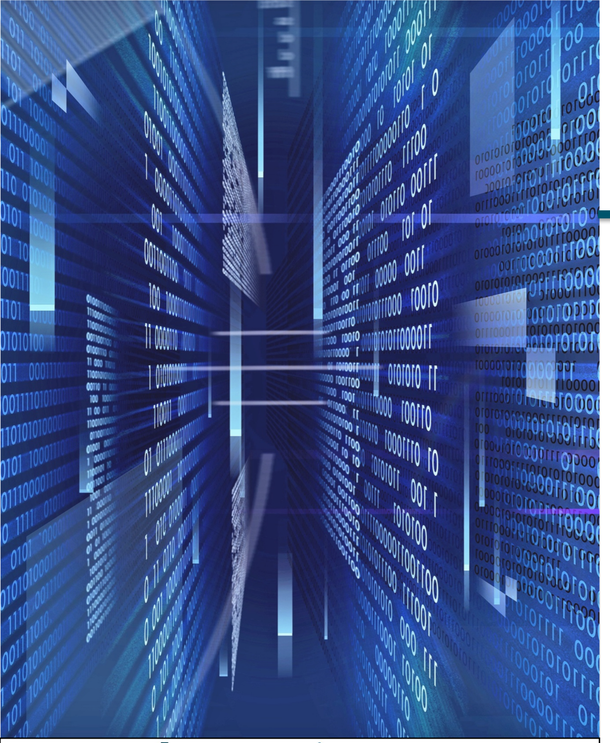


cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

CyberSecuritySoton.org [w]

@CybSecSoton [fb & tw]

UNIVERSITY OF Southampton

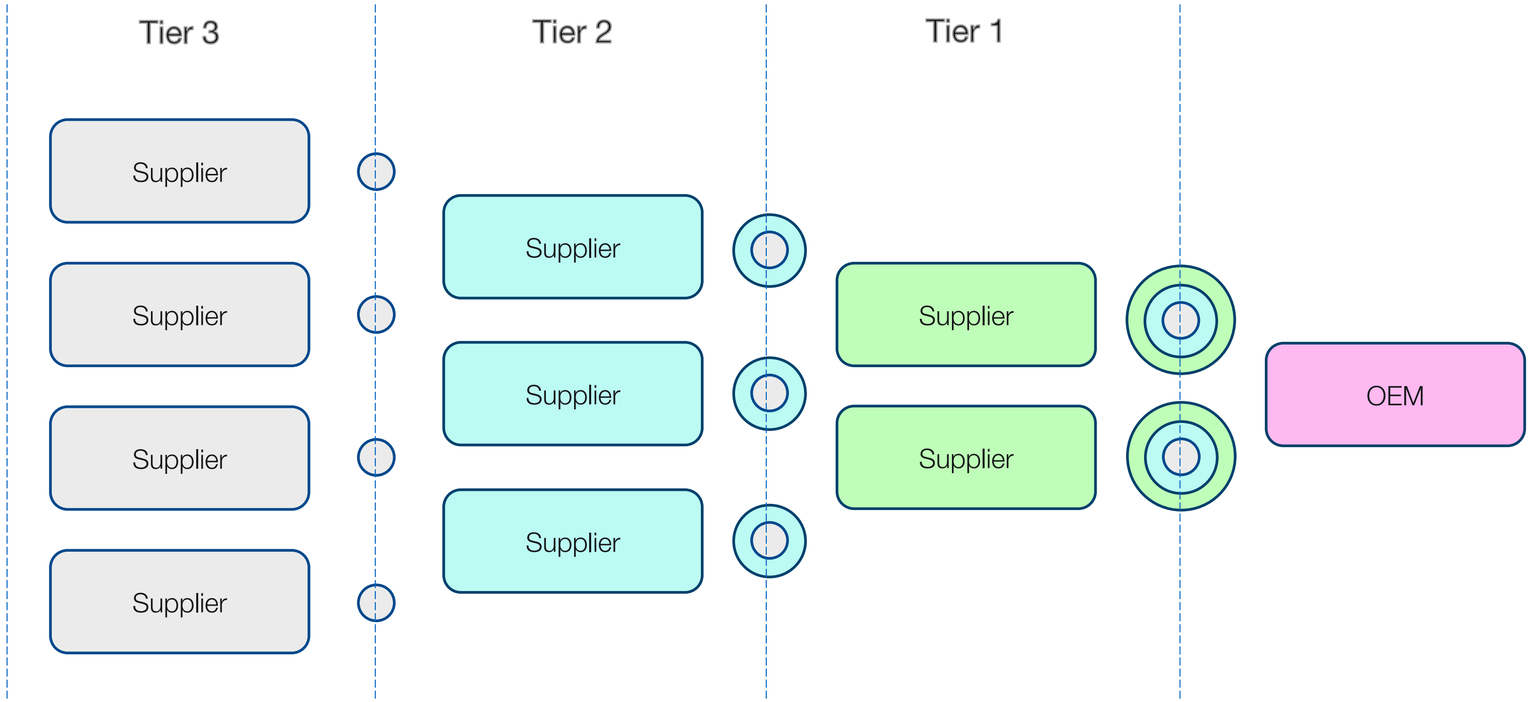
Counterfeit Mitigation in IC Supply Chains

