, pp. 3154-3164, Dec. 2017, doi: 10.1109/TII.2017.2709784.

[41] M. Du, Q. Chen, J. Chen and X. Ma, "An Optimized Consortium Blockchain for Medical Information Sharing," in IEEE Transactions on Engineering Management, vol. 68, no. 6, pp. 1677-1689, Dec. 2021, doi: 10.1109/TEM.2020.2966832

[42] D. Macrinici, C. Cartofeanu, & S. Gao, “Smart contract applications within blockchain technology: A systematic mapping study” in Telematics and Informatics, vol. 35, no. 8, pp. 2337-2354, Dec. 2018. DOI: https://doi.org/10.1016/j.tele.2018.10.004. [Online].

[43] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, “Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab,” in Financial Cryptography and Data Security Lecture Notes in Computer Science, pp. 79– 94, Aug. 2016. doi: https://doi.org/10.1007/978-3-662-53357-4_6

[44] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter,” in Proc. 23rd ACM SIGSAC Conf. Computer Communications Security, Vienna, Austria, Oct. 2016, pp. 254–269. DOI: http://dx.doi.org/10.1145/2976749.2978309.

[45] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," in IEEE Access, vol. 6, pp. 10179-10188, 2018, doi: 10.1109/ACCESS.2018.2799854

[46] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), 2018, pp. 54-63, doi: 10.1109/ICOSST.2018.8632190.

[47] A. Nazir et al., "An Optimized Concurrent Proof of Authority Consensus Protocol," 2023 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Taipa, Macao, 2023, pp. 874-877, doi: 10.1109/SANER56733.2023.00105.

[48] R. Pappu, B. Recht, J. Taylor, & N. Gershenfeld, “Physical One-Way Functions,” in Science, vol. 297, no. 5589, pp. 2026-2030, Sept. 2002, doi: doi/10.1126/science.1074376.

[49] S. Bhunia and M. Tehranipoor, “Hardware Security Primitives,” in *Hardware Security: A Hands-on Learning Approach,* 1st ed. Cambridge, MA, USA: MK, 2019, ch. 12, sec. 12.2, pp. 313-316.

[50] S. Bhunia and M. Tehranipoor, “Hardware Security Primitives,” in *Hardware Security: A Hands-on Learning Approach,* 1st ed. Cambridge, MA, USA: MK, 2019, ch. 12, sec. 12.3, pp. 316-324.

[51] B. Gassend, D. Clarke, M. Van Dijk and S. Devadas, “Silicon physical random functions,” in Proc. Of 9th ACM Conf. Computer and Communications Security, Washington, DC, USA, Nov. 2022, pp. 148-160. doi: 10.1145/586110.586132

[52] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," 2007 44th ACM/IEEE Design Automation Conference, 2007, pp. 9-14. doi: 10.1145/1278480.1278484

[53] Indian Institute of Technology-Madras. (2019). PUF (part 1). [Online]. Available: https://www.youtube.com/watch?v=woEUksF7R9o&t=388s

[54] N. A. Hazari, “Design and Analysis of Assured and Trusted ICs Using Machine Learning and Blockchain Technology,” Doctoral dissertation, The University of Toledo, 2021.

[55] P. Tuyls, , GJ. Schrijen, B. Škorić, J. van Geloven, N. Verhaegh, R. Wolters, “Read-Proof Hardware from Protective Coatings,” In Goubin, L., Matsui, M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006, Lecture Notes in Computer Science, vol 4249. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11894063_29

[56] R. Pappu, “Physical One-Way Functions,” PhD Thesis, Massachusetts Institute of Technology, 2001.

[57] R. Maes, “Physically Unclonable Functions: Properties,” In Physically Unclonable Functions, Springer, Berlin, Heidelberg, pp 49- 80, 2013, doi: https://doi.org/10.1007/978-3-642-41395-7_3.

[58] J. W. Lee, Daihyun 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," 2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525), 2004, pp. 176-179, doi: 10.1109/VLSIC.2004.1346548.

