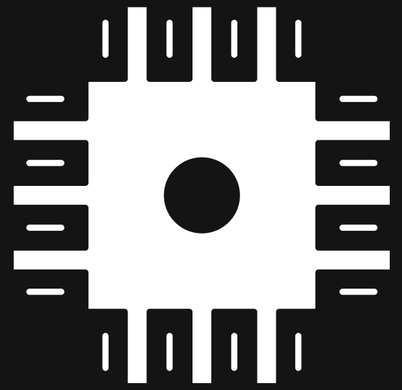
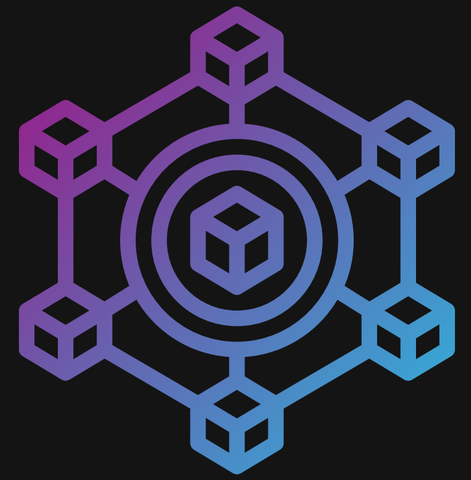
Talk On



Securing OTA Firmware Updates



Leveraging Blockchain for secure and immutable firmware updates

Whoami

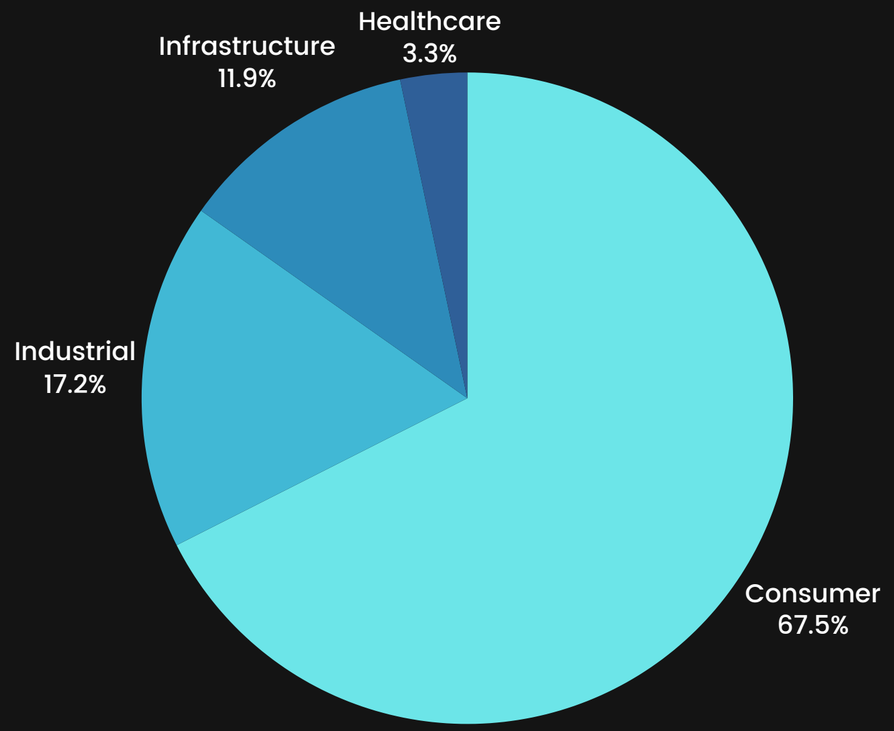
Google Summer of Code @OWASP

MLH Fellow @NEAR Protocol

MIT Bitcoin Hackathon Winner

LFX'23 @Linux Kernel

Some Stats

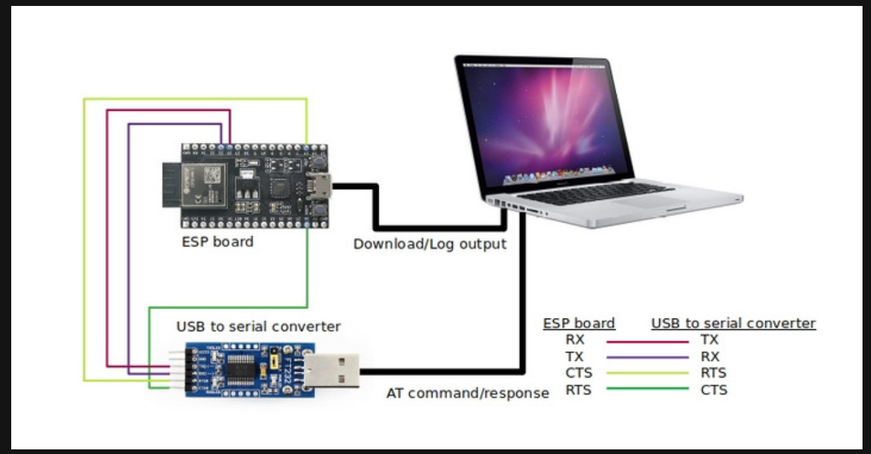


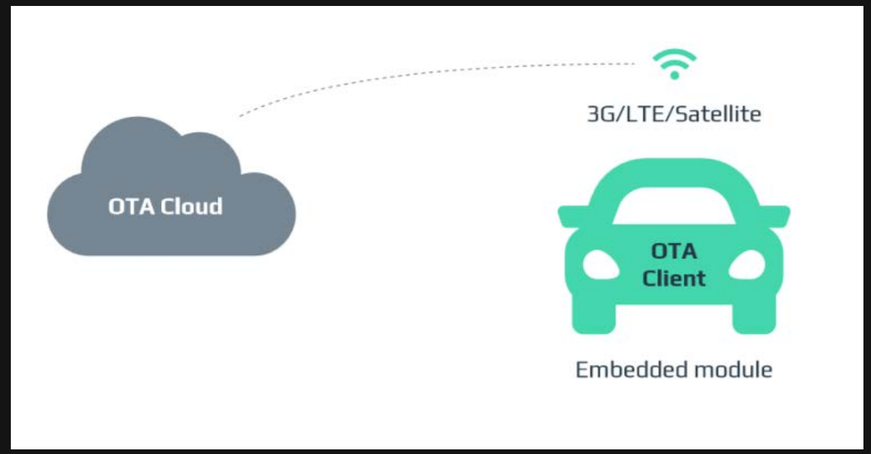
- 15.14 billion connected IoT devices worldwide (2023). Source
- 29.42 billion IoT devices will get added by 2030. Source

