Blockchain-based Framework for Securing Integrated Circuits in the Supply Chain

Julie Dixon, Department of Computer Science and Software Engineering, Auburn University, AL 36849
Pinchen Cui, Department of Computer Science and Software Engineering, Auburn University, AL 36849
Ujjwal Guin, Department of Electrical and Computer Engineering, Auburn University, AL 36849

Motivation

- Counterfeiting, impersonation, and piracy are serious threats to the security and reliability of Internet of Things (IoT) and Cyber-Physical Systems (CPS) infrastructures.
- An adversary can create a backdoor on a counterfeit device, compromising its authenticity
- Security challenges to account for include in-transit thefts, human errors, delivery and management failures, and dishonest entities in the supply chain.
- Blockchain Framework Solution is not only useful in providing a solution to tracking integrated circuits, it can be modified to become a secure solution to tracking any electronic part through a supply-chain

Introduction

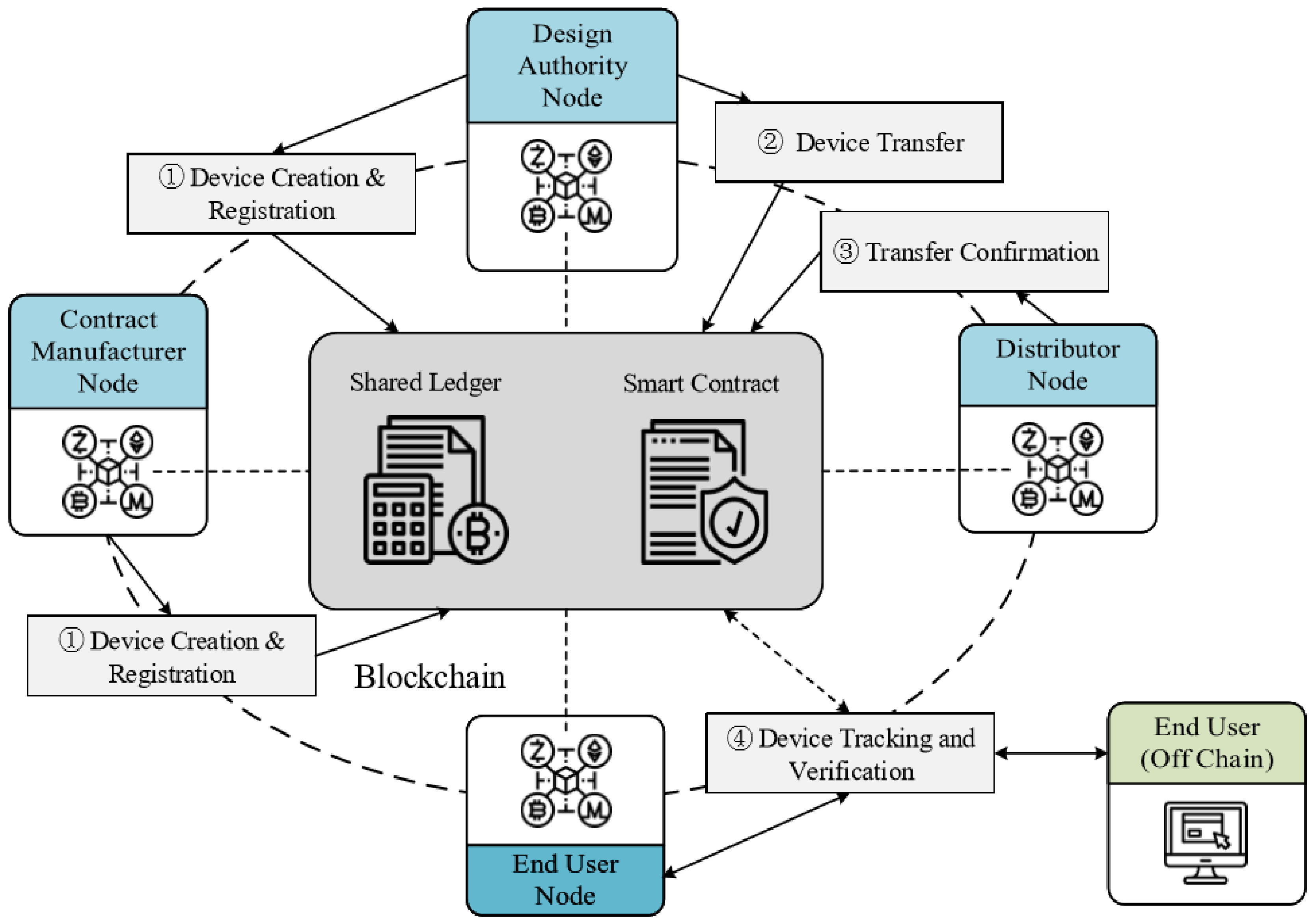
- We provide a low cost means for a user to authenticate Integrated Circuits
- Unique IDs are used to ensure traceability and using PUF specifically will ensure the device is unclonable
- This solution tracks and records the locations a chip has traversed, such as Design Authority, Manufacturer, Distributor, Customer, or Adversary location.
- Unauthentic device registrations and transactions are detected and prevented through a shared ledger, smart contract, and trusted entities