[59] S. S. Kumar, J. Guajardo, R. Maes, G. -J. Schrijen and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, 2008, pp. 67-70, doi: 10.1109/HST.2008.4559053.

[60] R. Yasaei, S. -Y. Yu, E. K. Naeini and M. A. A. Faruque, "GNN4IP: Graph Neural Network for Hardware Intellectual Property Piracy Detection," *2021 58th ACM/IEEE Design Automation Conference (DAC)*, San Francisco, CA, USA, 2021, pp. 217-222, doi: 10.1109/DAC18074.2021.9586150.

[61] Y. Alkabani and F. Koushanfer, “Active Hardware Metering for Intellectual Property Protection and Security,” in *Proc. USENIX Security Symposium*, 2007, pp. 291-306.

[62] A. Chakraborty, A. Mondai and A. Srivastava, "Hardware-Assisted Intellectual Property Protection of Deep Learning Models," *2020 57th ACM/IEEE*

Design Automation Conference (DAC), San Francisco, CA, USA, 2020, pp. 1-6, doi: 10.1109/DAC18072.2020.9218651

[63] S. Patnaik, M. Ashraf, O. Sinanoglu and J. Knechtel, "A Modern Approach to IP Protection and Trojan Prevention: Split Manufacturing for 3D ICs and Obfuscation of Vertical Interconnects," in *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1815-1834, 1 Oct.-Dec. 2021, doi: 10.1109/TETC.2019.2933572.

[64] J. Knechtel, S. Patnaik and O. Sinanoglu, "Protect Your Chip Design Intellectual Property : An Overview," in *International Conference on Omni-Layer Intelligent Systems*, May 2019, pp. 211-216, doi: 10.1145/3312614.3312657

[65] S. M. Hosseini Bamakan, N. Nezhadsistani, O. Bodaghi and Q, Qu, " A Decentralized Framework for Patents and Intellectual Property as NFT in Blockchain Networks," 2021. doi: 10.21203/rs.3.rs-951089/v1

[66] J. Arcenegui, R. Arjona, and I. Baturone, ''Secure management of IoT devices based on blockchain non-fungible tokens and physical unclonable functions,'' in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur*. Cham, Switzerland: Springer, 2020, pp. 24–40.

[67] S. Barakat, K. Yaghi and H. Al-Zagheer, "The Use of NFT for Patent Protection," in *Advances in Dynamical Systems and Applications*, vol. 17, no. 1, pp. 107-113, 2022.

[68] K. Xiao, D. Forte and M. Tehranipoor, "A Novel Built-In Self-Authentication Technique to Prevent Inserting Hardware Trojans," in IEEE

Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 33, no. 12, pp. 1778-1791, Dec. 2014, doi: 10.1109/TCAD.2014.2356453.

[69] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, & S. Bhunia, “MERO: A Stastical Approach for Hardware Trojan Detection,” in Cryptographic Hardware and Embedded Systems-CHES, Lecture Notes in Computer Science, vol. 5747, Springer, Berlin, Heidelberg, 2009, doi: 10.1007/978-3-642-04138-9_28

[70] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, Anaheim, CA, 2008, pp. 51-57, doi: 10.1109/HST.2008.4559049.

[71] P. -S. Ba, S. Dupuis, M. Palanichamy, M. -L. Flottes, G. Di Natale and B. Rouzeyre, "Hardware Trust through Layout Filling: A Hardware Trojan Prevention Technique," 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh, PA, USA, 2016, pp. 254-259, doi: 10.1109/ISVLSI.2016.22.

[72] B. Liu, & G. Qu, “VLSI supply chain security risks and mitigation techniques: A survey,” in Integration, vol. 55, pp. 438-448, Sept. 2016. DOI: 10.1016/j.vlsi.2016.03.002.

