EVOKE: Efficient Revocation of Verifiable Credentials in IoT Networks

33rd USENIX Security Symposium
14-16 August, Philadelphia, PA

Carlo Mazzocca[1], Abbas Acar[2],
Selcuk Uluagac[2], Rebecca Montanari[1]

[1]University of Bologna, [2]Florida International University

Motivation: Establishing Trust in IoT Networks

Lack of trust is one of the **major concerns** that limit the full usage of Internet of Things (IoT) devices and their data

Limited Storage and Computation

Limited Bandwidth

Unreliable Connectivity

Low Transmission Range

Identify Devices and Establish Mutual Trust

- Centralized identity management does not meet the requirements of IoT as they **rely heavily on centralized entities** (e.g., PKI CAs)

  → Scalability

  → Single Point of Failure

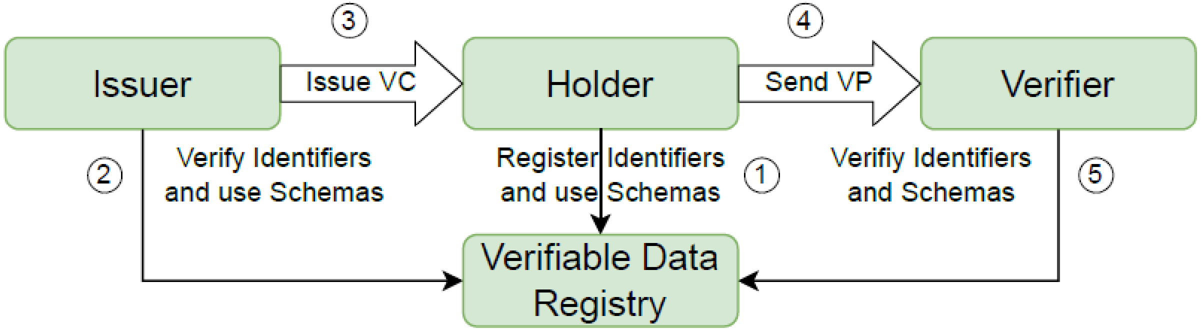
  → Latency and Network Dependence

- Digital identification methods that promotes **decentralization** are **more suitable** for IoT environments

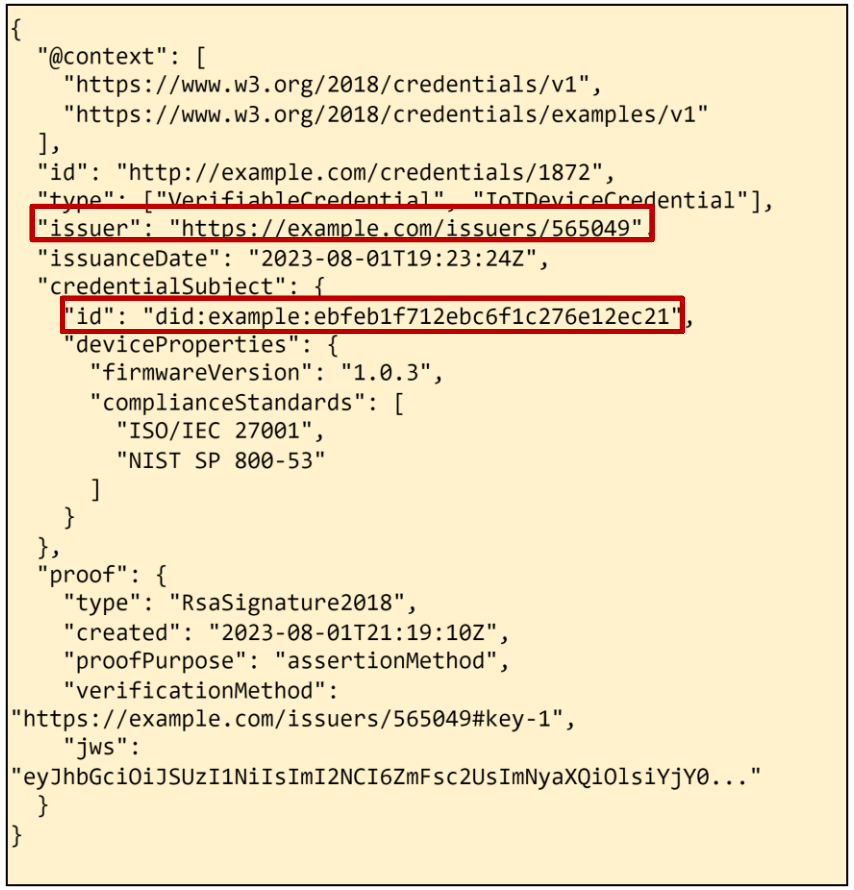
  → The World Wide Web Consortium standardized Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs)