- **Firmware blues**: 77% Increase in injecting malicious firmware updates (2022).
- **DDoS Attacks**: 60% Surge in DDoS targeting OTA Updates (2022). Source
- **Servers under siege**: Increase in MIT (Man in the Middle) attacks on IOT Devices. (2022)

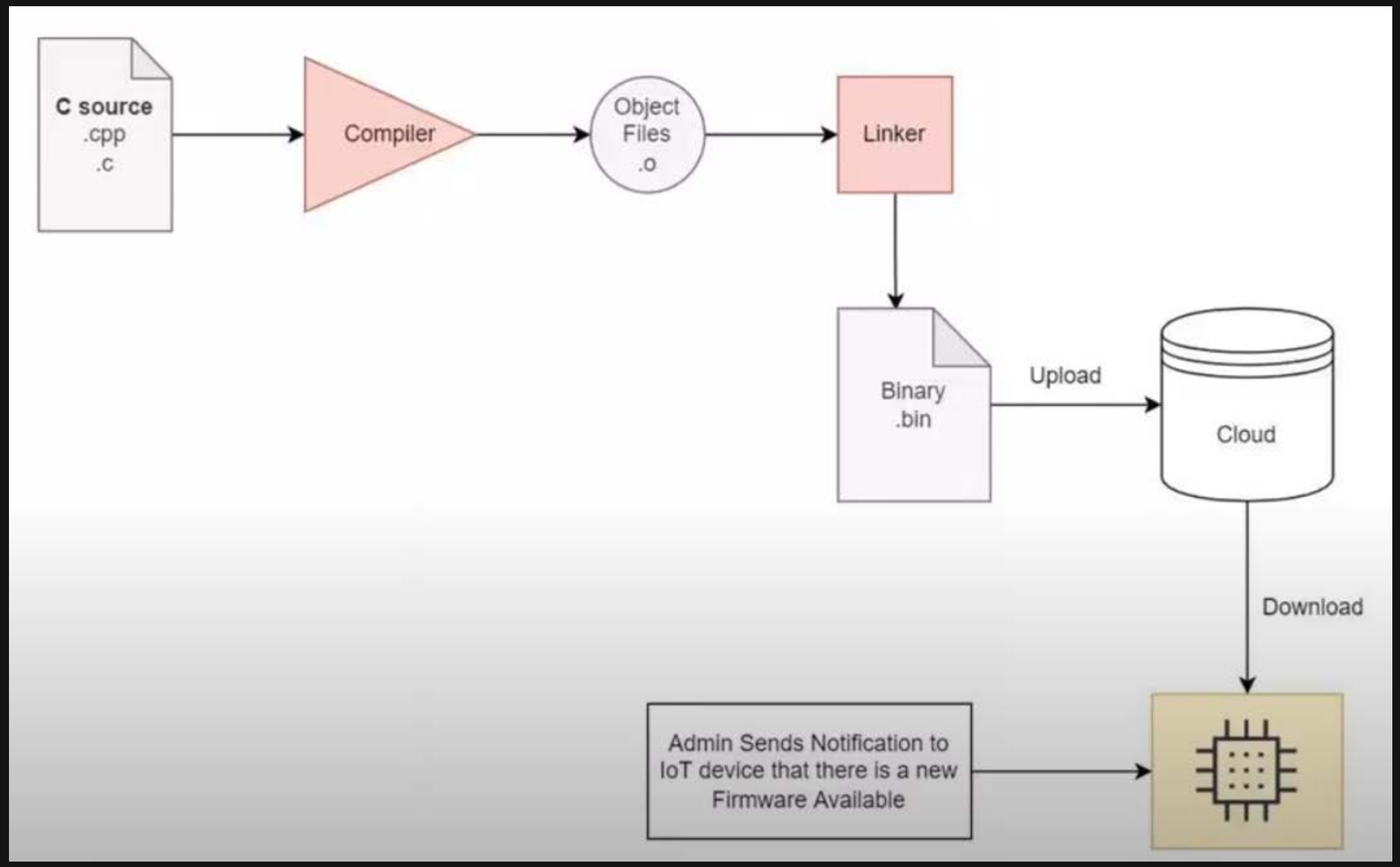
Problem

Importance of IoT security.

