Poster: Consortium Blockchain for the Assurance of Supply Chain Security

Haoting Shen, Shahriar Badsha, and Dongfang Zhao
Computer Science and Engineering Department, University of Nevada, Reno
hshen@unr.edu, sbadsha@unr.edu, and dzhao@unr.edu

***Abstract*—Today, the electronics supply chain involves participants from different regions around the world, making the assurance of the supply chain integrity and security challenging. To prevent potential threats, a trustworthy supply chain system shall provide reliable traceability, immutability, transparency, privacy, and flexible scalability. In this research, we propose a consortium blackchain technique for the trust of electronics supply chain, which is based on traceability ensured by irreproducible ID, transparency and privacy allowed by attribute-based access control, and scalability enabled by diskless implementation.**

I. Introduction

During the last few decades, the supply chain of electronic systems becomes remarkably complex and extensive due to the rise of globalization. Although the resource allocations are significantly optimized and the manufacturing costs are dramatically reduced along the progressing, the security and integrity of the supply chain are exposed to threats arising from untrusted parties that possibly involve in the design, fabrication, and distribution of electronic systems. For example, it is estimated that counterfeiting costs U.S. semiconductor manufacturers billions dollars a year[1]. The counterfeited devices result in lost revenue to the industry, compromise the reputation of manufacturers and sellers. In worse cases, when they are deployed in critical infrastructures (e.g. public transportation systems, medical systems, etc.), the counterfeit parts pose unexpectable potential risks to individuals and society because of the lower reliability.

To build a trusted and practical electronics supply chain to cover most electronic products in modern commercial environment, there are several essential considerations, including traceability, immutability, transparency, privacy, and scalability. **Traceability:** An unique ID is the prerequisite for traceability. To prevent possible counterfeits such as reproduction and/or overproduction, it should be difficult enough to reproduce the electronics with the same ID. **Immutability:** Along the whole supply chain, all confirmed transactions involving the electronics ownership transferring should be recorded and immutable. **Transparency:** The origins of the electronics and the related transactions should be available to parties with proper accesses, such as the owners and certain authorities. **Privacy:** Unrelated parties should not be granted the access, as the sales information can be commercial sensitive and the ownership information relates individuals' or groups' privacy. **Scalability:** Given the market size and number transactions for electronics, flexible scalability is necessary.

To provide a complete solution, researchers are starting to set their sights on blockchain technology as it provides a platform that potentially meets all the demands listed above. For example, in [2], consortium-based blockchain frameworks were introduced. In [3], using physical unclonable function (PUF) as unique device ID for blockchain was discussed. In [4], technical details about critical operations in blockchain application, including registration, transaction confirmation, and verification, were described. However, a comprehensive solution covering all the requirements is still in a lack. Different from the blockchain technology for completely data-based items (i.e. virtual products/currencies), the blockchain for trusted electronics supply chain involve physical items. Researches on unclonable ID, the privacy, and the scalability are particularly inadequate.

In this research, we are proposing a new blockchain-based framework for the establishment of trusted electronics supply chain. Our contributions will focus on:

- The design of reliable, low power consumption, and cost-efficient PUF serving as the ID of electronics including the ones for internet of things (IoT) and cyber-physical systems (CPS) applications.
- The development of attribute-based access control mechanism that considers the security, privacy, resource budget for the parties participating in.
- Possible solutions to handle the scalability of the proposed blockchain framework.

II. Proposed blockchain-based framework

According to the supply chain application scenarios, consortium blockchain architecture is employed here to ensure trusted electronics supply chains. As discussed in [2], [3], [4], the consortium blockchain enables transactions with limited resources, partially decentralized ledgers, and optimized efficiency. The architecture is shown in Fig. 1. Generally, there are three types of entities in our blockchain system: producers, users, and consortium nodes.

Producers are the entities allowed to bring new electronic products into the blockchain, such as manufacturers and as-

Network and Distributed Systems Security (NDSS) Symposium 2020
23-26 February 2020, San Diego, CA, USA
ISBN 1-891562-61-4
https://dx.doi.org/10.14722/ndss.2020.23xxx
www.ndss-symposium.org

