Next G Connect (NGC)

and

IoT Blockchain Solution (IBS)

August 5, 2019

Intro

- NGC has developed a unique cybersecurity solution to ensure the security and integrity of Internet of Things (IoT) devices
- The NGC solution is designed to solve IoT security concerns and prevent malware from infecting IoT devices
- The NGC solution utilizes blockchain smart contract technology to deliver and manage software
- The NGC solution is software that can be integrated into current and future IoT devices without requiring proprietary hardware or software
- The NGC solution is called IoT Blockchain Solution (IBS)

Overview

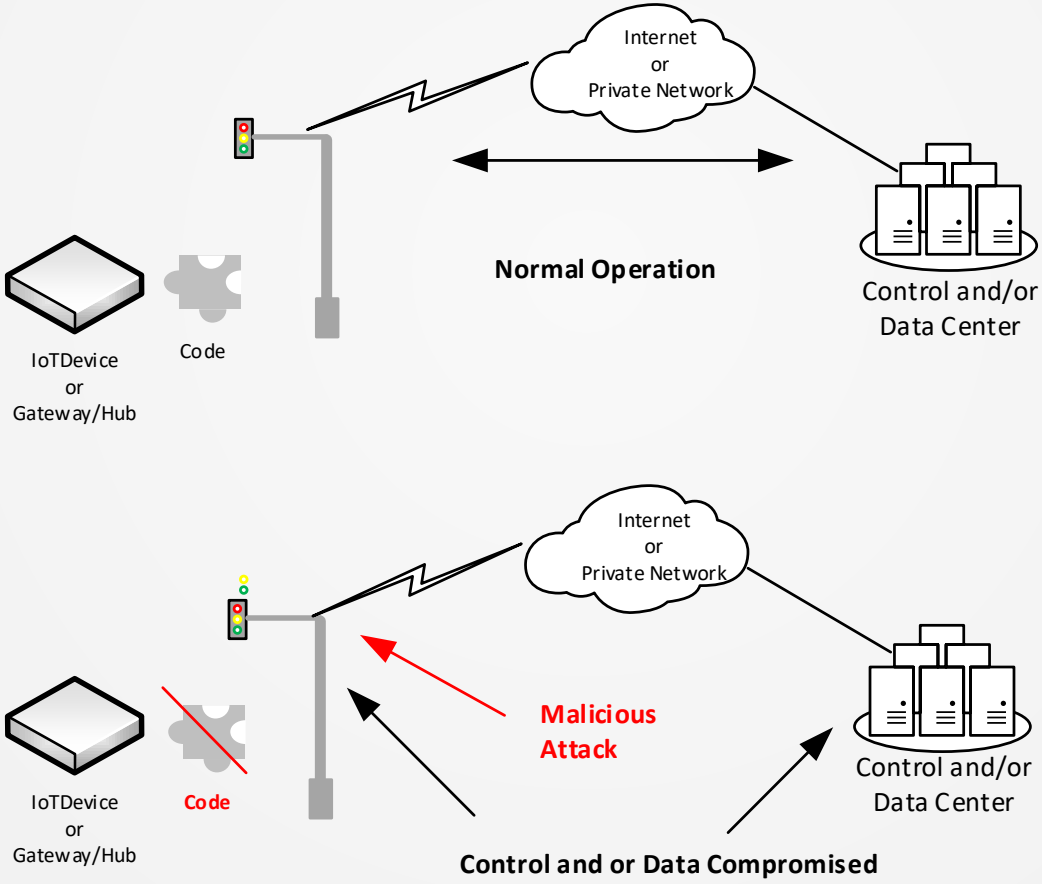
- IBS utilizes blockchain smart contracts technology
- IBS is a novel **cybersecurity** solution and **not** a cybercurrency
- IBS utilizes the security of blockchain to protect IoT devices:
- With IBS a smart contract is used for IoT devices either to deliver code, configure the device or perform software or configuration updates
- IBS utilizes the immutability of the blockchain to protect IoT devices

What is the Problem IBS is solving

- Security both software and hardware are a major concern when deploying IoT devices
- IoT device platforms, their operating systems, and the data they communicate all have to be guarded against malicious attacks
- Malicious attacks can come in the form of data hacking/manipulation, device tampering, and network overloading
- Simple IoT devices with a basic operating system utilizing minimalized hardware will not be able to support a complex security model