Key Features

- Permissioned Blockchain
  - Smart contract
  - Shared ledger
  - Trusted members
- Hyperledger is a permissioned Blockchain platform used to build our solution
  - No transaction fees
  - Low latency and high throughput

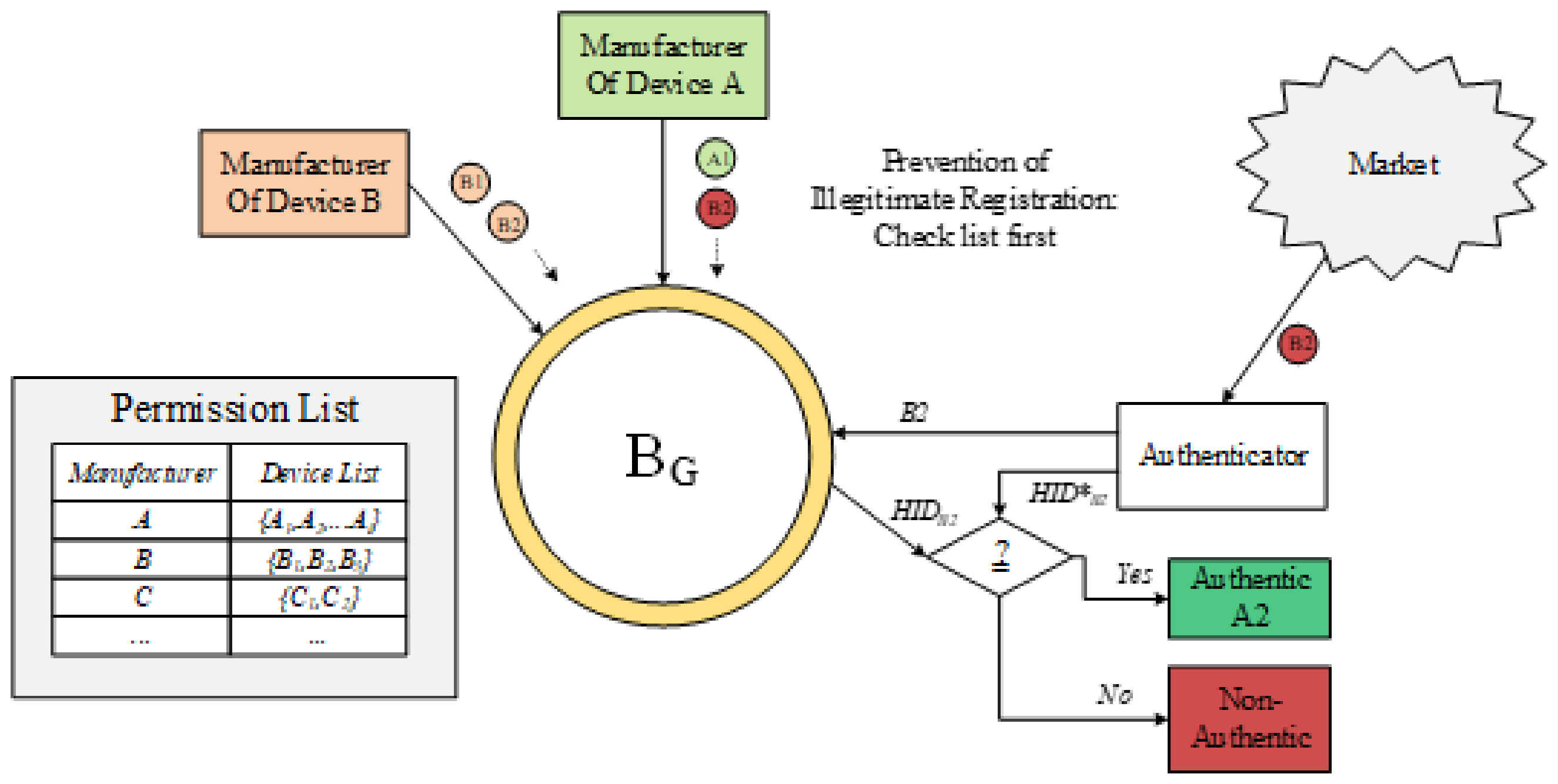
Blockchain Framework

- Registration
  - Design authorities and authentic manufacturers can register their device type and then individual chips by uploading hash of private ID (PUF response) and the public ID (serial number).
  - Once the device is registered in the shared ledger, anyone can access its identity from anywhere (the Blockchain architecture supports both integrity and availability).
  - Note that the values on the shared ledger are hashed, and the actual device IDs are not known to the public
- Transfer
  - The initial transaction that is performed to transfer devices from on entity to another requires:
    - Device type
    - Device amount
    - Individual device IDs
    - New owner
- Confirmation
  - After the initial transaction is performed a confirmation transaction is required and the device transfers will not be complete until the confirmation transaction is complete
  - New owner must verify the authenticity of the parameters: device type, device amount, individual device IDs
  - New owner must also compare the hash of the device IDs with the hash stored in the chain, if there is a discrepancy the transaction will be canceled due to a device compromised
- Query
  - There are two types of queries: normal query and rich query
    - Normal query return the data stored in the chaincode with a mapped keyword
    - Rich query allows for very specific requests to be implemented