Verifiable Credentials

A VC contains a set of statements about an entity that can be cryptographically verified by a third-party



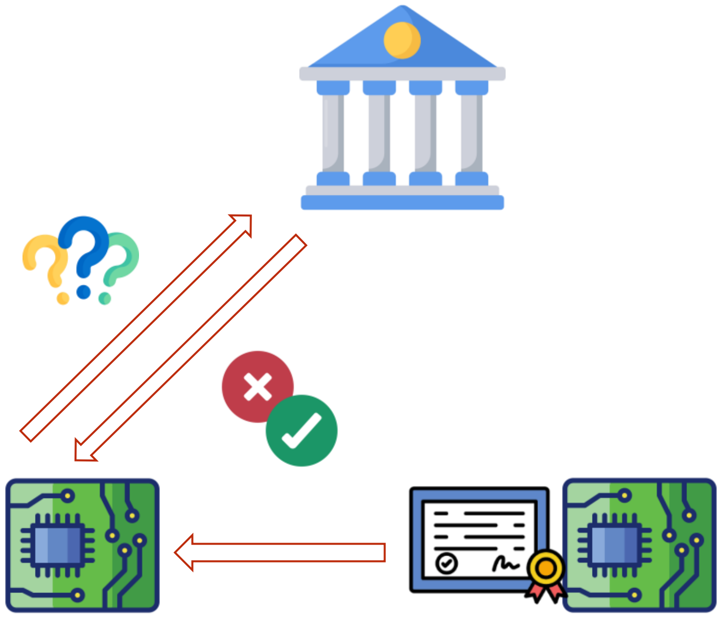
Issuer
3
Issue VC
Holder
4
Send VP
Verifier
2
Verify Identifiers and use Schemas
Register Identifiers and use Schemas
1
Verifiy Identifiers and Schemas
5
Verifiable Data Registry



```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.com/credentials/1872",
  "type": ["VerifiableCredential", "IoTDeviceCredential"],
  "issuer": "https://example.com/issuers/565049",
  "issuanceDate": "2023-08-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "deviceProperties": {
      "firmwareVersion": "1.0.3",
      "complianceStandards": [
        "ISO/IEC 27001",
        "NIST SP 800-53"
      ]
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2023-08-01T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod":
"https://example.com/issuers/565049#key-1",
    "jws":
"eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0..."
  }
}
```

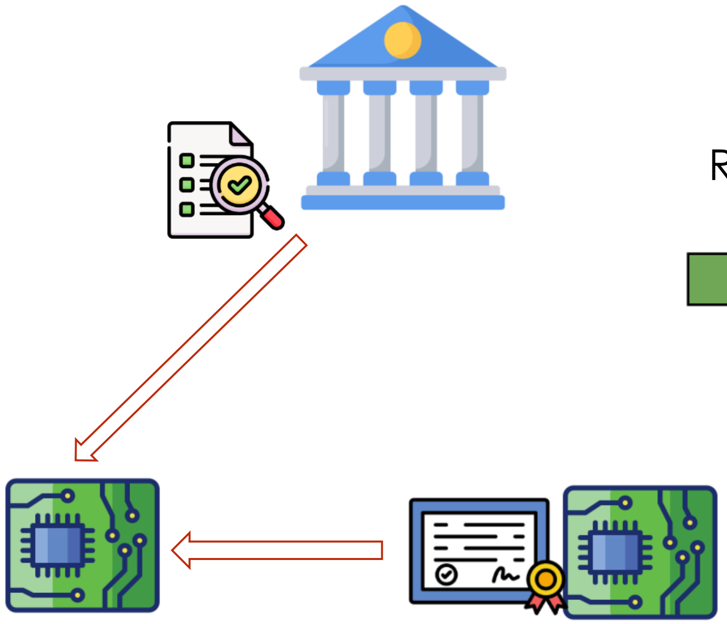
Limits of Existing Revocation Mechanisms