Dr Leonardo Aniello
l.aniello@soton.ac.uk

HD-Sec Workshop

September 16th, 2021

IC Supply Chain



Counterfeiting Problems

- Lack of visibility on provenance of procured components
- Available tracking data of procured components is fragmented and not 100% trustworthy
- Hard to keep component suppliers accountable for their conduct

Requirements of a Tracking Platform

- Platform integrated with the whole supply chain, to reliably record the history of each procured component
  - Better visibility on suppliers
  - Availability of tracking data about procured components
  - Ability to prove the bad conduct of suppliers

- Platform distributed over different countries and regulatory frameworks
  - Which organisation/institution would be best placed to control such a platform?
  - A decentralised approach would be more suitable

Proposed Solution

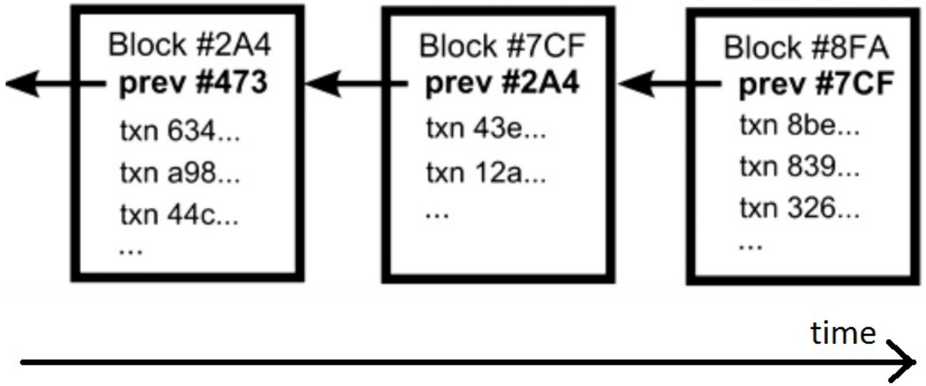
- How to build such decentralised tracking platform?
  - Consortium Blockchain

- How to identify components within the supply chain?
  - Physically Unclonable Function (PUF)

Based on: *L. Aniello, B. Halak, P. Chai, R. Dhall, M. Mihalea, A. Wilczynski. "Anti-BIUFf: towards counterfeit mitigation in IC supply chains using blockchain and PUF." International Journal of Information Security (2020): 1-16.*

Blockchain

- Decentralised system of peer nodes to store transactions
  - Ledger of transactions
  - Transactions added in batches (blocks)
  - Each node keeps a copy of the ledger
- Additional mechanisms to ensure ledger copies are kept consistent
- Strong guarantees on transaction integrity and availability
- Best known example: Bitcoin
  - Open membership
  - Transactions are public
  - Proof-of-Work – a new block generated every 10 minutes



Consortium Blockchain

- Limitations of Bitcoin-like blockchain
  - Bad performance
    - High latency (8-12 minutes in Bitcoin, 12 seconds in Ethereum)
    - Low throughput (3-7 tx/s in Bitcoin, 23-25 tx/s in Ethereum)
  - Privacy
  - Stability
- Consortium blockchain
  - Managed by a consortium of companies
  - Closed membership → better privacy
  - Authenticated nodes → no need for Proof-of-Work
    - More efficient mechanisms can be used
  - No cryptocurrency → better stability

Physically Unclonable Function (PUF)

- A physical entity whose behaviour is a function of its structure and the inherent random variations introduced by the chip manufacturing process
- A PUF can be integrated inside electronic components
- Two identical devices have two distinct PUF-based input/output behaviours
- PUF can be used to identify ICs reliably
  - This requires a set of challenge-response pairs
- PUF-based IC identification is tamper-proof