[73] T. Zhang, J. Wang, S. Guo and Z. Chen, "A Comprehensive FPGA Reverse Engineering Tool-Chain: From Bitstream to RTL Code," in IEEE Access, vol. 7, pp. 38379-38389, 2019, doi: 10.1109/ACCESS.2019.2901949.

[74] F. Ahmed, M. Shintani and M. Inoue, "Accurate Recycled FPGA Detection Using an Exhaustive-Fingerprinting Technique Assisted by WID

Process Variation Modeling," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 8, pp. 1626-1639, Aug. 2021, doi: 10.1109/TCAD.2020.3023684.

[75] A. Dorri, S. S. Kanhere, & R. Jurdak, “Blockchain in internet of things: challenges and solutions,” arXiv preprint arXiv:1608.05187, May, 2016, doi: 10.48550/arXiv.1608.05187.

[76] W. Viriyasitavat, T. Anuphaptrirong, & D. Hoonsopon, “When blockain meets Internet of Things: Characteristics, challenges, and business opportunities,” in Journal of industrial information integration, vol. 15, pp. 21-28, Sept. 2019, doi: 10.1016/j.jii.2019.05.002.

[77] Z. A. Collier, & J. Sarkis, “The zero trust supply chain: Managing supply chain risk in the absence of trust,” International Journal of Production Research, vol. 59, no. 11, pp. 3430-3445, Feb. 2021. doi: https://doi.org/10.1080/00207543.2021.1884311, [Online].

[78] M. Sultana, A. Hossain, F. Laila, K. A. Taher, & M. N. Islam, “Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology,” in BMC Medical Informatics and Decision Making, vol. 20, no. 1, pp. 1-10, Oct. 2020, DOI: https://doi.org/10.1186/s12911-020-01275-y. [Online].

[79] S. Dhar, & I. Bose, “Securing IoT Devices Using Zero Trust and Blockchain,” in Journal of Organizational Computing and Electronic Commerce, vol. 31, no. 1, pp. 18-34, Nov. 2021. DOI: https://doi.org/10.1080/10919392.2020.1831870. [Online].

[80] L. Alevizos, , V. T. Ta, & M. H. Eiza, “Augmenting Zero Trust Architecture to Endpoints Using Blockchain: A Systematic Review,” in arXiv preprint arXiv:2104.00460. Nov. 2021. DOI: 10.1002/spy2.191.

[81] S. Hamdioui, J. -L. Danger, G. Di Natale, F. Smailbegovic, G. van Battum and M. Tehranipoor, "Hacking and protecting IC hardware," 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 2014, pp. 1-7, doi: 10.7873/DATE.2014.112.

[82] X. Wang, M. Tehranipoor, & J. Plusquellic, “Detecting malicious inclusions in secure hardware: Challenges and solutions,” 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, Anaheim, CA, USA, 2008, pp. 15-19, doi: 10.11009/HST.2008.4559039.

[83] S. Brown, R. Francis, J. Rose and Z. Vranesic, *Field-Programmable Gate Arrays*, 1st ed. Boston, MA: Kluwer Academic Publisher, 1992.

[84] R. Ghayoula, J. Fattahi, A. Smida, I. El Gmati, E. Pricop and M. Ziadia, "FPGA Implementation of SIMON-128 Cryptographic Algorithm Using Artix-7," 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2022, pp. 1-5, doi: 10.1109/ECAI54874.2022.9847520

[85] T. Zhang, F. Rahman, M. Tehranipoor and F. Farahmandi, "FPGA-Chain: Enabling Holistic Protection of FPGA Supply Chain with Blockchain Technology," in IEEE Design & Test, 2022, doi: 10.1109/MDAT.2022.3213998.

[86] M. Xue, C. Gu, W. Liu and M. O’Neill, “Ten years of hardware Trojans : a survey from attacker’s perspective,” in IET Computers & Digital Techniques, vol. 16, no. 6, pp. 231-246, Nov. 2020, doi: 10.1049/iet-cdt.2020.0041

[87] R. S. Chakraborty, I. Saha, A. Palchaudhuri and G. K. Naik, "Hardware Trojan Insertion by Direct Modification of FPGA Configuration Bitstream," in IEEE Design & Test, vol. 30, no. 2, pp. 45-54, April 2013, doi: 10.1109/MDT.2013.2247460.