Online Certificate Status Protocol

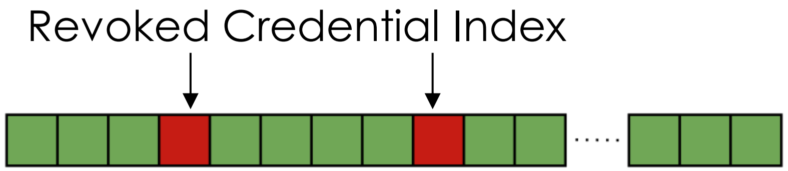


Reliable Network Connection

Certificate Revocation List



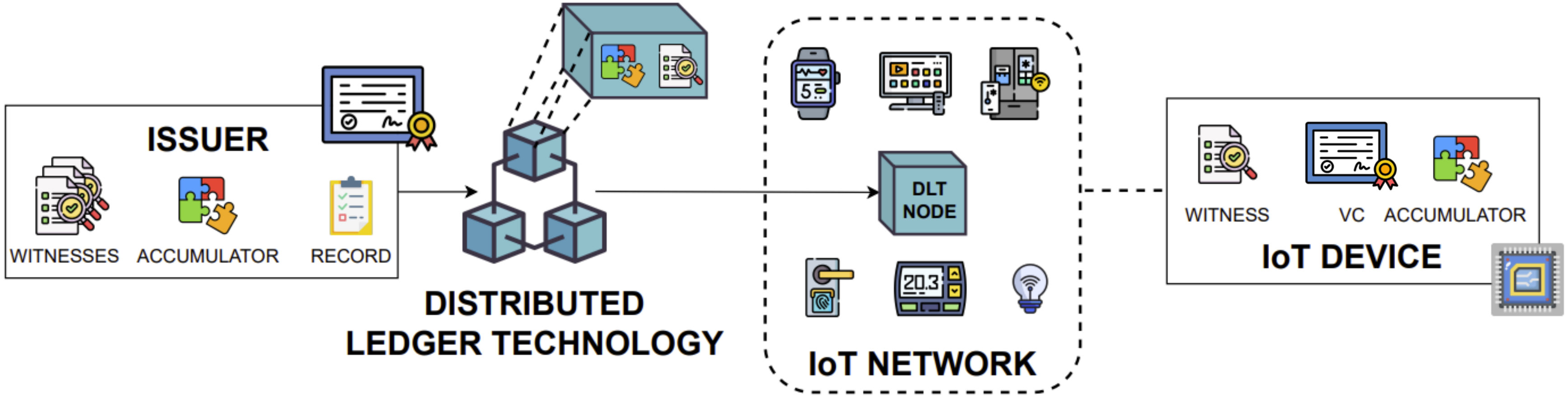
Bitstring Status List



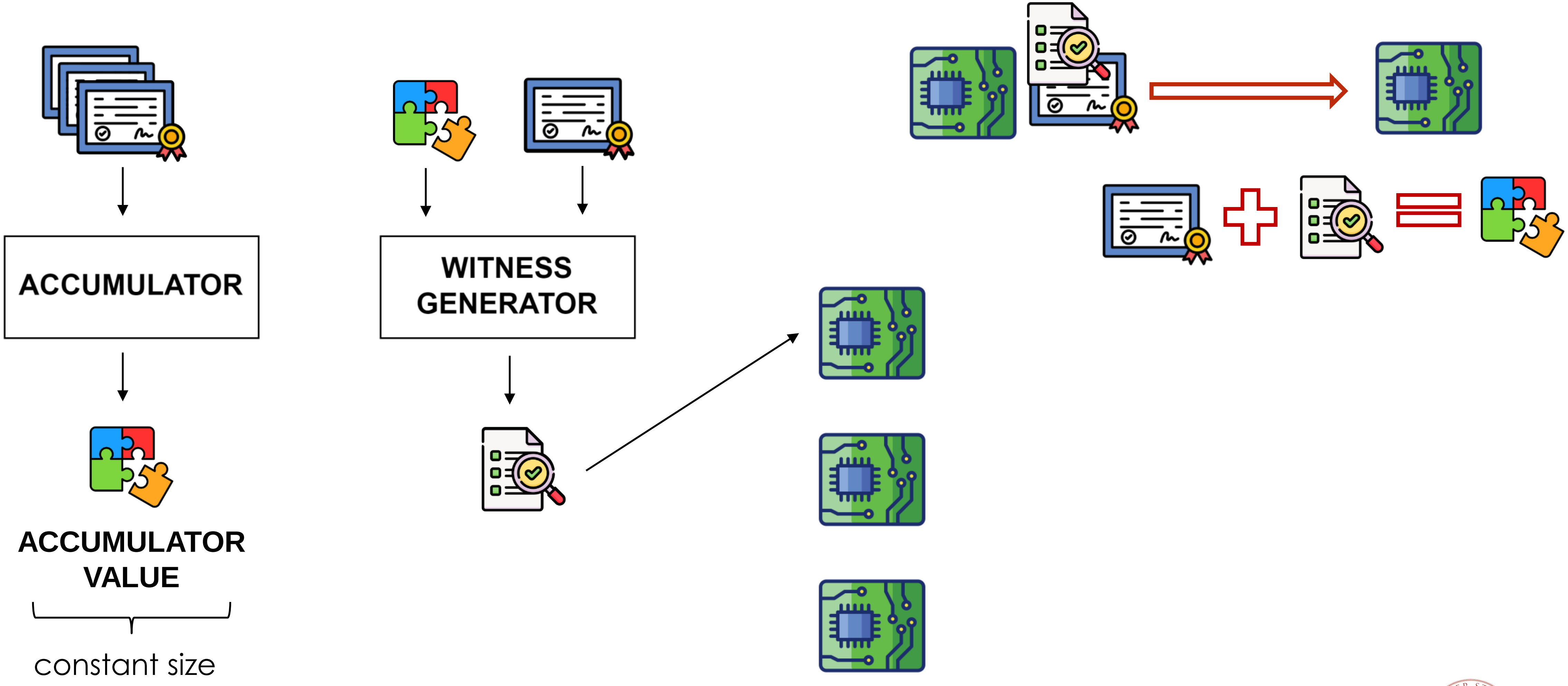
Storage and Network Overhead

EVOKE: Efficient Revocation of Verifiable Credentials in IoT Networks

- Lightweight revocation mechanism tailored for IoT networks
- Establishing trust requires **minimal computing** a **storing capabilities**
- Devices can share updates with **limited networking overhead**

