IoT - Secure Firmware Update

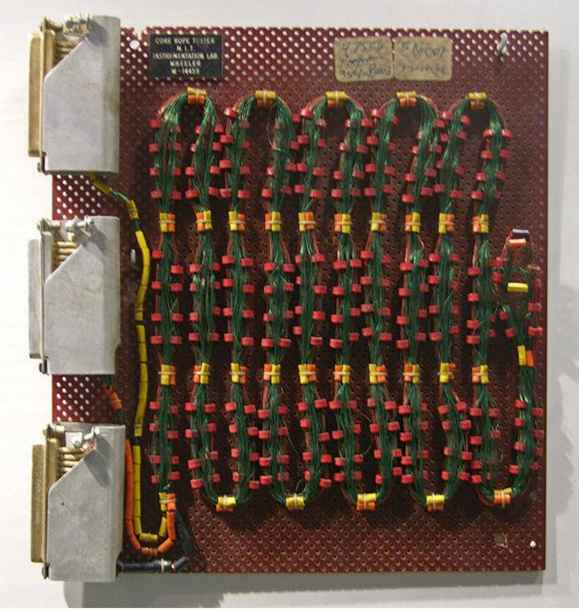
Kyle Haefner
August 2018

Firmware

- Software that provides low level control over a device’s hardware
- Stored in non-volatile memory
- For some devices constitutes:
  - Operating System
  - Network Stack
  - Application
  - Drivers

Firmware - Vintage

- Apollo Lunar Module Guidance Computer
  - ○ Rope Core Memory
  - ○ 1’s and 0’s *literally hardwired*
  - ○ 72KB foot^3!
  - ○ Updatability: umm no...



https://en.wikipedia.org/wiki/Core_rope_memory

Firmware - Today

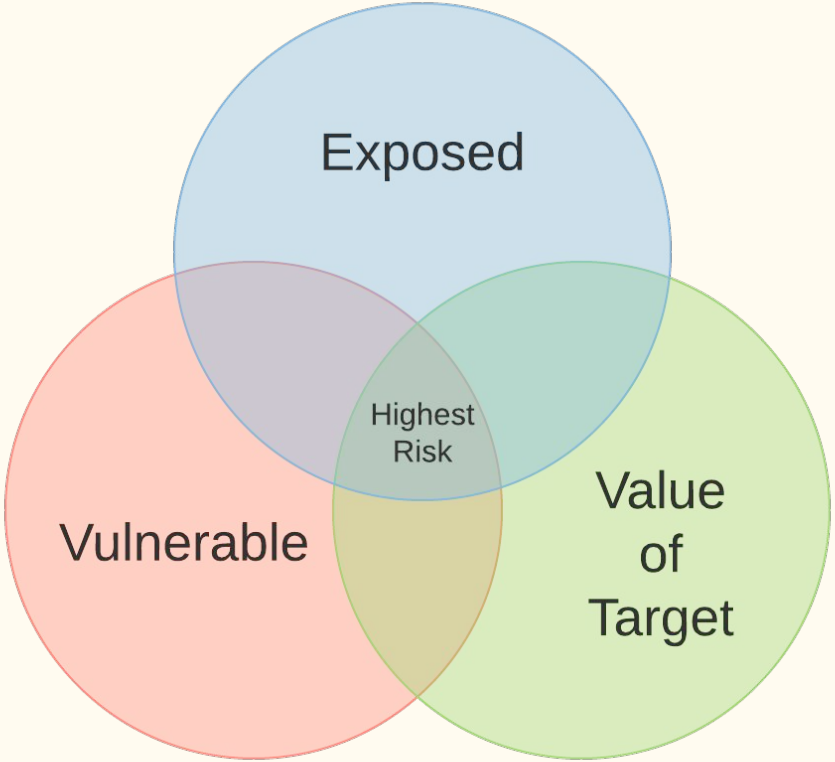
- Commonly stored in EEPROM or Flash
- Hundreds of Gigabytes and growing
- Relatively simple to write/rewrite
- In everything
- *Disaster waiting to happen*

“Nothing is certain but death, taxes and…

…Vulnerable Software”

--Benjamin Franklin (if he were alive today)

Firmware is unique, once compromised can be impossible to fix.