[88] M. Moraitis and E. Dubrova, “FPGA Bitstream Modification with Interconnect in Mind,” In Hardware and Architectural Support for Security and Privacy (HASP '20) Association for Computing Machinery, New York, NY, USA, Article 5, pp. 1–9. 2021, https://doi.org/10.1145/3458903.3458908.

[89] T. Bonny and Q. Nasir, “Clock glitch fault injection attack on an FPGA-based non-autonomous chaotic oscillator,” in Springer Nonlinera Dyn, vol. 96, pp. 2087-8101, Apr. 2019, doi: 10.1007/s11071-019-04907-9.

[90] N. Asadizanjani, M. T. Rahman and M. Tehranipoor, “Counterfeit Detection and Avoidance with Physical Inspection,” in Physical Assurance, Springer Cham, 2020, ch. 2, pp. 21-44, doi: 10.1007/978-3-030-62609-9_2.

[91] J. Zhang and G. Qu, “Recent Attacks and Defenses on FPGA-based systems,” in ACM Trans. Reconfigurable Technology System, vol. 12, no. 3, Art. 14, Aug. 2019, doi: 10.1145/3340557.

[92] C. Herder, M. -D. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1126-1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516

[93] M. Mustapa, M. Niamat, M. Alam and T. Killian, "Frequency uniqueness in ring oscillator Physical Unclonable Functions on FPGAs," 2013 IEEE 56th

International Midwest Symposium on Circuits and Systems (MWSCAS), Columbus, OH, USA, 2013, pp. 465-468, doi: 10.1109/MWSCAS.2013.6674686.

[94] N. A. Hazari, A. Oun and M. Niamat, "Analysis and Machine Learning Vulnerability Assessment of XOR-Inverter based Ring Oscillator PUF Design," 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS), 2019, pp. 590-593, doi: 10.1109/MWSCAS.2019.8885037

[95] A. S. Shanta, M. B. Majumder, M. S. Hasan and G. S. Rose, "Physically Unclonable and Reconfigurable Computing System (PURCS) for Hardware Security Applications," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 3, pp. 405-418, March 2021, doi: 10.1109/TCAD.2020.2999907

[96] M. Mustapa and M. Niamat, “Relationship between number of stages in ROPUF and CRP generation on FPGA,” in Proc. Int. Conf. Security Manag. (SAM) Steering Committee World Congr. Comput. Sci. Comput. Eng. Appl. Comput. (WorldComp), Las Vegas, NV, USA, 2014, pp. 120–126

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

[98] N. Vashistha, M. M. Hossain, M. R. Shahriar, F. Farahmandi, F. Rahman and M. M. Tehranipoor, "eChain: A Blockchain-Enabled Ecosystem for Electronic Device Authenticity Verification," in IEEE Transactions on Consumer Electronics, vol. 68, no. 1, pp. 23-37, Feb. 2022, doi: 10.1109/TCE.2021.3139090.

[99] D. Yaga, P. Mell, N. Roby and K. Scarfone, “Blockchain Technology Overview,” in NIST 8202, Oct. 2018, pp. 1-68. doi: 10.6028/NIST.IR.8202.

[100] S. Trimberger, "Trusted Design in FPGAs," 2007 44th ACM/IEEE Design Automation Conference, 2007, pp. 5-8.

[101] “Risks in the Semiconductor Manufacturing and Advanced Packaging Supply Chain,” The Mitre Corporation. https://downloads.regulations.gov/BIS-2021-0011-0032/attachment_1.pdf (accessed Nov. 5, 2022).