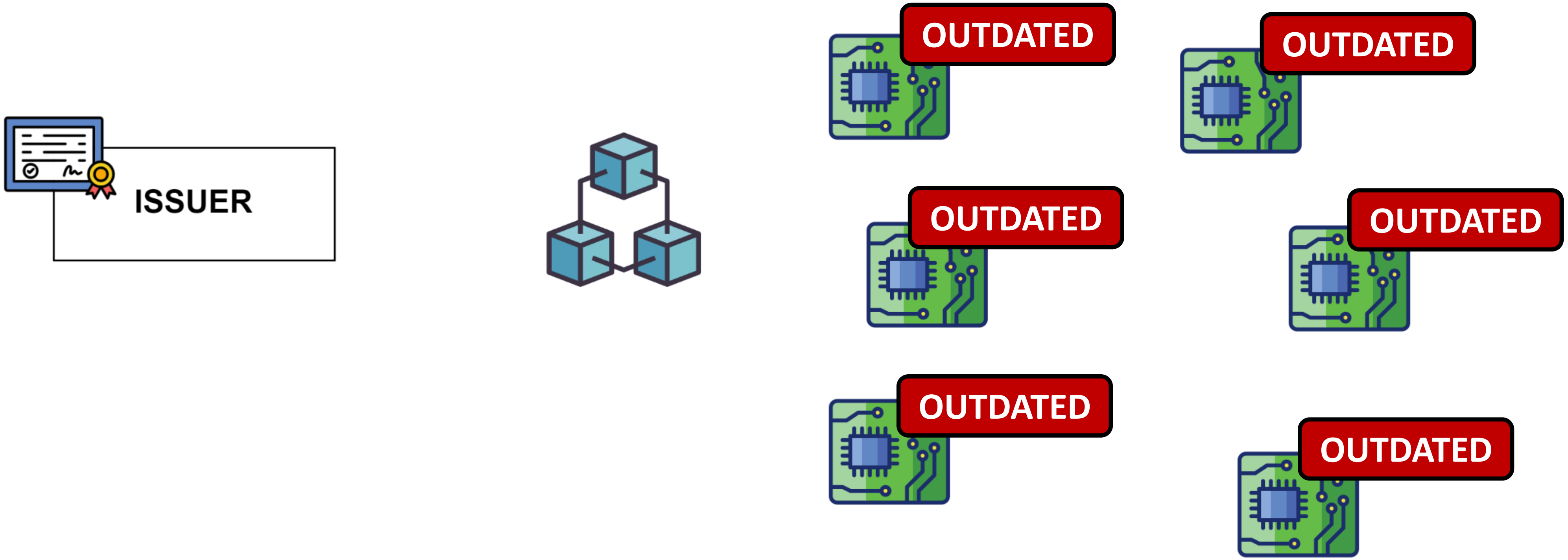


Overview


ACCUMULATOR
WITNESS GENERATOR
ACCUMULATOR VALUE
constant size

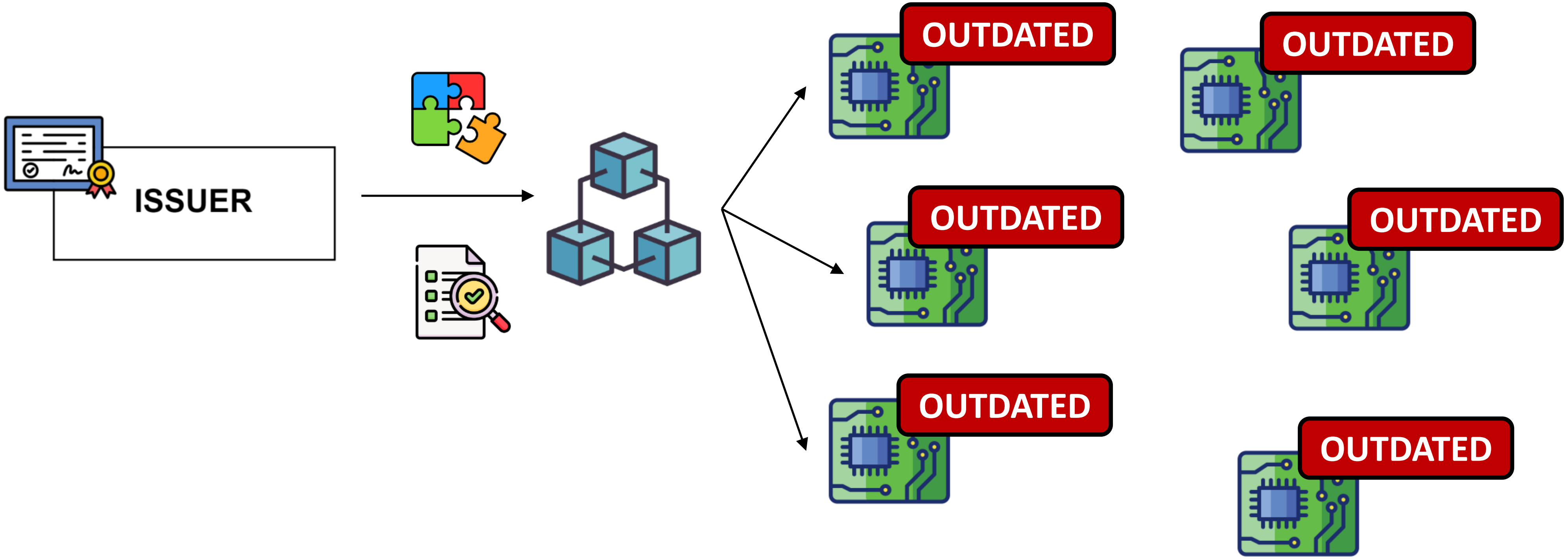
Revocation

- When VCs are revoked, the issuer must update the accumulator value and recompute witnesses