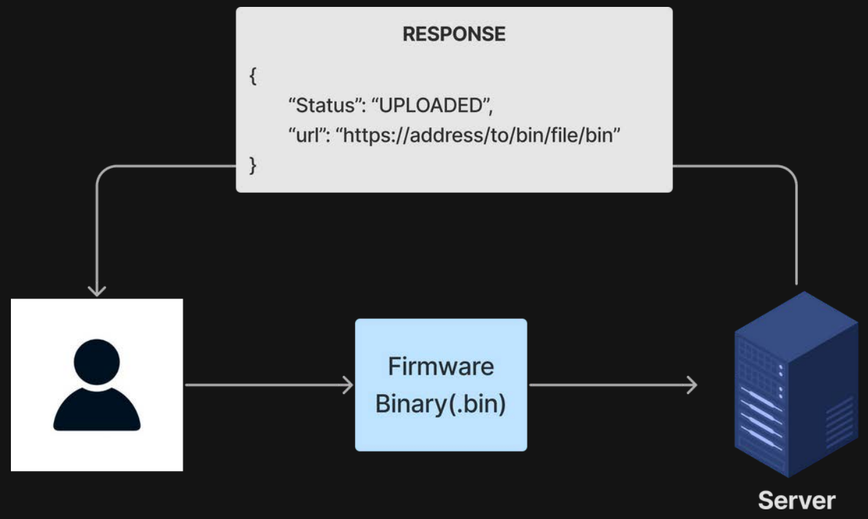




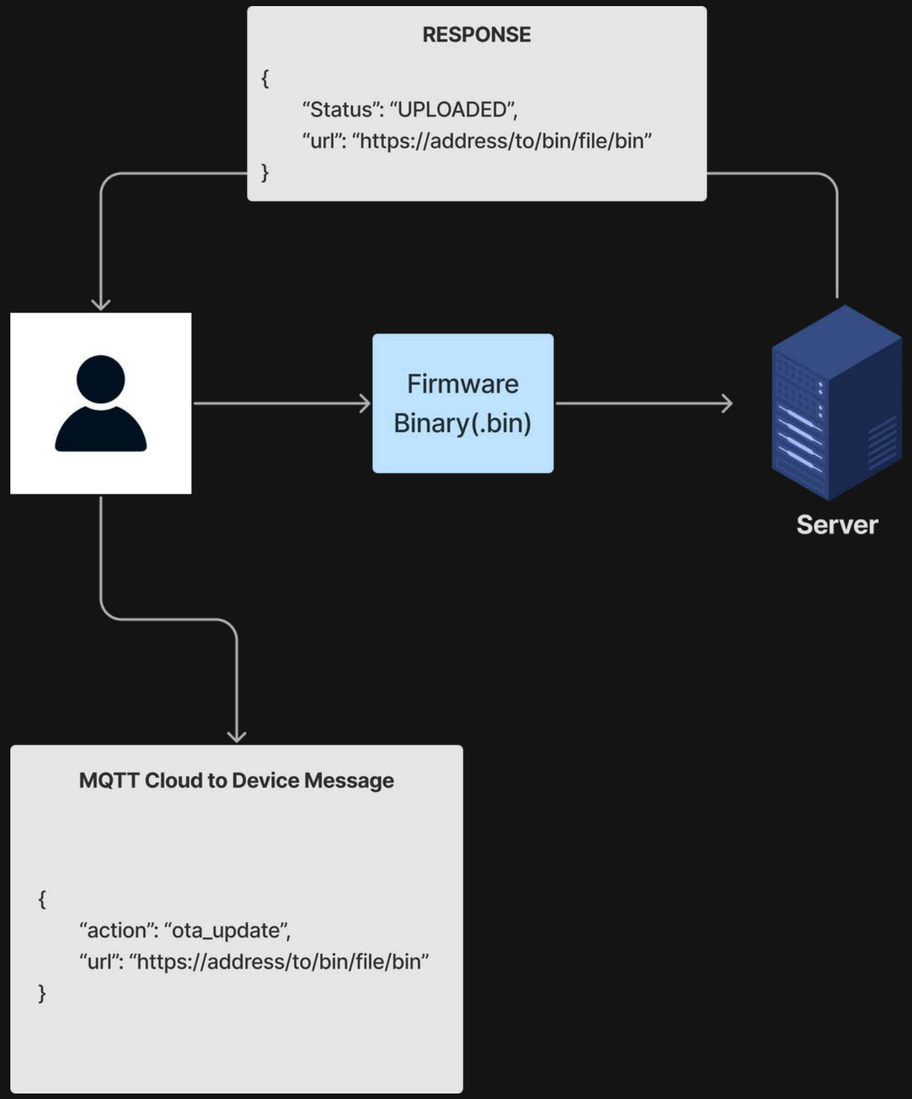
How OTA Works



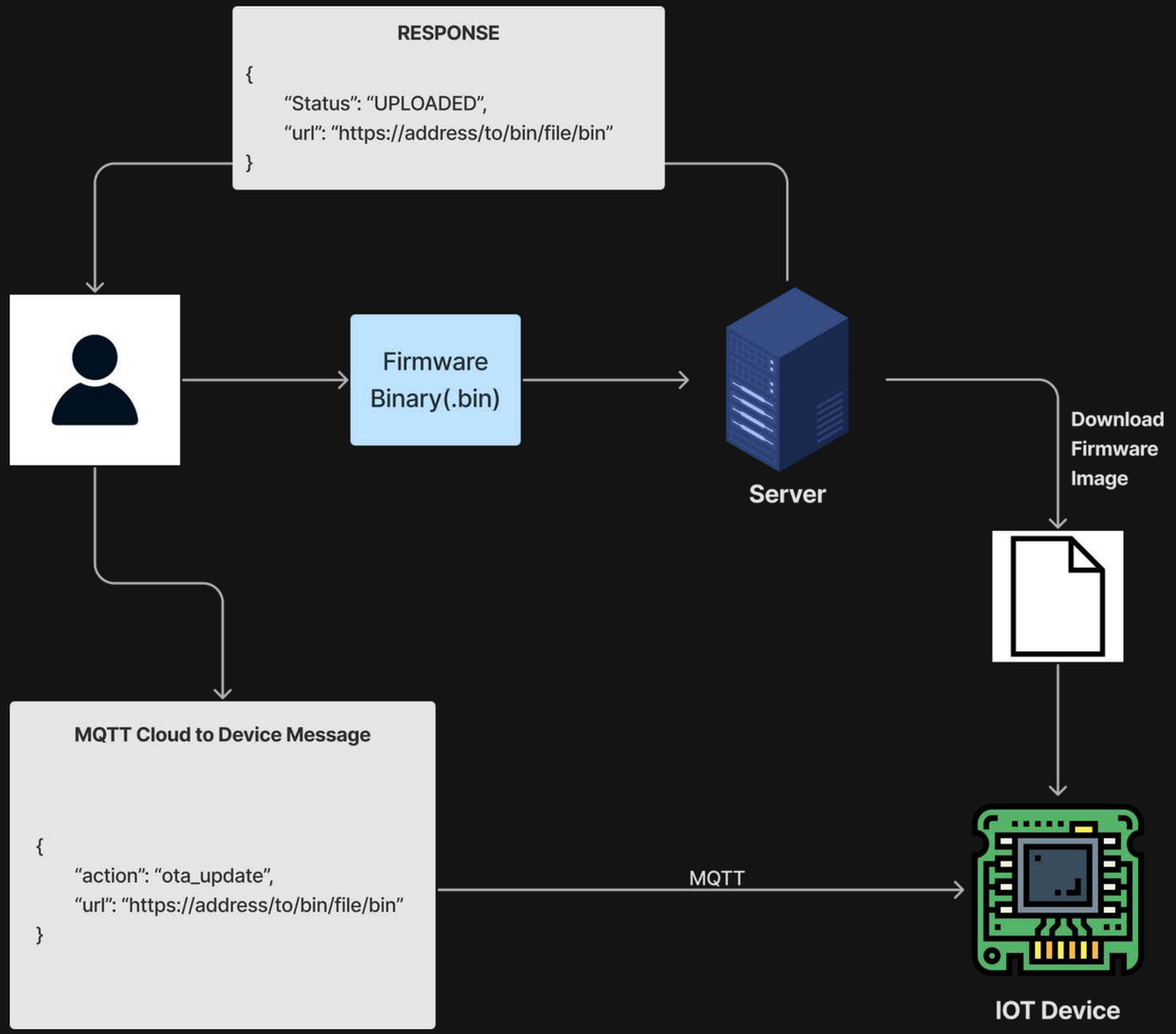
STEP 1


RESPONSE
{
“Status”: “UPLOADED”,
“url”: “https://address/to/bin/file/bin”
}
Firmware Binary(.bin)
Server