[102] R. Kumar, & R. Tripathi, “Blockchain-based framework for data storage in peer-to-peer scheme using interplanetary file system,” in Handbook of Research on Blockchain Technology, S. Krishnan, V. Balas, E. G. Julie, Y. H. Robinson, S. Balaji, & R. Kumar Eds. San Dieago, CA, USA: Academic Press, 2020, ch. 2, pp. 35-57. doi: 10.1016/B978-0-12-819816-2.00002-2

[103] N. A. Hazari, A. Oun and M. Niamat, "Analysis and Machine Learning Vulnerability Assessment of XOR-Inverter based Ring Oscillator PUF Design," 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS), 2019, pp. 590-593, doi: 10.1109/MWSCAS.2019.8885037.

[104] Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., & Shafiq, M. (2019). A secure data sharing platform using blockchain and interplanetary file system. Sustainability, 11(24), 7054. spectrum, 43(5), 37-46.

[105] Jarvis, R., McIntyre, M. (2004). Split Manufacturing Method for Advanced Semiconductor Circuits (U.S. Patent No. US20040102019A1). U.S. Patent and Trademark Office.

https://patentimages.storage.googleapis.com/9b/17/74/f41cfe50a2eb2c/US20040102019A1.pdf

[106] B. Hill, R. Karmazin, C. T. O. Otero, J. Tse and R. Manohar, "A split-foundry asynchronous FPGA," Proceedings of the IEEE 2013 Custom Integrated Circuits Conference, San Jose, CA, USA, 2013, pp. 1-4, doi: 10.1109/CICC.2013.6658536.

[107] J. Rajendran, O. Sinanoglu and R. Karri, "Is split manufacturing secure?," 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 2013, pp. 1259-1264, doi: 10.7873/DATE.2013.261.

[108] F. Imeson, A. Emtenam, S. Garg and M. V. Tripunitara, "Securing Computer Hardware Using 3D Integrated Circuit (IC) technology and Split Manufacturing for Obfuscation", in USENIX Security Symposium, Washingtion, D.C. 2013, pp. 495-510, ISBN: 978-1-931971-03-4.

[109] Truffle Suite, "What is Ganache," trufflesuite.com. [Online]. Available: https://trufflesuite.com/docs/ganache/. (accessed June 5th, 2023).

[110] X. Zheng, Y. Zhu and X. Si, "A Survey on Challenges and Progress in Blockchain Technologies: A Performance and Security Perspective," in *Applied Sciences,* vol. 9, no. 22. Pp. 4731-4755, Nov. 2019, doi: 10.3390/app9224731.

[111] S. Bilonikar, C. Mendonca, D. Phadakale and M. Shetty, "Blockchain Based Model for Royalty Payments of Artists and Remix-Makers," in *International Conference on Smart Data Intelligence (ICSMDI 2021)*, Trichy, India, 2021, doi: 10.2139/ssrn.3852878.

[112] R. Yasaweerasinghelage, M. Staples and I. Weber, "Predicting Latency of Blockchain-Based Systems Using Architectural Modelling and Simulation," 2017 *IEEE International Conference on Software Architecture (ICSA)*, Gothenburg, Sweden, 2017, pp. 253-256, doi: 10.1109/ICSA.2017.22.

[113] S. M. Trimberger, *Field-Programmable Gate Array Technology*, 1st ed. Boston, MA, USA: Kluwer Academic Publishers, 1994.

[114] S. M. Trimberger and J. J. Moore, "FPGA Security: Motivations, Features, and Applications," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1248-1265, Aug. 2014, doi: 10.1109/JPROC.2014.2331672.

[115] A. Duncan, F. Rahman, A. Lukefahr, F. Farahmandi and M. Tehranipoor, "FPGA Bitstream Security: A Day in the Life," 2019 IEEE International Test Conference (ITC), Washington, DC, USA, 2019, pp. 1-10, doi: 10.1109/ITC44170.2019.9000145.

[116] M. Ender, A. Moradi, C. Paar, “The Unpatchable Silicon : A Full Break of the Bitstream Encryption of Xilinx 7-Series FPGAs,” In 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 1803-1819.