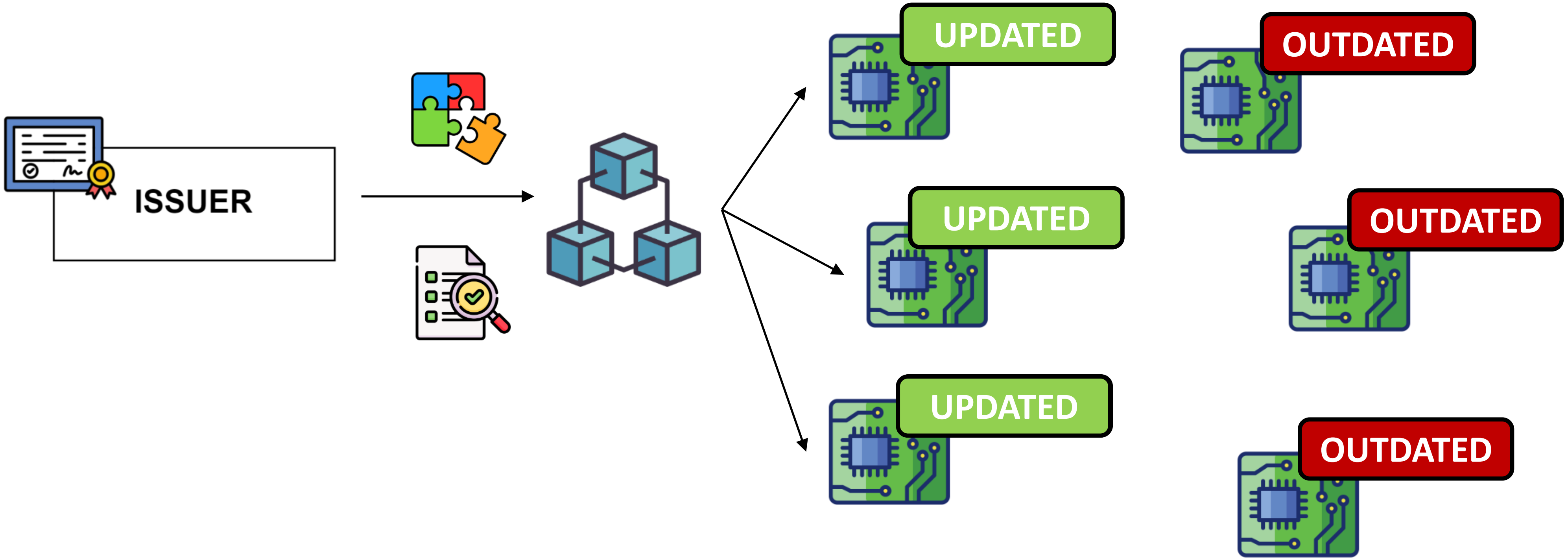
Revocation

- When VCs are revoked, the issuer must update the accumulator value and recompute witnesses

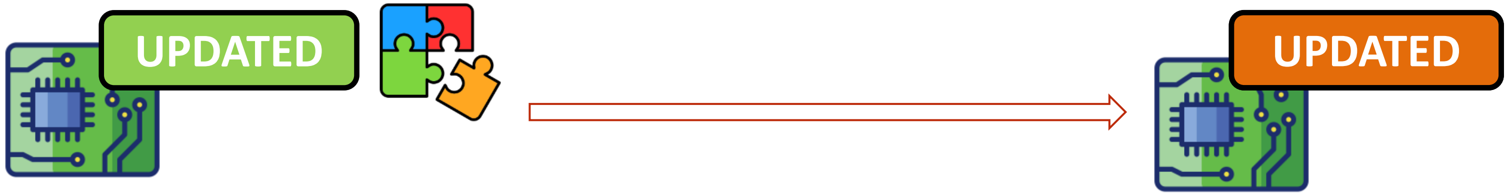


Revocation

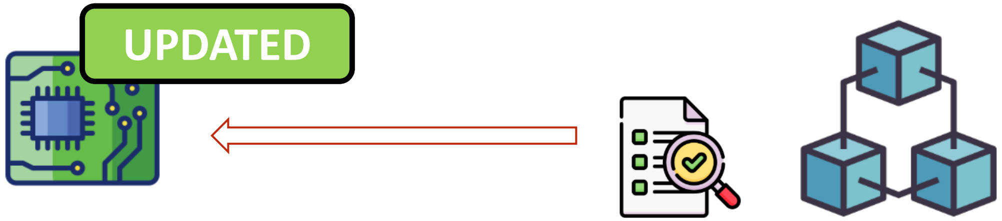
- When VCs are revoked, the issuer must update the accumulator value and recompute witnesses



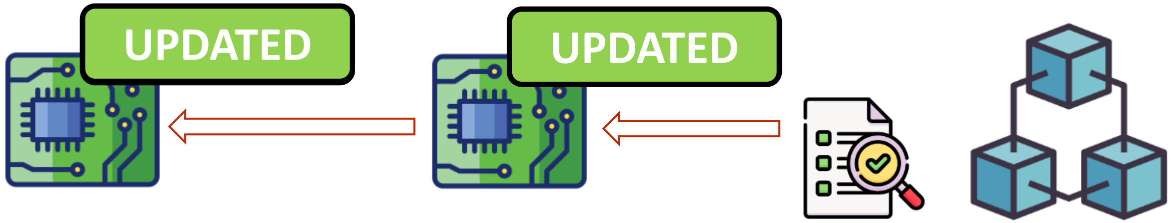
Offline Updates



The outdated device updates the accumulator value and disable trusted communications