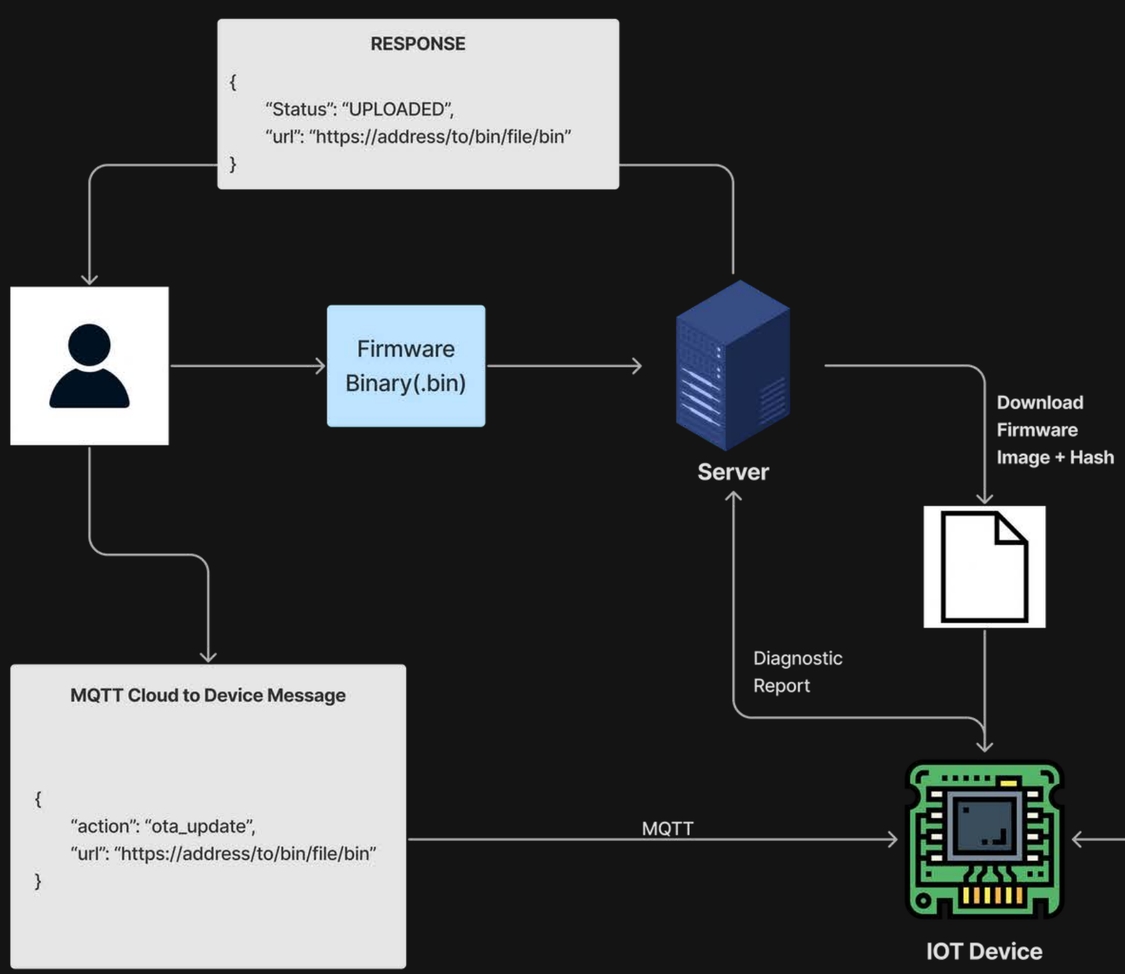
STEP 2

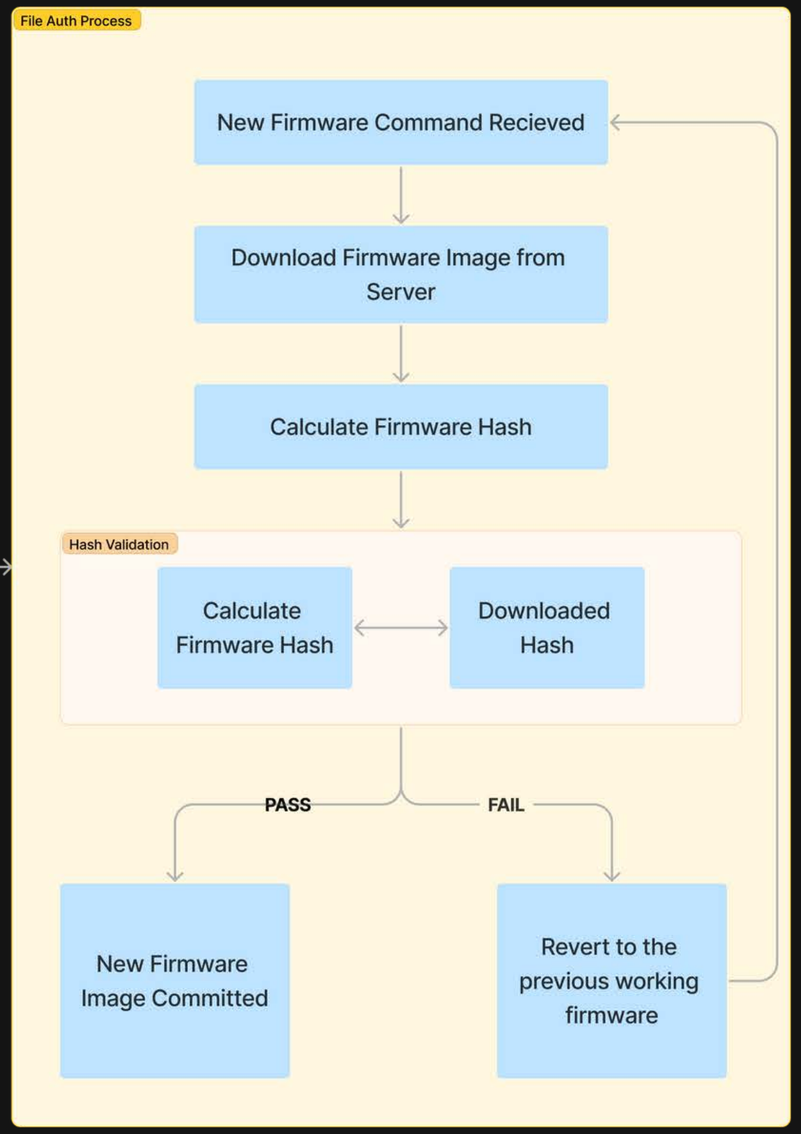

RESPONSE
{
“Status”: “UPLOADED”,
“url”: “https://address/to/bin/file/bin”
}
Firmware Binary(.bin)
Server
MQTT Cloud to Device Message
{
“action”: “ota_update”,
“url”: “https://address/to/bin/file/bin”
}