[117] S. Mal-Sarkar, A. Krishna, A. Ghosh, & S. Bhunia, “Hardware Trojan attacks in FPGA devices: threat analysis and effective countermeasures,” in Proceedings of the 24th edition of the great lakes symposium on VLSI, pp. 287-292, May 2014. doi: 10.1145/2591513.2591520

[118] D. R. Collins, “Trust in Integrated Circuits,” Defense Advanced Research Projects Agency, Arlington VA, 2008.

[119] H. Dogan, D. Forte and M. M. Tehranipoor, "Aging analysis for recycled FPGA detection," 2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Amsterdam, Netherlands, 2014, pp. 171-176, doi: 10.1109/DFT.2014.6962099.

[120] Z. Zheng, S. Xie, H. N. Dai, W. Chen, X. Chen, J. Weng, & M. Imran, “An overview on smart contracts: Challenges, advances and Platforms,” in Future Generation Computer Systems, vol. 105, pp. 475-491, Apr. 2020. DOI: 10.1016/j.future.2019.12.019.

[121] J. Sun, X. Yao, S. Wang and Y. Wu, "Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS," in IEEE Access, vol. 8, pp. 59389-59401, 2020, doi: 10.1109/ACCESS.2020.2982964.

[122] F. Aloul, S. Zahidi and W. El-Hajj, "Two factor authentication using mobile phones," 2009 IEEE/ACS International Conference on Computer Systems and Applications, 2009, pp. 641-644, doi: 10.1109/AICCSA.2009.5069395.

[123] A. Oun, N. A. Hazari and M. Y. Niamat, "Analysis of Swarm Intelligence Based ANN Algorithms for Attacking PUFs," in IEEE Access, vol. 9, pp. 121743-121758, 2021, doi: 10.1109/ACCESS.2021.3109235.

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

[125] F. Hofmann, S. Wurster, E. Ron and M. Böhmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization," 2017

ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), 2017, pp. 1-8, doi: 10.23919/ITU-WT.2017.8247004.

[126] M. Keating and P. Bricaud, *Reuse methodology manual for system-on-a-chip designs*, 3rd ed. New York, Kluwer Academic Publisher, 2002.

[127] W. Savage, J. Chilton and R. Camposano, "IP reuse in the system on a chip era," *Proceedings 13th International Symposium on System Synthesis*, Madrid, Spain, 2000, pp. 2-7, doi: 10.1109/ISSS.2000.874022

[128] R. S. Chakraborty and S. Bhunia, "Hardware protection and authentication through netlist level obfuscation," *2008 IEEE/ACM International Conference on Computer-Aided Design*, San Jose, CA, USA, 2008, pp. 674-677, doi: 10.1109/ICCAD.2008.4681649.

[129] A. B. Kahng *et al*., "Constraint-based watermarking techniques for design IP protection," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 20, no. 10, pp. 1236-1252, Oct. 2001, doi: 10.1109/43.952740.

[130] R. S. Chakraborty and S. Bhunia, "HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 28, no. 10, pp. 1493-1502, Oct. 2009, doi: 10.1109/TCAD.2009.2028166.

[131] M. Rostami, F. Koushanfar, J. Rajendran and R. Karri, "Hardware security: Threat models and metrics," *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, San Jose, CA, USA, 2013, pp. 819-823, doi: 10.1109/ICCAD.2013.6691207.

[132] D. C. Musker, “Protecting and exploiting intellectual property in electronics,” in *Proc. IBC Conf.*, 1998. [Online]. Available: http://www. jenkins.eu/articles/reverse-engineering.asp

[133] S. Bhasin, J. -L. Danger, S. Guilley, X. T. Ngo and L. Sauvage, "Hardware Trojan Horses in Cryptographic IP Cores," *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Los Alamitos, CA, USA, 2013, pp. 15-29, doi: 10.1109/FDTC.2013.15.