DIRECT RETRIEVAL

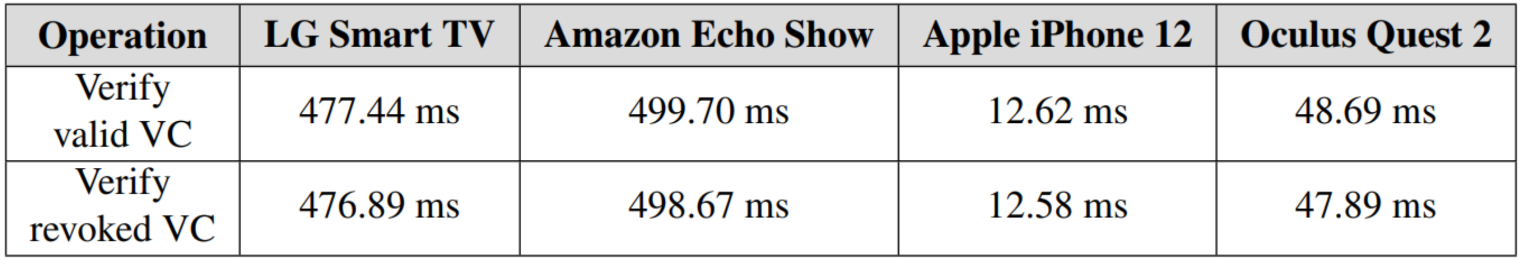


INDIRECT RETRIEVAL

Evaluation: Commodity IoT Devices

- Due to programmability constraints, we only consider devices supporting browser connection

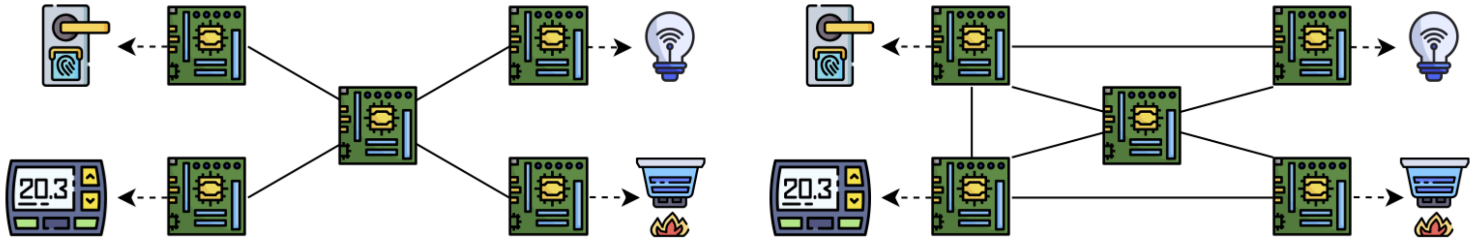
- Each device is required to store 1.5 KB for the accumulator value and the corresponding witness



Operation	LG Smart TV	Amazon Echo Show	Apple iPhone 12	Oculus Quest 2
Verify valid VC	477.44 ms	499.70 ms	12.62 ms	48.69 ms
Verify revoked VC	476.89 ms	498.67 ms	12.58 ms	47.89 ms

Evaluation: Hybrid Networks

- We consider star and mesh network topology
- Baseline represents latencies when sending minimal amount of data