Problem

- The advent of massive IoT deployment greatly increase the threat surface for hackers
- Many of these devices are out in the open and potentially could be tampered with



NGC IBS Solution

- NGC's IBS solution is designed to address the security concerns with IoT devices proactively

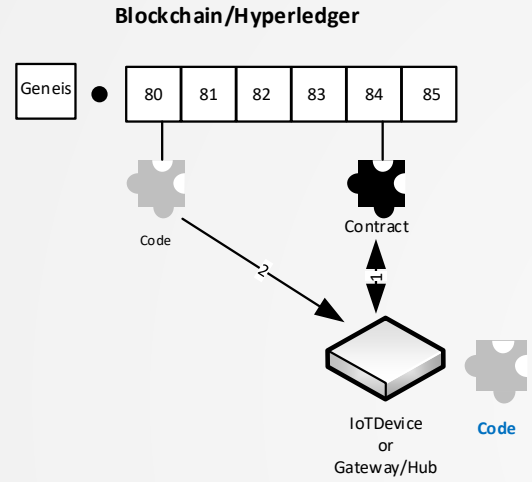
1. IBS uses smart contracts to proactively detect/prevent malicious devices through our security token
2. Stores pieces of code in the blockchain which can be invoked by IoT devices or a smart contract within the blockchain
3. Addresses provisioning of the device where the device gets its provisioning script from the blockchain

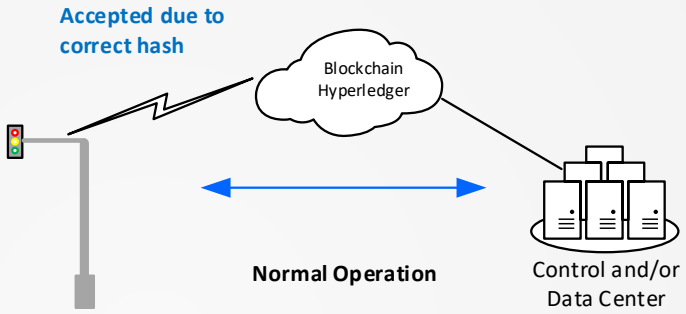
NGC IBS Solution

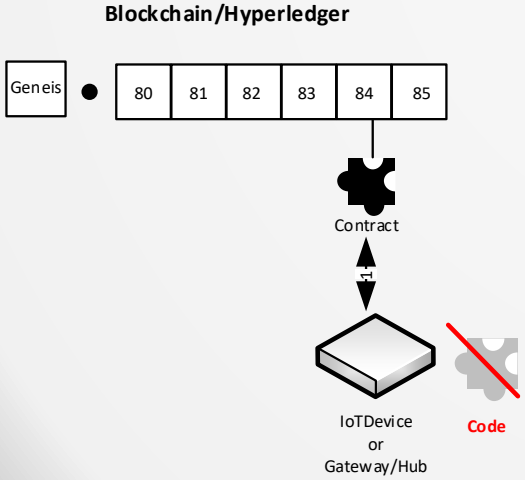
- With IBS the software code and device configurations reside on the blockchain and can not be altered
- With IBS there is no single point of attack since the blockchain is a distributed ledger
- Protocols such as Interplanetary File System (IPFS) will be used to store code/scripts that are too large to be stored in the blockchain. However a hash of the file is stored in the blockchain to be used in verifying authenticity

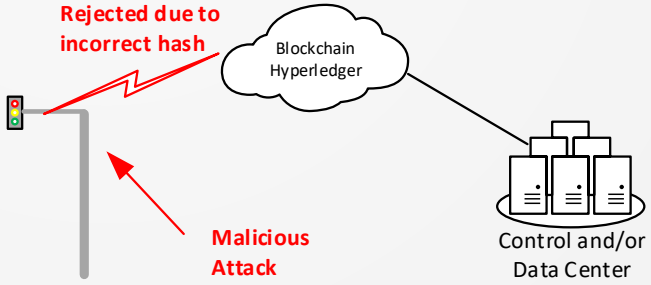
NGC IBS Solution

- With IBS the software code and device configurations reside on the blockchain and can not be altered