Requirements for Secure Update

- Confidentiality
  - Firmware image is encrypted - guards against reverse engineering
- Integrity
  - Hash of firmware to make sure it has not been altered
- Access/Availability
  - Digitally signed by manufacturer
  - Devices must be able to find and download firmware
    - This must scale to hundreds of millions of devices
  - Firmware should persist through
    - Mergers
    - Bankruptcies

Integrity
Availability
Information Security
Confidentiality

Proposal

Blockchain!

...a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively.

DECENTRALIZATION WILL CHANGE EVERY-THING.
SUCH AS?
DILBERT.COM
@SCOTTADAMSSAYS
WELL... FOR EXAMPLE, UM... THE BITCOIN AND THE ETHEREUM.
6-6-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel
DID YOU RECENTLY READ AN ARTICLE?
SOME OF IT.

http://dilbert.com/strip/2018-06-06

Blockchain: Confidentiality

- No need for need for trusted third parties.
  - Blockchain is the PKI.
  - Devices must ship trusting the manufacturer's blockchain public key
  - Used to encrypt firmware image
  - Used to encrypt communications channel for downloading firmware

Integrity
Availability
Information Security
Confidentiality

Blockchain: Integrity

- Each firmware update is hashed and signed in the blockchain
- Blockchain stores
  - Hash of each firmware version stored in blocks in blockchain.
  - URL for each firmware version

Integrity
Availability
Information Security
Confidentiality

Blockchain: Access/Availability

- Blockchain private key can sign firmware
- All transactions can be certified to a manufacturer
- High availability
- Access to firmware can outlive any single company

Integrity
Availability
Information Security
Confidentiality

Advantages of Blockchain for Firmware

- A distributed ledger can provide transparency for each firmware lifecycle
- Firmware can be cryptographically transferred
- No single entity owns the blockchain
- No single entity needs to be trusted on the blockchain.

Proposal: OCF Firmware Blockchain Community

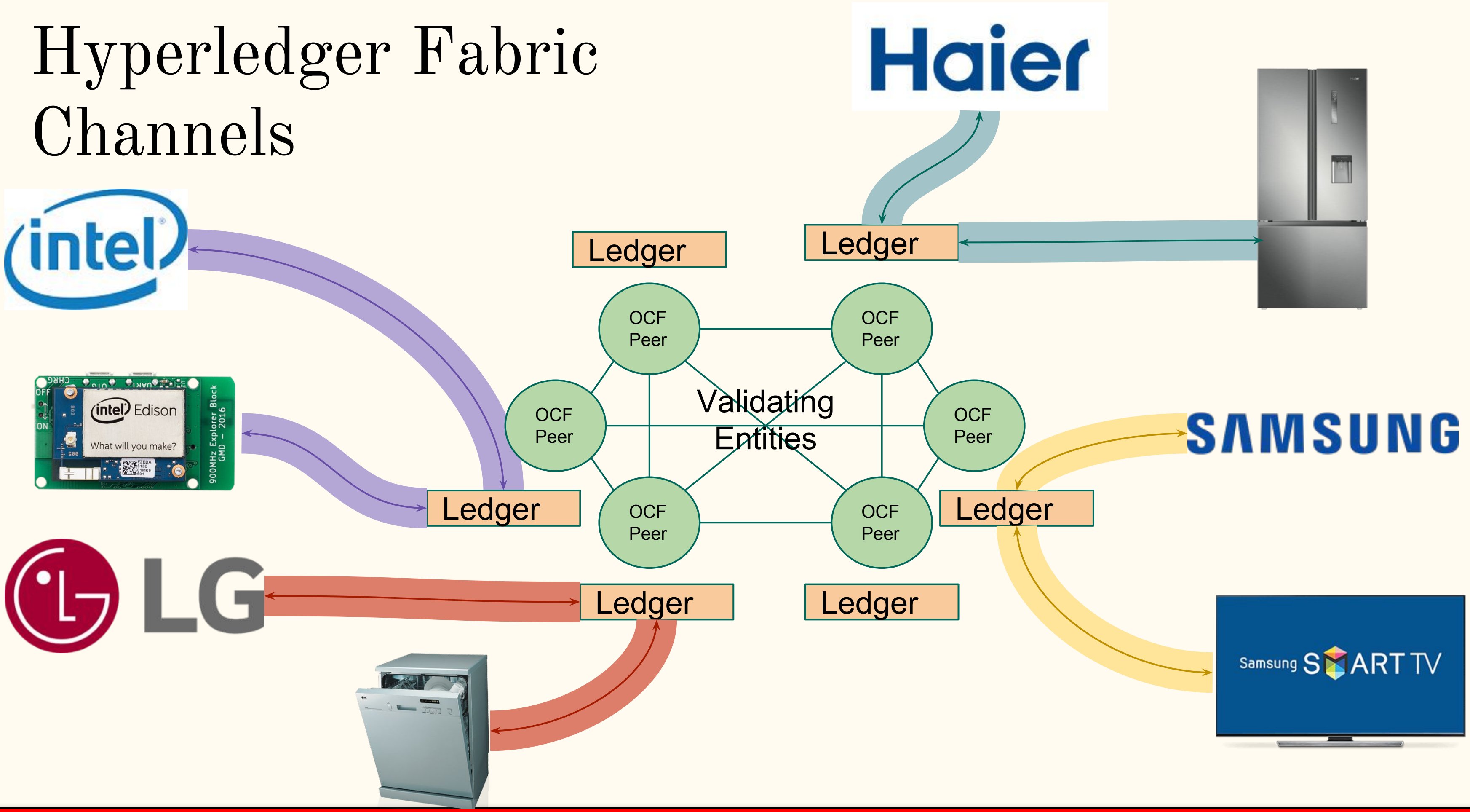
- Based on a *permissioned* blockchain network
- Members of OCF maintain one or more validation nodes in the blockchain firmware network
- Any node in the community can respond to firmware verification requests
- Firmware network is responsible for:
  - Performing consensus algorithm
  - Maintains entire ledger of firmware transactions.
  - Executing smart contracts
- Firmware is stored outside of blockchain
  - Traditional Server -- Client Model
  - P2P network