Threat Analysis

- The Blockchain's internal structure prevents faulty registration, unauthenticated device transfers, and provides transparency between users

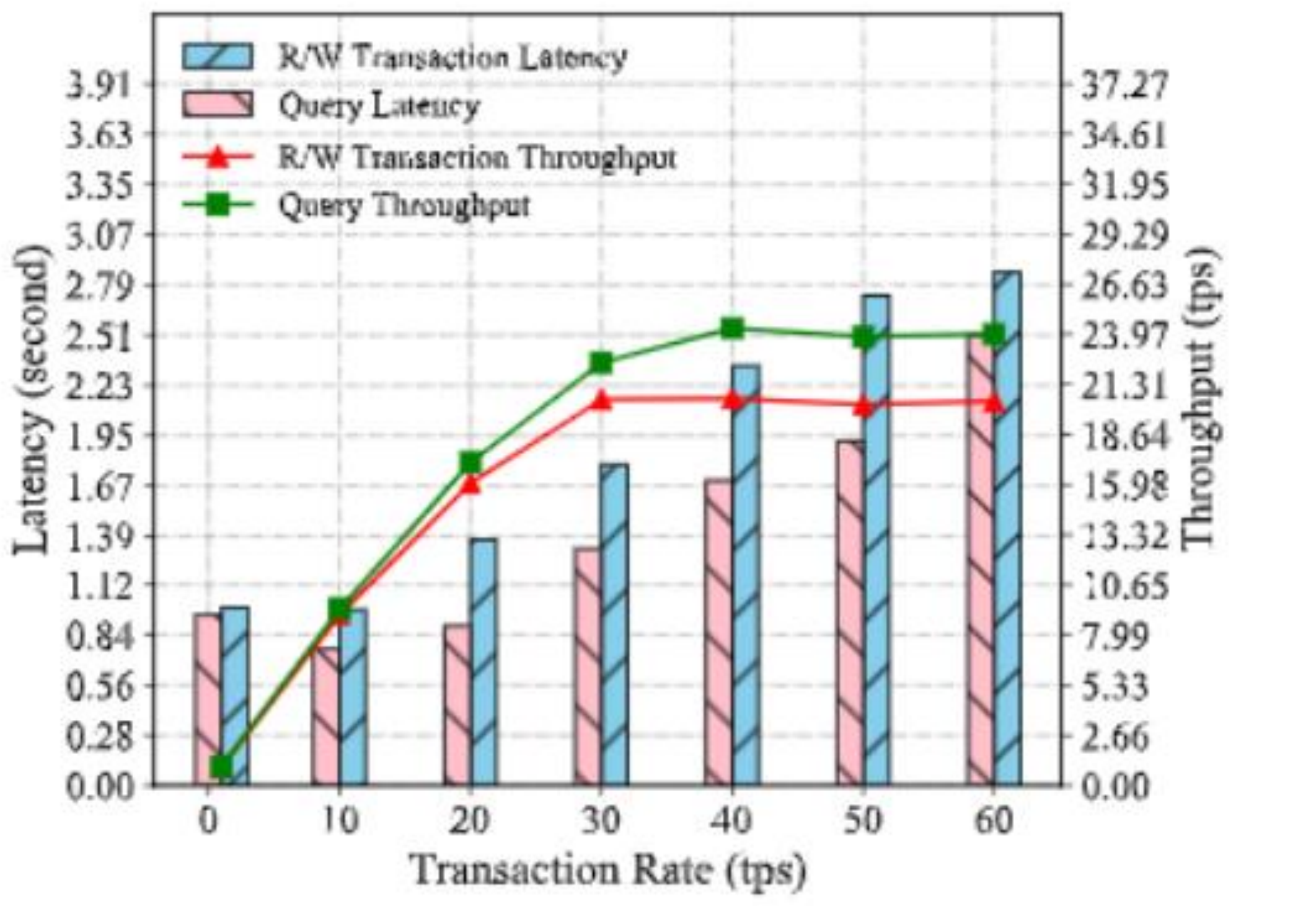


Security Analysis

- Illegitimate Device Registration
  - If faulty registration occurs where an adversary registers a illegitimate device or device ID and this device is successfully transferred in the chaincode, one can prevent the device from being transferred (physically) by implementing an addition verification stage where the blockchain will be queried as to whether the devices are present in the system
- Illegitimate Device Transfer
  - Requiring both a transfer transaction and confirmation transactions in order to successfully transfer ownership of the IDs prevents adversaries or human error from illegitimately transferring devices
- Illegitimate Off-chain Distribution
  - In order to enforce the authenticity of devices, we do not register devices from independent distributors or brokers outside the members of the blockchain framework

Performance

- Transactions can be performed with a latency of less than 1.5 seconds
- Bottlenecks at 20 – 25 tps in a channel


R/W Transaction Latency
Query Latency
R/W Transaction Throughput
Query Throughput
Latency (second)
Throughput (tps)
Transaction Rate (tps)