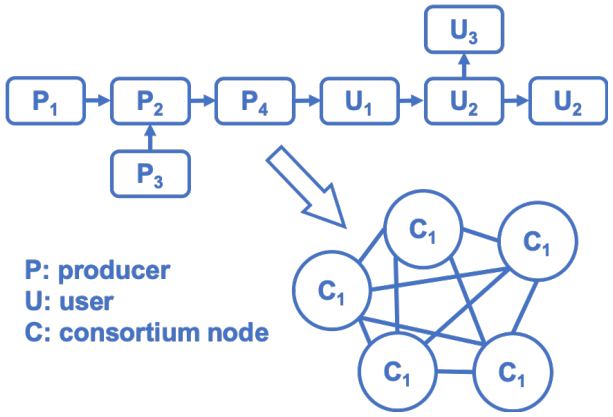


Fig. 1. Proposed consortium-based blockchain.

semblers. Each new products brought in shall come with an irreproducible ID (e.g. PUF). For assembled electronic systems, new ID should be generated according to the subcomponents' IDs. **Users** include the retailers, distributors, and customers. They submit product verification request to the consortium, confirm the receipt of products, release the products to the next user, and terminate the life-cycle of the products. Producers have all these accesses as well. **Consortium nodes** are the distributed critical entities that possess more resources and satisfy high level security standards, such as related government agencies, good reputation enterprises, and authoritative associations. The nodes are responsible for recording and syncing the blockchain data, handling the verification requests, and voting on the verification results.

III. Proposed approaches

Deriving from the blockchain technology developed for virtual items, many techniques can be readily utilized for the proposed technique. However, there are a few vital challenges exclusively for the electronics supply chain applications.

A. Irreproducible ID

To make physical electronics IDs irreproducible, PUF might be the most available solution at this moment. However, efficient modeling attacks are able to successfully build accurate physical model of PUFs, making the reproducing of a PUF possible [5]. Meanwhile, PUF is typically realized in integrated circuit (IC) chips, the PUF solution is thus only available for active electronics (e.g. IC chips) but not for passive electronic components (e.g. capacitors, resistors, etc.). For this, we developed unclonable chipless RFID in addition to IC-based PUF, carrying a unique analog ID that can be extracted by reading the RF resonance signal [6].

B. Access control

Unlike the cryptocurrency, anonymous account in blockchain may not be suitable to applied directly in supply chain management. Considering the different responsibilities for different entities, as well as the protection of sensitive business data and individual privacy, entity-ID-based access control strategy will be exploited here. Blockchain with smart contract, allowing monitoring and enforcing access permissions under complex conditions, makes it a trustable alternative infrastructure for access control systems. Here, we plan to use XACML, an XML-based standard defining various components [1], to manage and perform attribute-based access control for the blockchain. We will use the charge-response-pairs (CRP) obtained from PUFs that are embeded in the products as the key to manage the access rights instead of having traditional public key based cryptography as there is no key generator entity and CRP can be produced by the device it self. For practical implementation, we will test it in XACML in Ethereum smart contracts.

C. Scalability

Scalability is one of the most challenging technical barriers for widely adopting blockchains for applications such as supply chains, mainly because the number of messages for peer-to-peer communication is in the quadratic order of the participants. Recent studies [7], [8], however, showed that it is possible to built practically efficient communication channels for blockchains. Our research shows that a diskless implementation [9] (i.e., memory-only) of blockchains can also be an important building block for the proposed infrastructure of large-scale supply chains. Now We are working on a blockchain prototype optimized for the supply chain workloads by leveraging the latest wisdom from various communities such as databases and high-performance computing.

References

[1] S. A. S. Committee *et al.*, "Inquiry into counterfeit electronic parts in the department of defense supply chain," *Washington, DC*, 2012.
[2] X. Xu, F. Rahman, B. Shakya, A. Vassilev, D. Forte, and M. Tehranipoor, "Electronics supply chain integrity enabled by blockchain," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 24, no. 3, pp. 1–25, 2019.
[3] M. N. Islam and S. Kundu, "Enabling ic traceability via blockchain pegged to embedded puf," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 24, no. 3, pp. 1–23, 2019.
[4] P. Cui, J. Dixon, U. Guin, and D. Dimase, "A blockchain-based framework for supply chain provenance," *IEEE Access*, vol. 7, pp. 157 113–157 125, 2019.
[5] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 237–249.
[6] K. Yang, U. Botero, H. Shen, D. L. Woodard, D. Forte, and M. M. Tehranipoor, "Ucr: An unclonable environmentally sensitive chipless rfid tag for protecting supply chain," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 23, no. 6, pp. 1–24, 2018.
[7] J. Hellings *et al.*, "Resilientdb: Global scale resilient blockchain fabric," in *International Conference on Very Large Data Bases (VLDB)*, 2020.
[8] S. Rahnama *et al.*, "Coordination-free byzantine replication with minimal communication costs," in *International Conference on Database Theory (ICDT)*, 2020.
[9] A. Al-Mamun *et al.*, "In-memory blockchain: Toward efficient and trustworthy data provenance for hpc systems," in *International Conference on Big Data (BigData)*, 2018.