Prototype Ledger

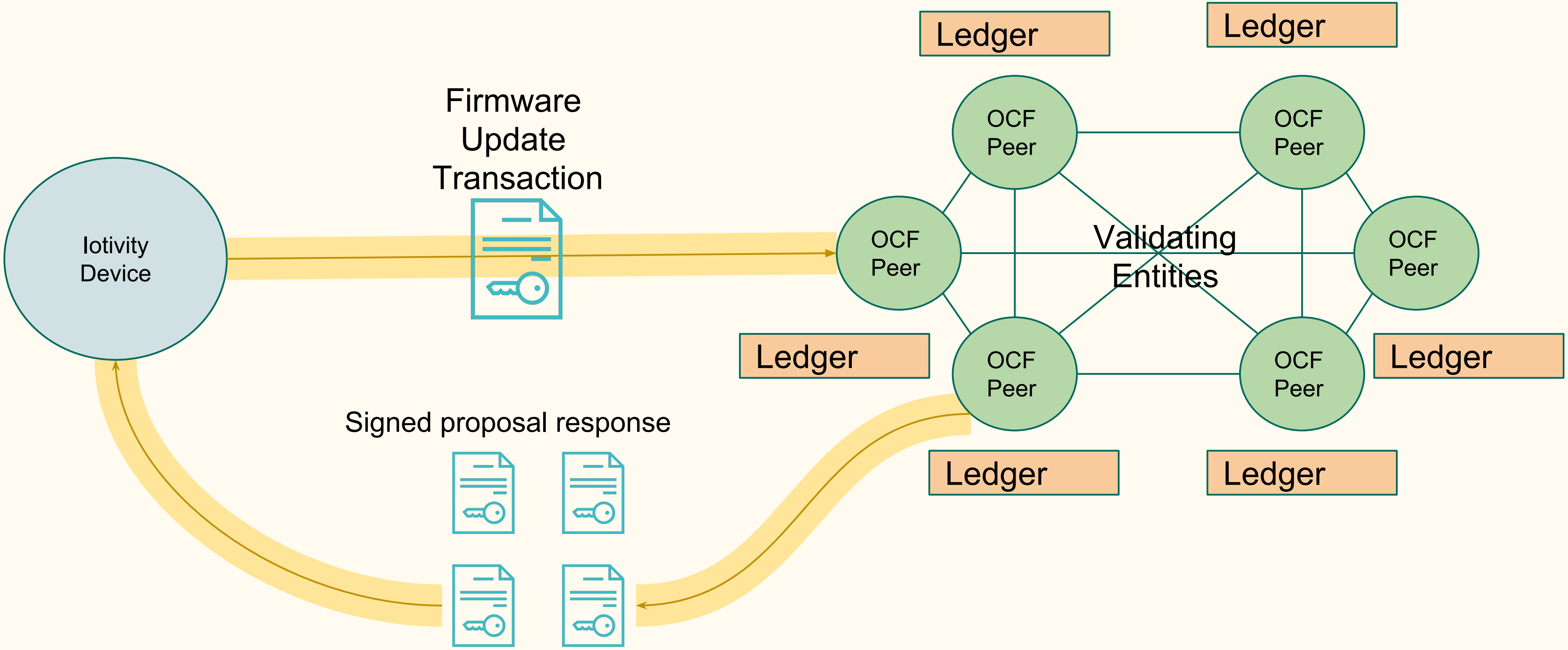
HYPERLEDGER

- Blockchain built using the Hyperledger Fabric framework
  - https://www.hyperledger.org/
  - Linux Foundation
  - Created for the Enterprise
  - Open Source
  - Permissioned - only certain authenticated entities can update ledger
- Channels
  - Overlay on blockchain.
  - Allows for segmenting blockchain network and transactions
  - Only authorized entities can communicate on a channel
  - Each OCF Member gets one or more channels

Hyperledger Fabric Channels



Firmware Update Request

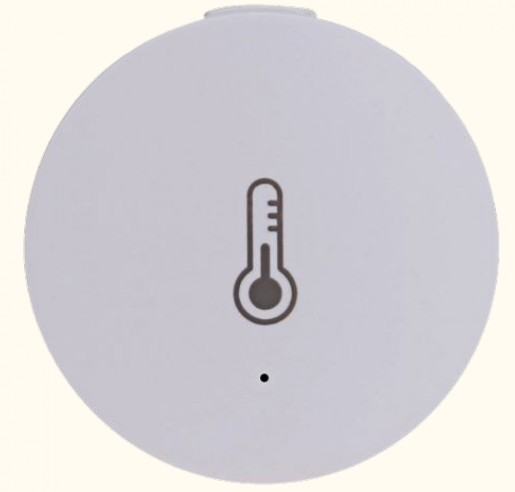


Unconstrained Devices

- Continuously connected
- Enough RAM and storage to handle firmware downloads
- CPU capable of asymmetric cryptographic functions
- Can act as a client on the blockchain
- Can download, decrypt and store firmware for constrained devices