(a) Star network topology

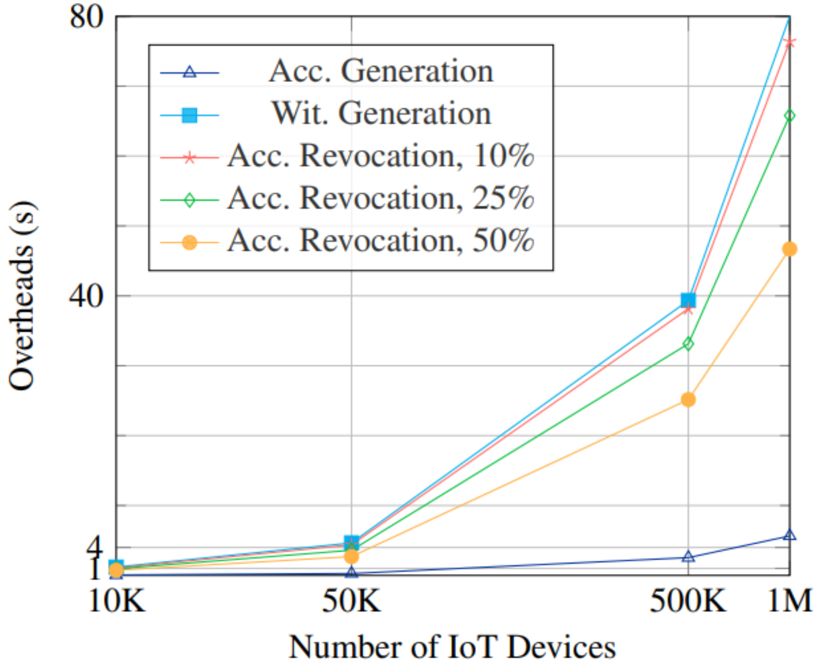
(b) Mesh network topology

Topology	Approach	Total Latency (Verify + Transfer)	E2E Latency
Star Network	EVOKE	1152.7 ms	948.3 ms
	Baseline	967.7 ms	705.5 ms
Mesh Network	EVOKE	545.2 ms	307.5 ms
	Baseline	97.4 ms	91.7 ms

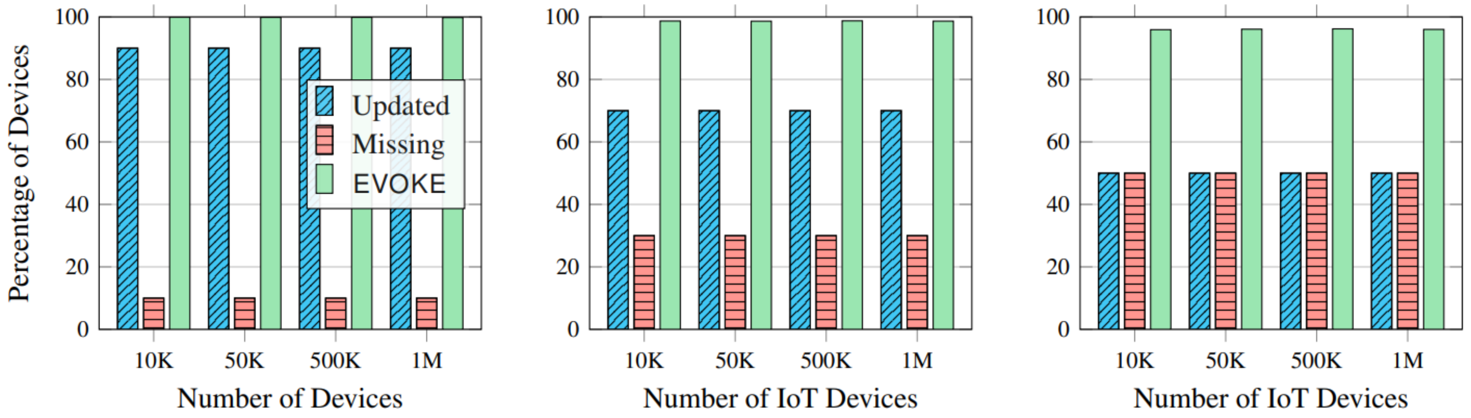
Evaluation: Large-scale Analysis

- 11th Gen Intel(R) Core(TM) i7-11370H @ 3.30 GHz, 4 cores and 16GB RAM
- Up to 1 million nodes
- 0.028% VCs revoked per day (10% yearly)
- Each device interacts with 5 random devices within an hour
- Percentage of devices missing updates (10%, 30%, and 50%)

Evaluation: Large-scale Analysis



Witness generation decreases over time as credentials getting revoked



(a) 10% devices missing updates

(b) 30% devices missing updates

(c) 50% devices missing updates

96% of the whole network is updated in the first hour

Conclusion

- **Minimal Computational and Storage Overhead**

  → Devices are only required to store 1.5 KB of data

- **High Scalability**

  → Memory requirements and verification time are independent from number of VCs

- **Offline Updates**

  → Even if a large portion of the network misses updates, almost the whole network can be updated in 1 hour

FIU

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

CSL
Cyber-Physical Systems
Security Lab

Thank you!

Carlo Mazzocca

Department of Computer Science and Engineering
University of Bologna

carlo.mazzocca@unibo.it