STEP 3

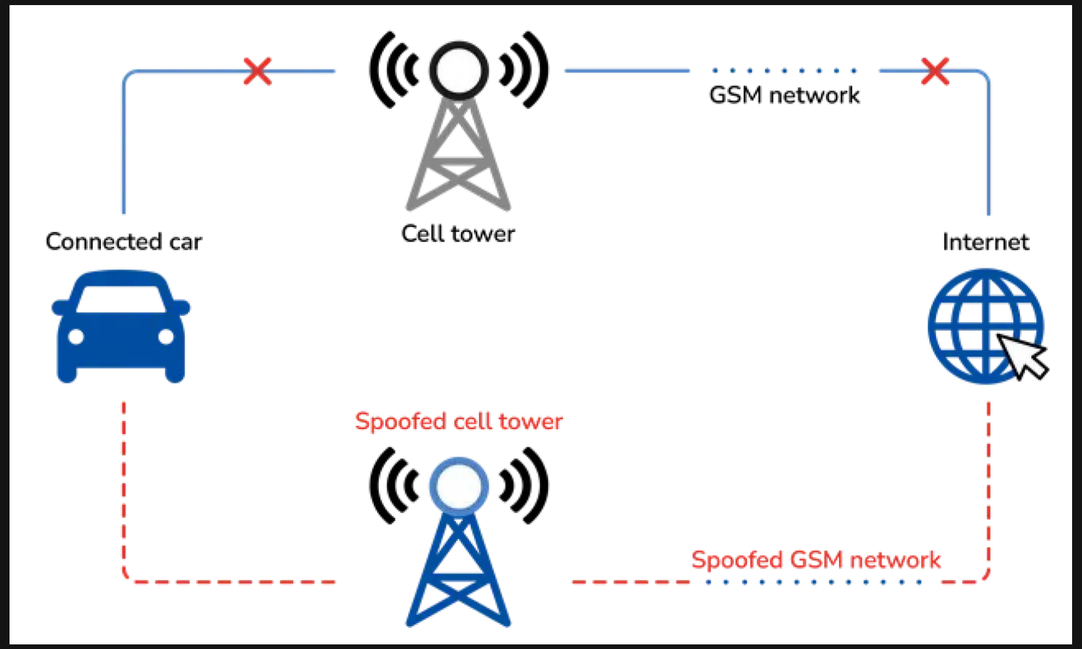

RESPONSE
{
“Status”: “UPLOADED”,
“url”: “https://address/to/bin/file/bin”
}
Firmware Binary(.bin)
Server
Download Firmware Image
MQTT Cloud to Device Message
{
“action”: “ota_update”,
“url”: “https://address/to/bin/file/bin”
}
MQTT
IOT Device

STEP 4

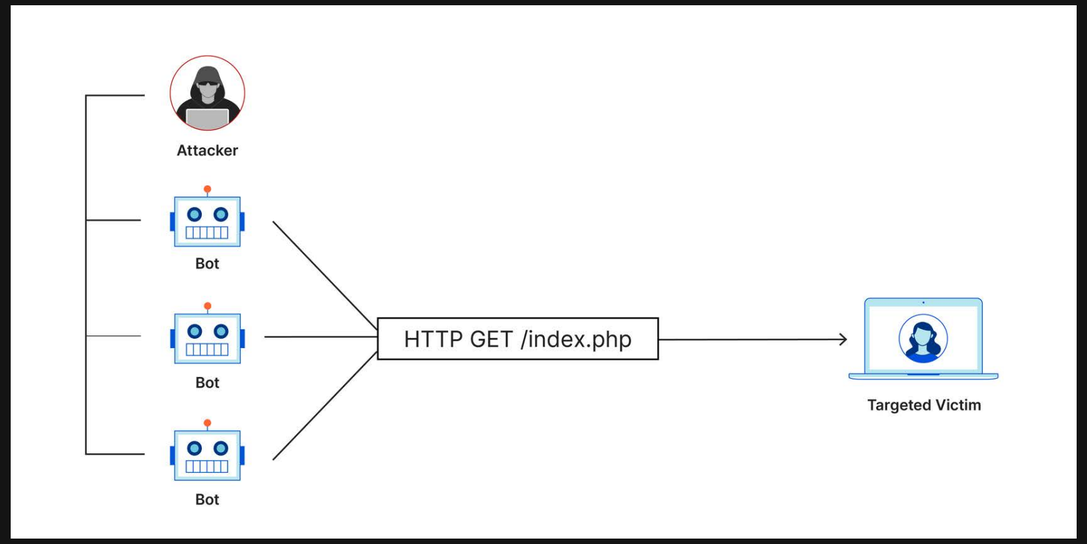

RESPONSE
{
“Status”: “UPLOADED”,
“url”: “https://address/to/bin/file/bin”
}
Firmware Binary(.bin)
Server
Download Firmware Image + Hash
Diagnostic Report
MQTT Cloud to Device Message
{
“action”: “ota_update”,
“url”: “https://address/to/bin/file/bin”
}
MQTT
IOT Device


File Auth Process
New Firmware Command Recieved
Download Firmware Image from Server
Calculate Firmware Hash
Hash Validation
Calculate Firmware Hash
Downloaded Hash
PASS
FAIL
New Firmware Image Committed
Revert to the previous working firmware