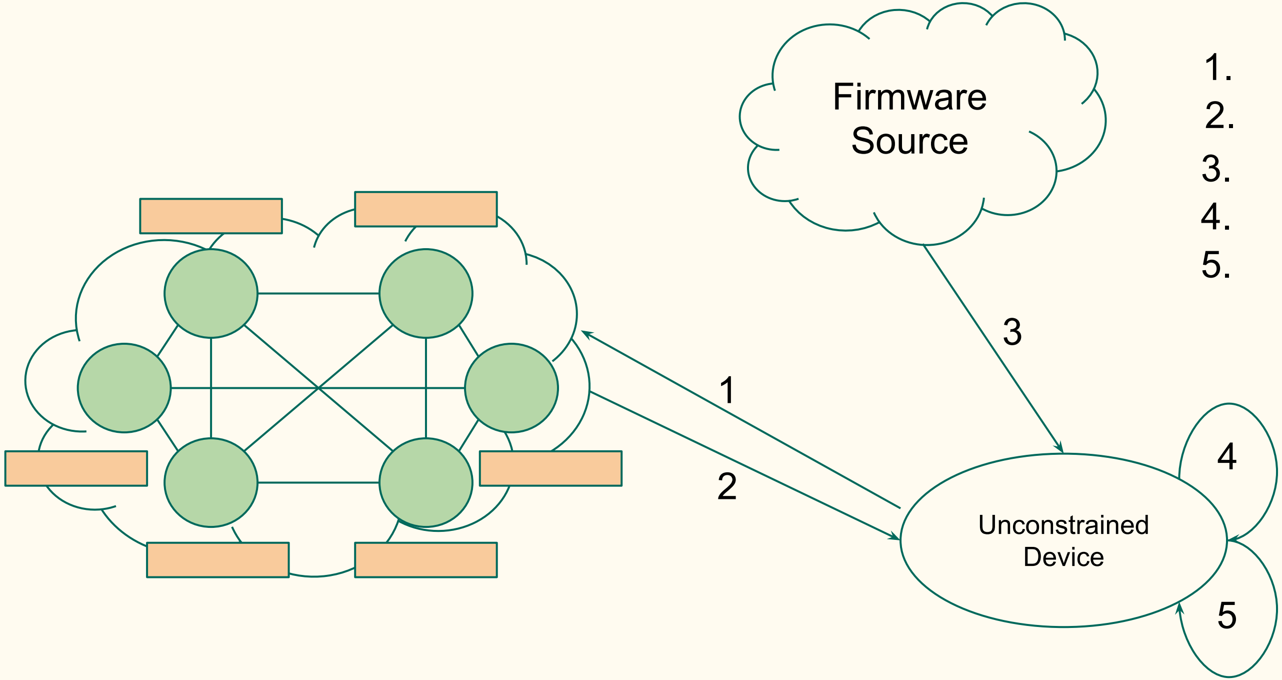
Constrained Devices

- May not have continuous connection
- Battery operated
- Low RAM/Storage
- CPU designed for power efficiency
- Does not interact directly with blockchain