[134] R. J. May and S. L. Cooper, “Copyrights and patents, piracy and theft,” *The Washington Times,* April 24, 2018. [Online]. Available: https://www.washingtontimes.com/news/2018/apr/24/copyrights-and-patents-piracy-and-theft/

[135] “Special 301 report,” the United States Trade Representative, 2017. [Online]. Available: https://ustr.gov/issue-areas/intellectual-property/special-301#:~:text=The%20Report%20identifies%20a%20wide,in%20trade%20secret%20protection%20in

[136] J. Fairfield, “Tokenized: The law of non-fingible tokens and unique digital property,” in *Indiana Law Journal Forthcoming*, 2022.

[137] S. Pope, "Trusted Integrated Circuit Strategy," in IEEE Transactions on Components and Packaging Technologies, vol. 31, no. 1, pp. 230-234, March 2008, doi: 10.1109/TCAPT.2008.918319.

[138] M. Tehranipoor et al., "Trustworthy Hardware: Trojan Detection and Design-for-Trust Challenges," in Computer, vol. 44, no. 7, pp. 66-74, July 2011, doi: 10.1109/MC.2010.369.

[139] U. J. Botero, R. Wilson, H. Lu, M. T. Rahman, M. A. Mallaiyan, F. Ganji, N. Asadizanjani, M. Tehranipoor, D. L. Woodard, & D. Forte, " Hardware Trust and Assurance through Reverse Engineering: A Tutorial and Outlook from Image Analysis and Machine Learning Perspective," in Journal of Emerging Technology in Computer Systems, vol. 17, no. 4, June 2021, doi: 10.1145/3464959

[140] A. Sengupta, "Hardware Security of CE Devices [Hardware Matters]," in IEEE Consumer Electronics Magazine, vol. 6, no. 1, pp. 130-133, Jan. 2017, doi: 10.1109/MCE.2016.2614552.

[141] U. Guin, Z. Zhou and A. Singh, "Robust Design-for-Security Architecture for Enabling Trust in IC Manufacturing and Test," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 26, no. 5, pp. 818-830, May 2018, doi: 10.1109/TVLSI.2018.2797019.

[142] F. Olivieri, "A Secondary Source Analysis of the Business Models and Supply Chain Strategies of Semiconductor Manufacturers," Masters Thesis, School of Industrial and Information Engineering, Politecnico di Milano, Milan, Italy.

[143] S. Rizvi, *Handbook of Photomask Manufacturing Technology*, 1st ed. Boca Raton, FL: CRC Press, Taylor & Francis Group, 2005. Accessed: Mar. 2023. [Online]. Available: http://diyhpl.us/~bryan/papers2/optics/photolithography/Rizvi2005HandbookofPhotomaskManufacturingTechnology.pdf

[144] C. Saint & J. Saint, *IC Mask Design : Essential Layout Techniques*, 1st ed. McGraw Hill, USA, 2002. Accessed Mar. 2023 [Online]. Available:

https://www.accessengineeringlibrary.com/binary/mheaeworks/095c1ea2cd188cb6/a4a333b70e0e1c53e21286817266e06bf88b30986e419206dba89cbd02fcab50/book-summary.pdf?implicit-login=true

[145] C. . K. Frantz and M. Nowostawski, "From Institutions to Code: Towards Automated Generation of Smart Contracts," *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*, Augsburg, Germany, 2016, pp. 210-215, doi: 10.1109/FAS-W.2016.53.

[146] M. Taghavi, J. Bentahar, H. Otrok, & K. Bakhtiyari, “A reinforcement learning model for the reliability of blockchain oracles,” in Expert Systems with Applications, vol. 214, Oct. 2022, doi: 10.1016/j.eswa.2022.119160

[147] A. Pasdar, Y. C. Lee, & Z. Dong, “Connect API with Blockchain: A Survey on Blockchain Oracle Iplementation,” in ACM Computing Surveys, vol. 55, no. 10, pp. 1-39, Feb. 2023, Art. 208, doi: 10.1145/3567582