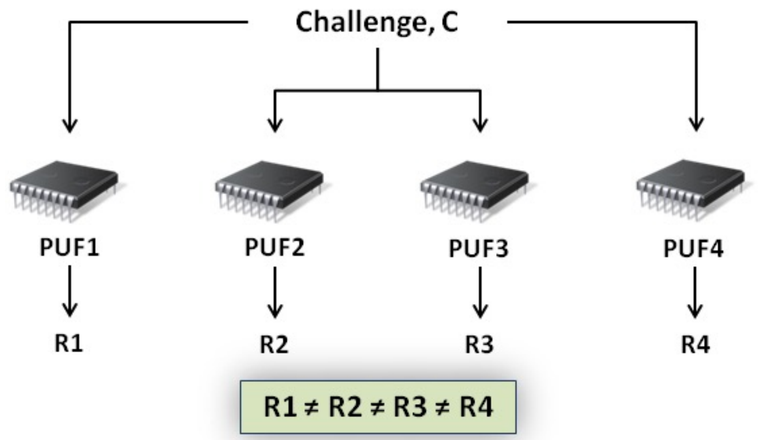
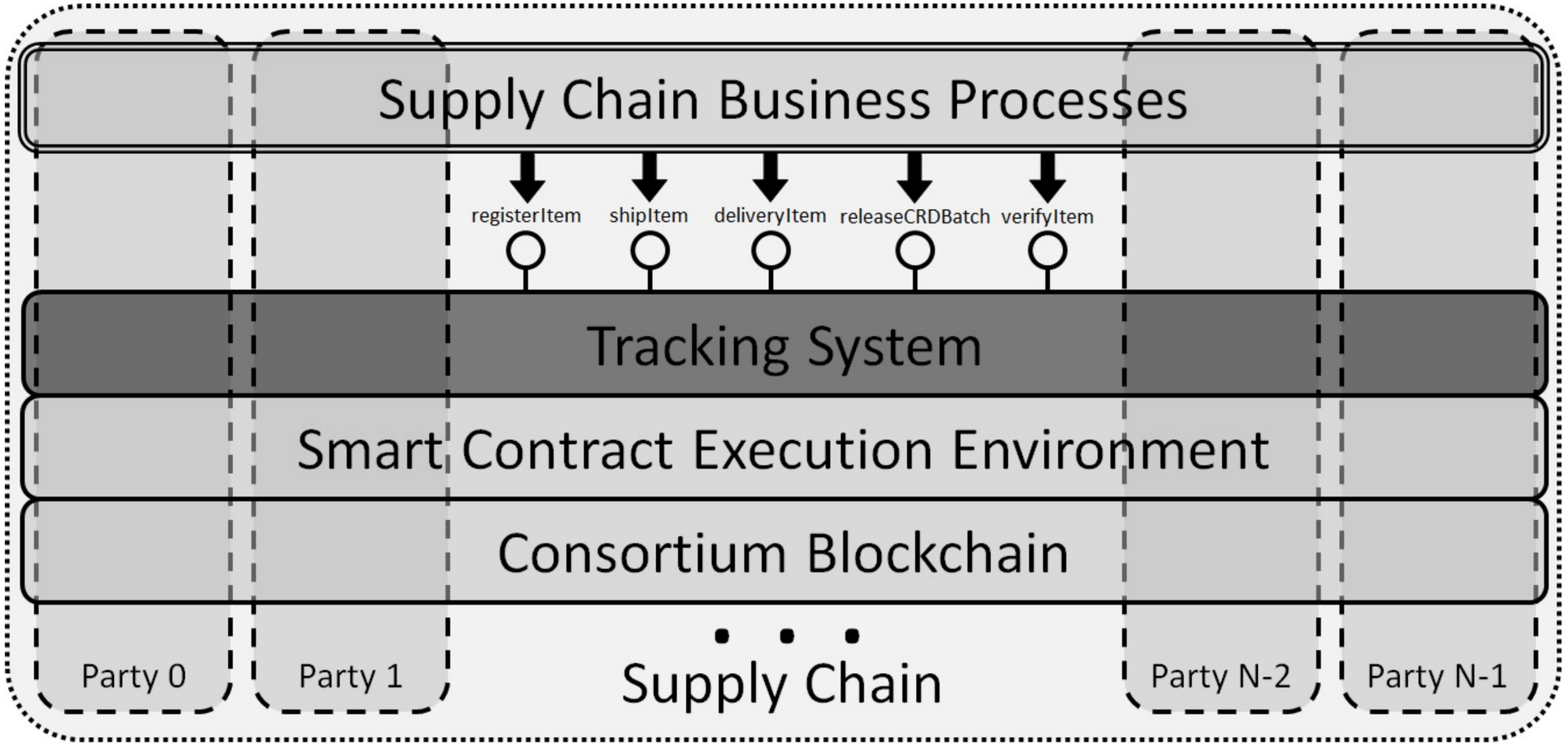


Image from http://rijndael.ece.vt.edu/puf/background.html

Anti-counterfeiting Blockchain- and PUF-based infrastructure



Anti-counterfeiting Blockchain- and PUF-based infrastructure

Tracking Mechanism

1. Registration – `registerItem()`
   - Challenge-response (CR) batch of the PUF obfuscated and stored
2. Shipping – `shipItem()`
3. Delivery and Verification
   - Delivery – `deliverItem()`
   - Release of CR batch – `releaseCRDBatch()`
   - Verification – `verifyItem()`

Anti-counterfeiting Blockchain- and PUF-based infrastructure

Attack Analysis

- If an adversary tampers with an IC somewhere in the supply chain
  - The function computed by the PUF is highly likely to change
  - The verification step would show the IC has been tampered with
- CR batches and other data stored in the blockchain cannot be modified
- Counterfeit ICs can be detected accurately
  - However, if the adversary were the supplier that registers the item, then they could compromise CR batches too…

Anti-counterfeiting Blockchain- and PUF-based infrastructure

Limitations and Future Work

- Different types of attack
- Privacy
- Performance and scalability
- Integration of PUF inside products
- Integration of the tracking platform within a supply chain