Wireless Sensor

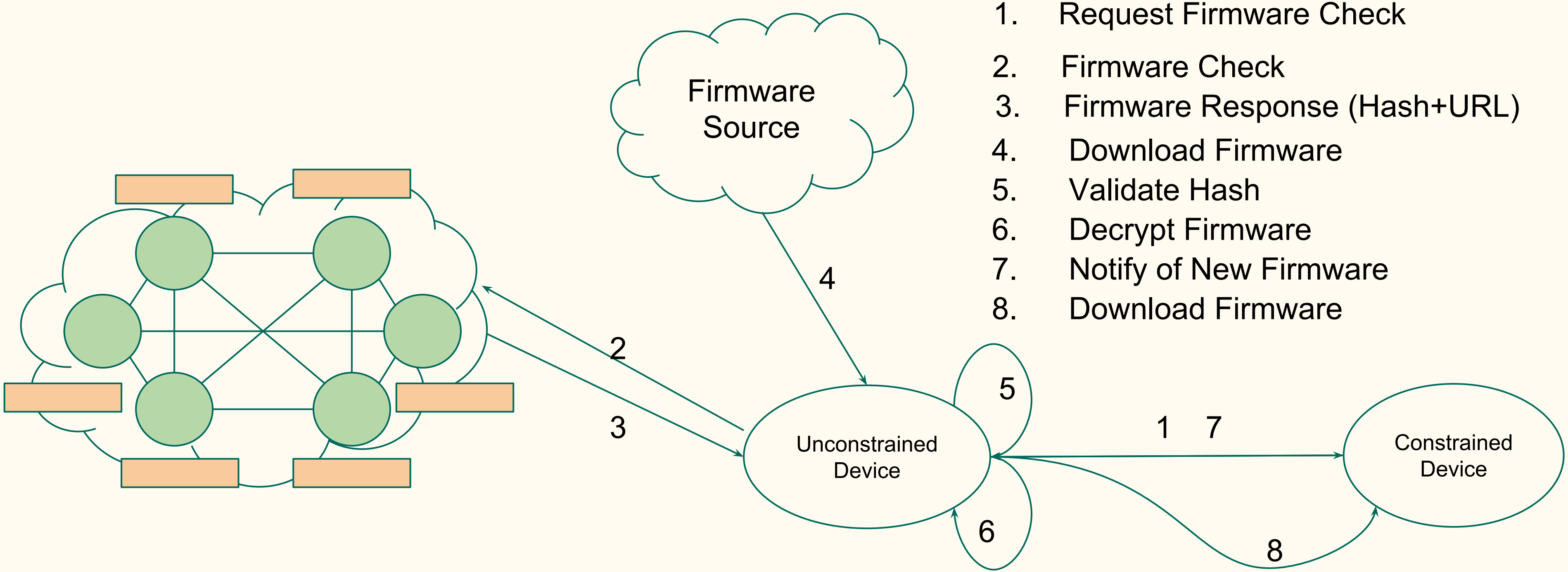
Unconstrained Devices



1. Firmware Check
2. Firmware Response (Hash+URL)
3. Download Firmware
4. Validate Hash
5. Decrypt Firmware

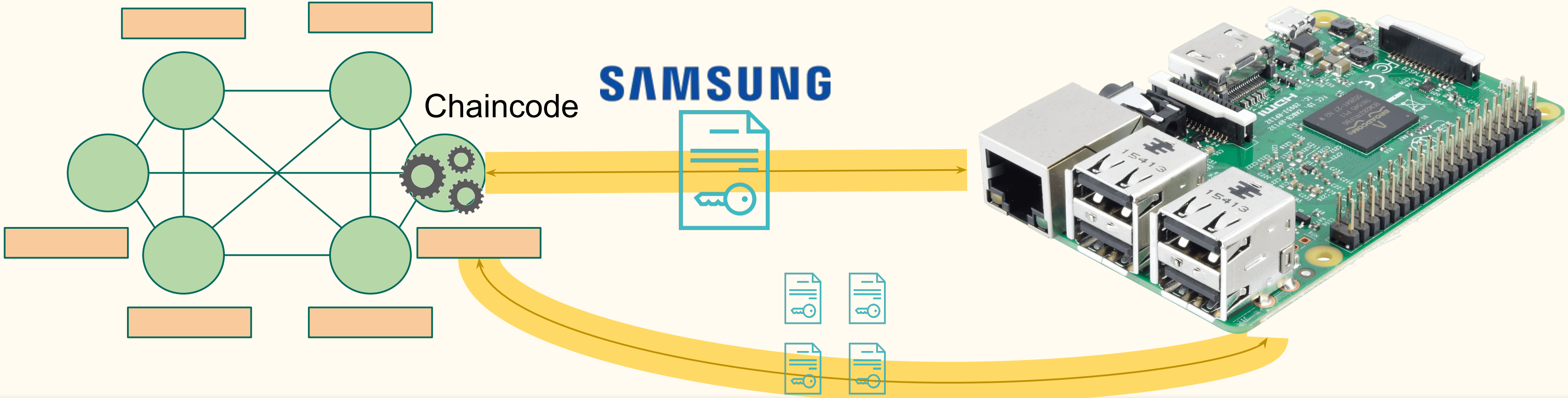
Constrained Devices

1. Request Firmware Check
2. Firmware Check
3. Firmware Response (Hash+URL)
4. Download Firmware
5. Validate Hash
6. Decrypt Firmware
7. Notify of New Firmware
8. Download Firmware



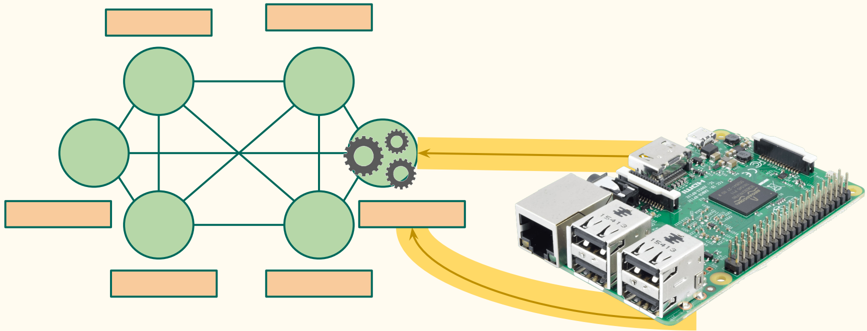
Prototype: Unconstrained Devices

- Raspberry Pi prototype unconstrained device
  - Authorized to transact on a specific channel (eg. Samsung)
  - Uses chaincode applications/smart contract to interact with that channel
  - Advertises firmware capability to other IoTivity Devices



Prototype: Constrained Devices

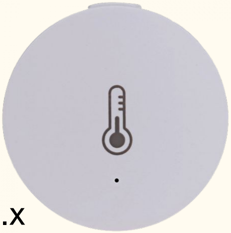
- Talk to an unconstrained device on the network
- Communication and trust established at
  - On-boarding and
  - Exchange of symmetric keys



RETRIEVE /oic/res?oic.r.firmware.version=1.2

Group Symmetric Key

RETRIEVE Response /oic/res?oic.r.firmware.url=x.x.x.x



Wireless Sensor

Links

1. Open Connect Foundation
   1. https://www.oregoncf.org/
2. Iotivity
   1. https://iotivity.org/
3. Hyperledger Fabric
   1. https://www.hyperledger.org/projects/fabric

Questions

Thank You.

Monday April 16, 2018 The Losing Team
★★★★☆
I'D LIKE TO WORK ON OUR BLOCKCHAIN PROJECT TO KEEP MY SKILLS UPDATED.
DILBERT.COM @SCOTTADAMSSAYS
I NEED YOU TO BE A TEAM PLAYER AND MAINTAIN OUR LEGACY SYSTEMS UNTIL YOUR TECHNICAL SKILLS BECOME OBSOLETE.
4-16-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel
WHAT KIND OF TEAM IS THAT?
YOU'LL BE ON THE LOSING TEAM.

http://blog.dilbert.com/wp-content/uploads/2018/05/Blockchain-skills.png