[1] http://docs.oasis-open.org/xacml/

Consortium Blockchain for the Assurance of Supply Chain Security

University of Nevada, Reno

Haoting Shen, Shahriah Badsha, and Dongfang Zhao
University of Nevada, Reno {hshen, sbadha, dzhao}@unr.edu

INTRODUCTION

During the last few decades, although the resource allocations are significantly optimized and the manufacturing costs are dramatically reduced with the globalization, the security and integrity of the supply chain are exposed to threats arising from untrusted parties that possibly involve in the design, fabrication, and distribution of electronic systems. For example, the U.S. Department of Commerce estimates that more than 8% of total electronic merchandise trade is counterfeit.

REQUIREMENTS AND CHALLENGES

Traceability. A unique ID is the prerequisite for traceability. To prevent possible counterfeits such as reproduction and/or overproduction, it should be difficult enough to reproduce the electronics with the same ID.

Immutability. Along the whole supply chain, all confirmed transactions involving the electronics ownership transferring should be recorded and immutable.

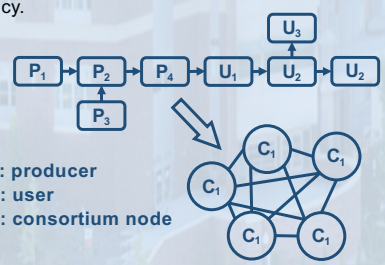
Transparency. The origins of the electronics and the related transactions should be available to parties such as the owners and certain authorities.

Privacy. Sales information can be commercial sensitive and the ownership information relates individuals' or groups' privacy.

Scalability. Given the market size and number transactions for electronics, flexible scalability is necessary.

CONSORTIUM-BASED BLOCKCHAIN

The consortium blockchain enables transactions with limited resources, partially decentralized ledgers, and optimized efficiency.



Producers
- Manufacturers
- Assemblers

Users' rights +
Reg. new items
Provide irreprod. ID

Users
- Distributors
- Customers

Request Verification
Confirm receipt
Release ownership

Consortium nodes

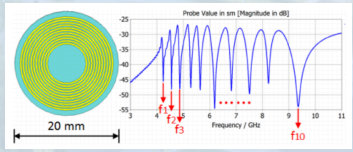
Distributed critical entities that possess more resources and meet high level security standards.
- Government agencies
- Good reputation enterprises
- Authoritative associations, etc.

Transaction recording | Verification
Data syncing | Consensus

PROPOSED TECHNIQUE I IRREPRODUCIBLE ID FOR TRACEABILITY

Active physical unclonable function is based on IC chips. To cover various types of electronics including lightweight items with limited resources, we will need low power consumption design.

Passive unclonable IDs (e.g. RFID) is chipless. The ID is analog signal and more robust against modeling attack compared to PUF.



PROPOSED TECHNIQUES II: ACCESS CONTROL FOR TRANS. AND PRIVACY

Unlike the cryptocurrency, anonymous account in blockchain may not be suitable to applied directly in supply chain management.

Considering the different responsibilities for different entities, as well as the protection of sensitive business data and individual privacy, entity-ID-based access control strategy will be exploited here.

Here, we plan to use XACML, an XML-based standard defining various components, to manage and perform attribute-based access control for the blockchain.

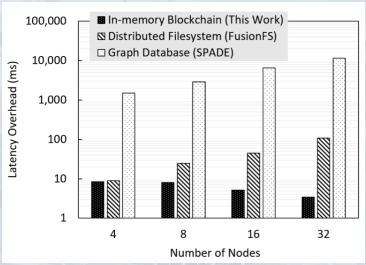
We will use the PUFs that are embedded in the products as the key to manage the access rights instead of having traditional public key-based cryptography as there is no key generator entity.

For practical implementation, we will test it in XACML in Ethereum smart contracts.

PROPOSED TECHNIQUES III: SCALABILITY

Scalability is challenging, but our research shows that a diskless implementation of blockchains can also be an important building block for the proposed infrastructure of large-scale supply chains.

Now We are working on a blockchain prototype optimized for the supply chain workloads by leveraging the latest wisdom from various communities such as databases and high-performance computing.



Latency Overhead of In-memory Blockchain, Distributed File system, and Graph Database.