Challenges in OTA Firmware Updates



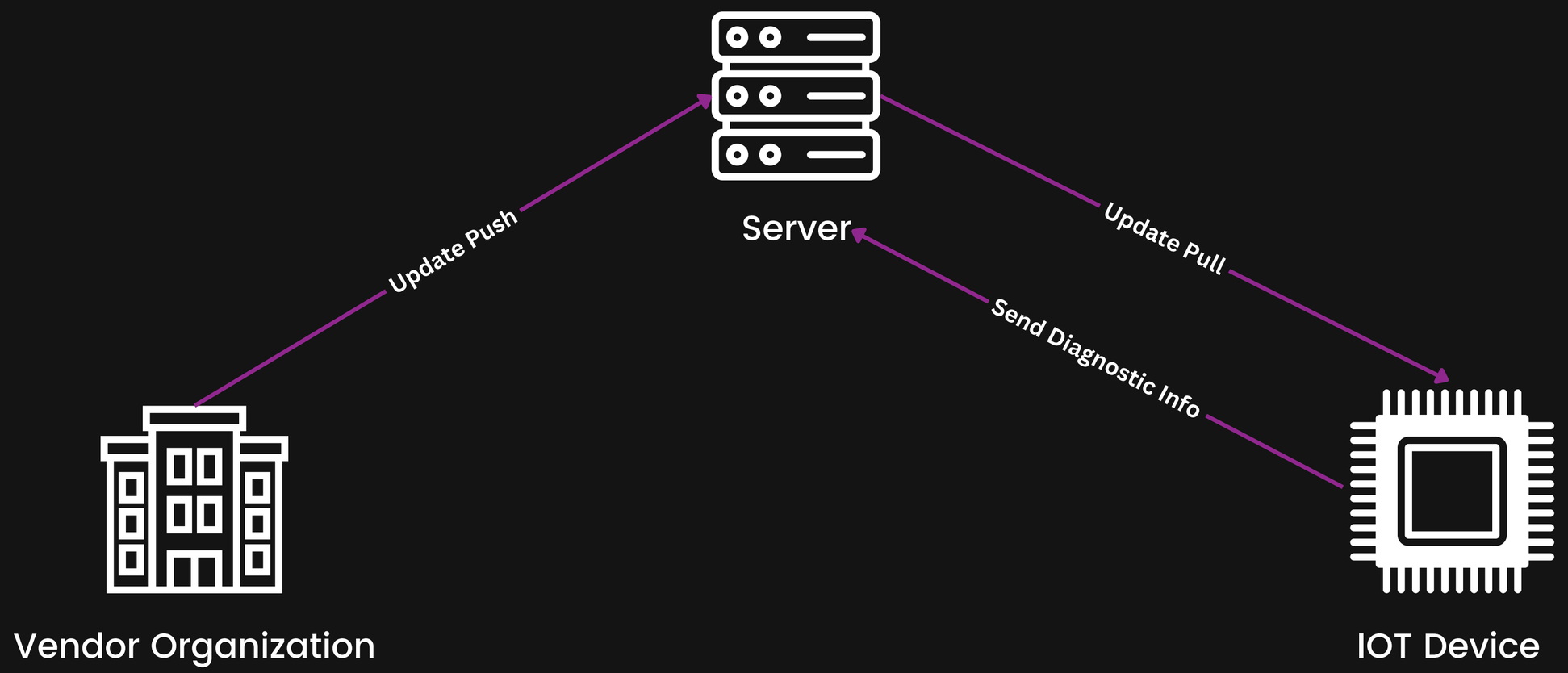
Man In The Middle Attack



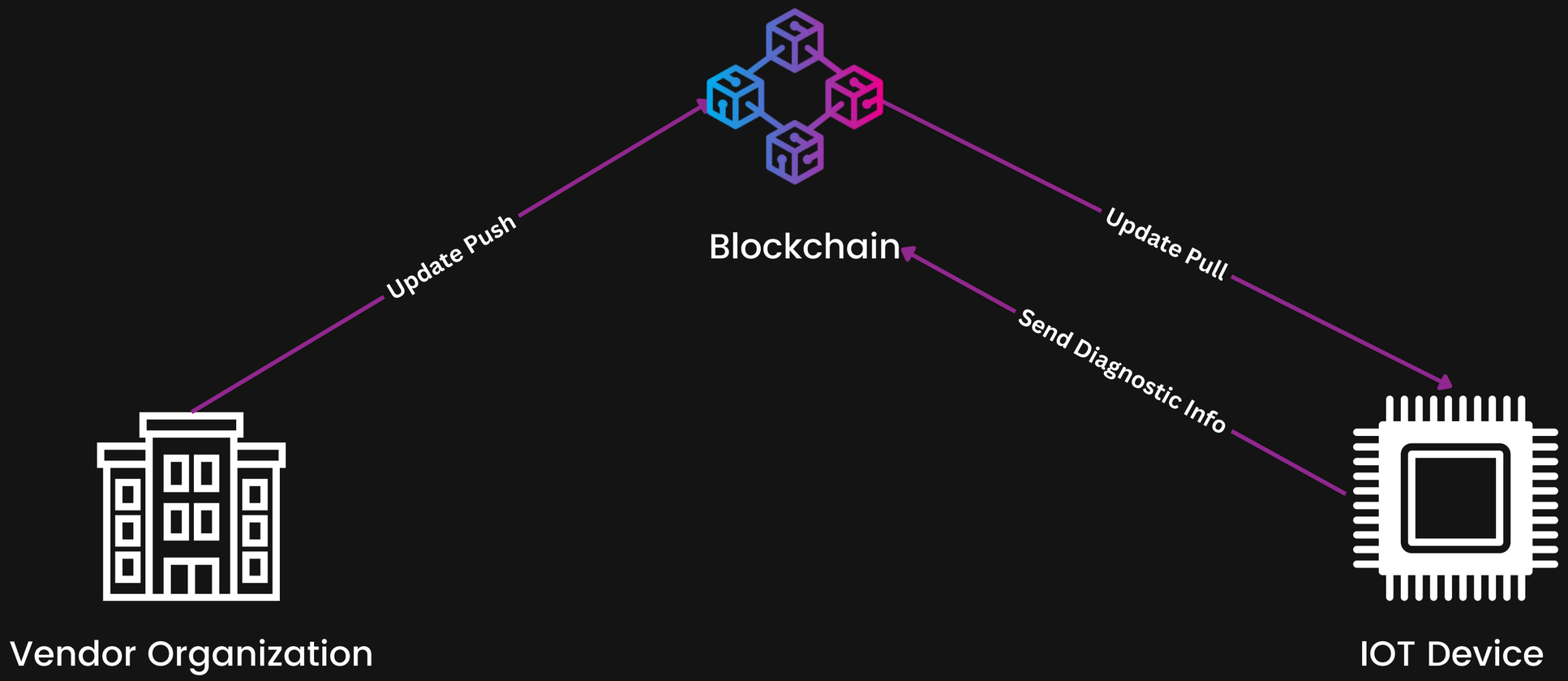
DDoS Attack

Centralised server got Compromised

The Need for Blockchain

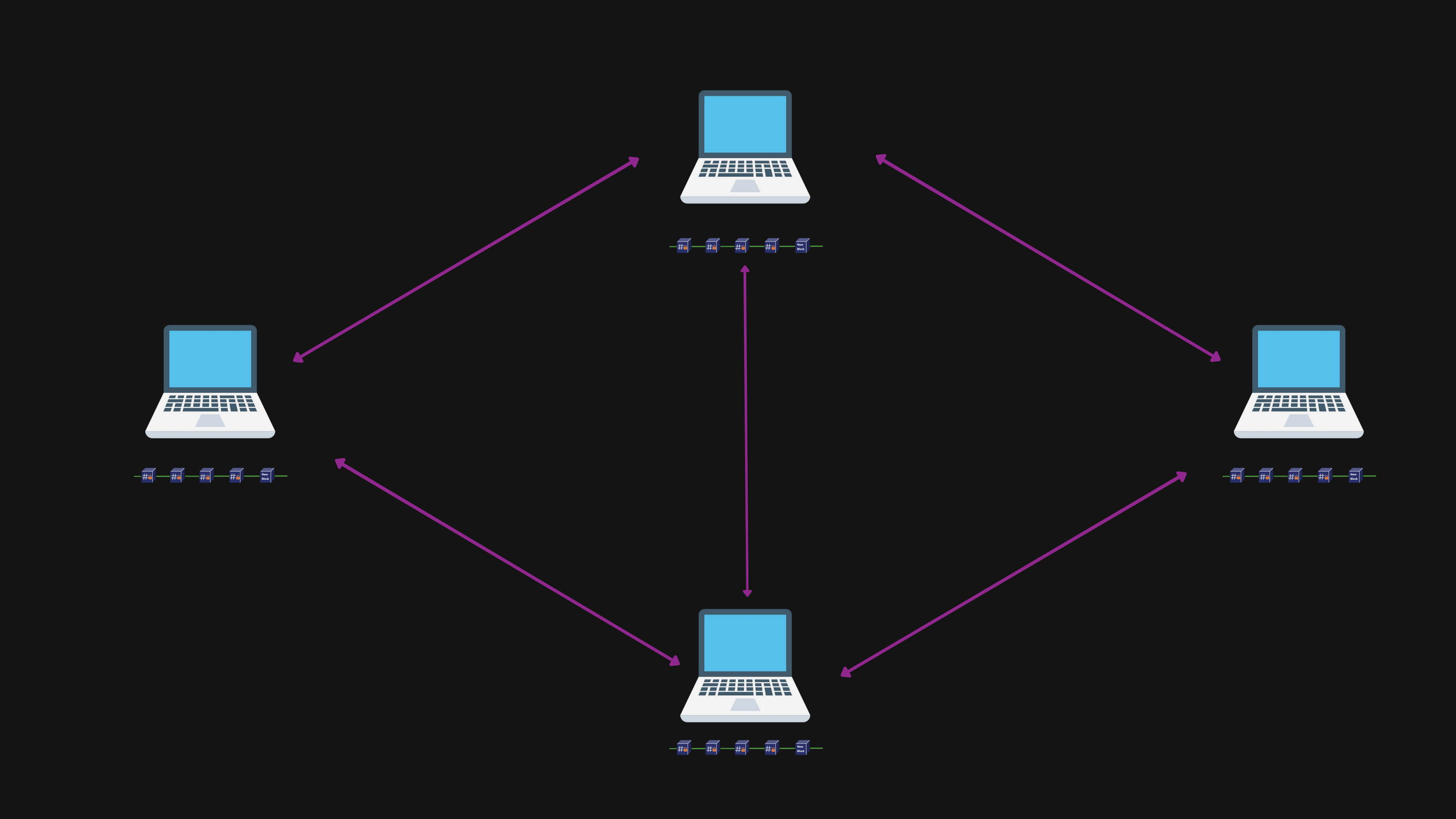


The Need for Blockchain



What is Blockchain

What is Blockchain


New Block
New Block
New Block
New Block

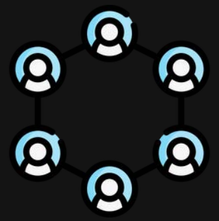
Why Blockchain

IMMUTABLE LEDGER

The immutability of blockchain ensures that once firmware update transactions are recorded, they remain unalterable, bolstering trust in the update process's integrity.

SMART CONTRACT ENFORCEMENT

Smart contracts enforce update rules, including time constraints and cryptographic verification, mitigating the risk of unauthorized updates or attacks.



DECENTRALIZED SECURITY

Distributed ledger nodes enhance system resilience; even if one is compromised, blockchain consensus safeguards the overall update process integrity.

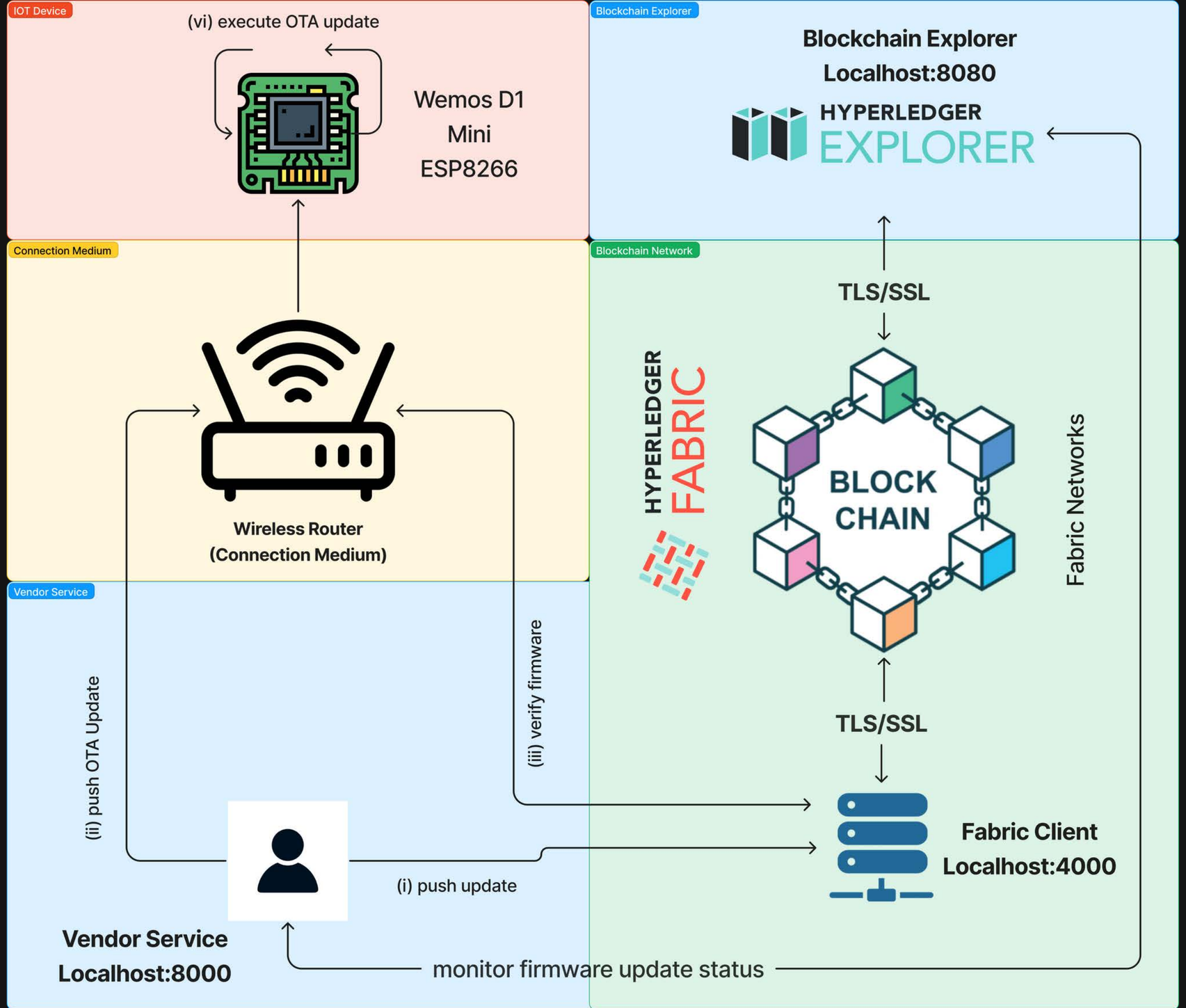
Implementation

Choosing A Blockchain Implementation

Ethereum

Hyperledger Fabric

Polkadot Substrate


IOT Device
(vi) execute OTA update
Wemos D1
Mini
ESP8266
Blockchain Explorer
Blockchain Explorer
Localhost:8080
HYPERLEDGER
EXPLORER
Connection Medium
Wireless Router
(Connection Medium)
Blockchain Network
TLS/SSL
HYPERLEDGER
FABRIC
BLOCK
CHAIN
Fabric Networks
TLS/SSL
Vendor Service
(ii) push OTA Update
(iii) verify firmware
(i) push update
Fabric Client
Localhost:4000
Vendor Service
Localhost:8000
monitor firmware update status

Restful API's for Smart Contract

PUSH()

Request Type: POST
Parameters: transaction attributes as JSON object
Response: transaction ID

VERIFY()

Request Type: POST
Parameters: transaction ID, firmware SHA1 hash
Response: verification results

QUERY()

Request Type: GET
Parameters: transaction ID
Response: verification status

Resilience Against Attacks

Denial-of-service Attack

```
Booting Sketch...
firmware v1.0

Update: v2.ino.bin
sleep disable
Chunk 1 size: 2048 Hash: 22c47838cb13932a3ac369f14e3532cf6a99b399
Chunk 2 size: 2048 Hash: eb2aacf95642ff895ded64ad4ca86ea6c3c7ec84
Chunk 3 size: 2048 Hash: 0e682492ab3a819805c7a3043cd6caa441d69de3
Chunk 4 size: 2048 Hash: 181652e107cd162d3356cfd1ce57b322a1f5c14b
Chunk 5 size: 2048 Hash: fa50f70248c8512a7a2a323b89694ef52229712a
...
Chunk 145 size: 2048 Hash: 01d041ca710e15c218736471187b08dbf714ebfd
Chunk 146 size: 144 Hash: 60688f5c953f2fd247fe31dda3c97bad14b3b569
final hash is 457de643c3113667f18660bf12c999db721a3fc4
Verifying with blockchain...
Hyperledger Client Token: eyJhbGciOiJIUzI1NiIsInR5cCI6I...O9itsGBM
{"fcn": "verify",
"args": ["ESP00001", "457de643c3113667f18660bf12c999db721a3fc4"]}
Failed to order the transaction.
Message: ERROR!!! transaction is expired.
Verification FAILED! OTA update aborted! Will REBOOT!

Booting Sketch...
firmware v1.0
```

Man In The Middle Attack

```
1  Booting Sketch...
2  firmware v1.0
3
4  Update: v2.ino.bin
5  sleep disable
6  Chunk 1 size: 2048 Hash: 22c47838cb13932a3ac369f14e3532cf6a99b399
7  Chunk 2 size: 2048 Hash: eb2aacf95642ff895ded64ad4ca86ea6c3c7ec84
8  Chunk 3 size: 2048 Hash: 0e682492ab3a819805c7a3043cd6caa441d69de3
9  Chunk 4 size: 2048 Hash: 181652e107cd162d3356cfd1ce57b322a1f5c14b
10 Chunk 5 size: 2048 Hash: fa50f70248c8512a7a2a323b89694ef52229712a
11 ...
12 Chunk 145 size: 2048 Hash: 01d041ca710e15c218736471187b08dbf714ebfd
13 Chunk 146 size: 144 Hash: 60688f5c953f2fd247fe31dda3c97bad14b3b569
14 final hash is 457de643c3113667f18660bf12c999db721a3fc4
15 Verifying with blockchain...
16 Hyperledger Client Token: eyJhbGciOiJIUzI1NiIsInR5cCI6I...O9itsGBM
17 {"fcn": "verify",
18 "args": ["ESP00001", "457de643c3113667f18660bf12c999db721a3fc4"]}
19 Failed to order the transaction.
20 Message: ERROR!!! transaction is expired.
21 Verification FAILED! OTA update aborted! Will REBOOT!
22
23 Booting Sketch...
24 firmware v1.0
```

Sources:

- Securing Over-The-Air IoT Firmware Updates using Blockchain
- A Highly Secure IoT Firmware Update Mechanism Using Blockchain
- Security considerations for OTA software updates for IoT gateway devices
- Unsecured AWS S3 Bucket Found Leaking Data of Over 30K Cannabis Dispensary Customers
- A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems

Do you have any questions?

Send it to me! I hope you learned something new.

SCAN ME