NGC IBS

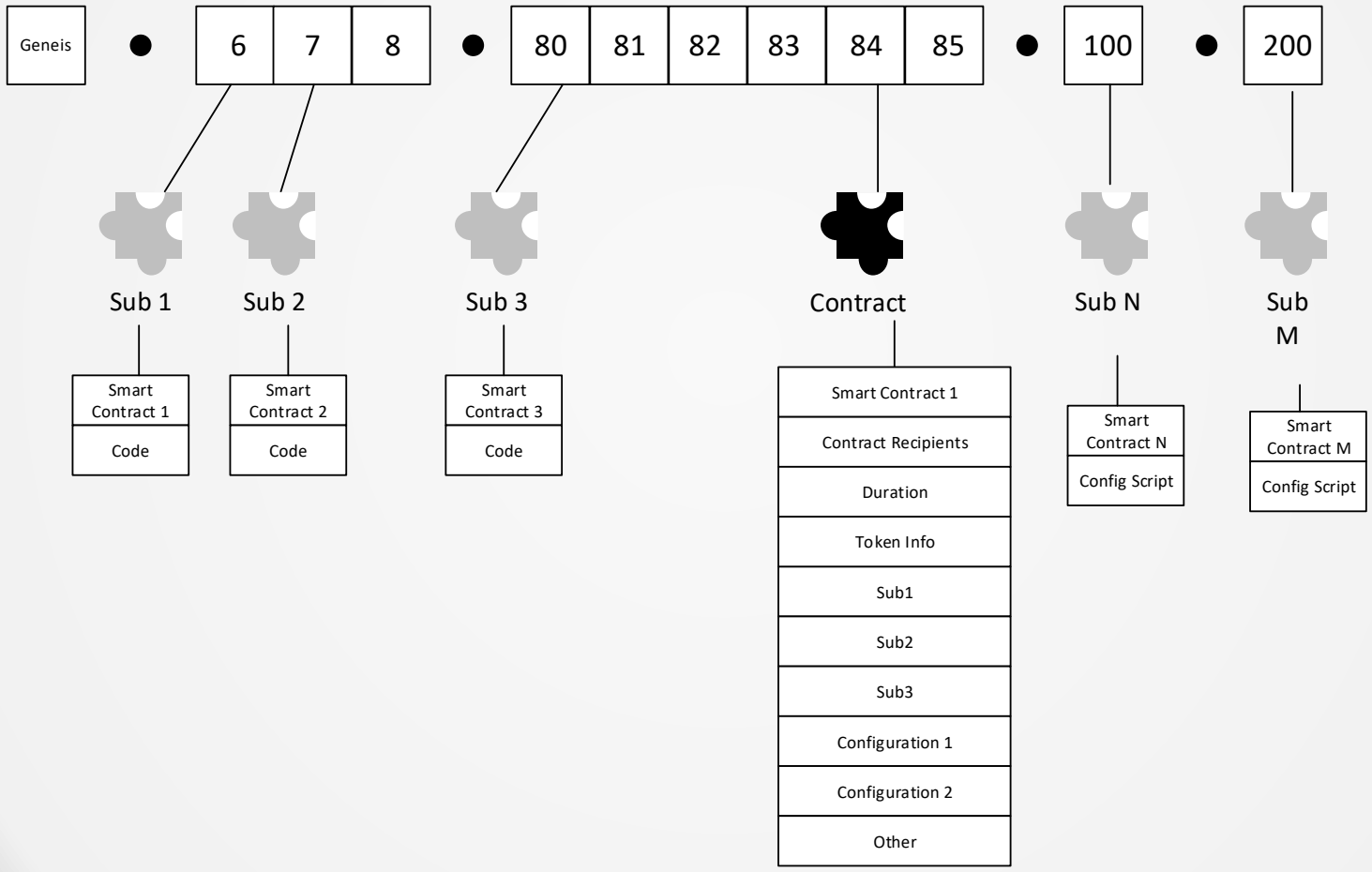
- The NGC IBS solution uses smart contracts to deliver software code and configuration scripts to the IoT device

- The smart contact solution with IBS is immutable because it has three primary attributes

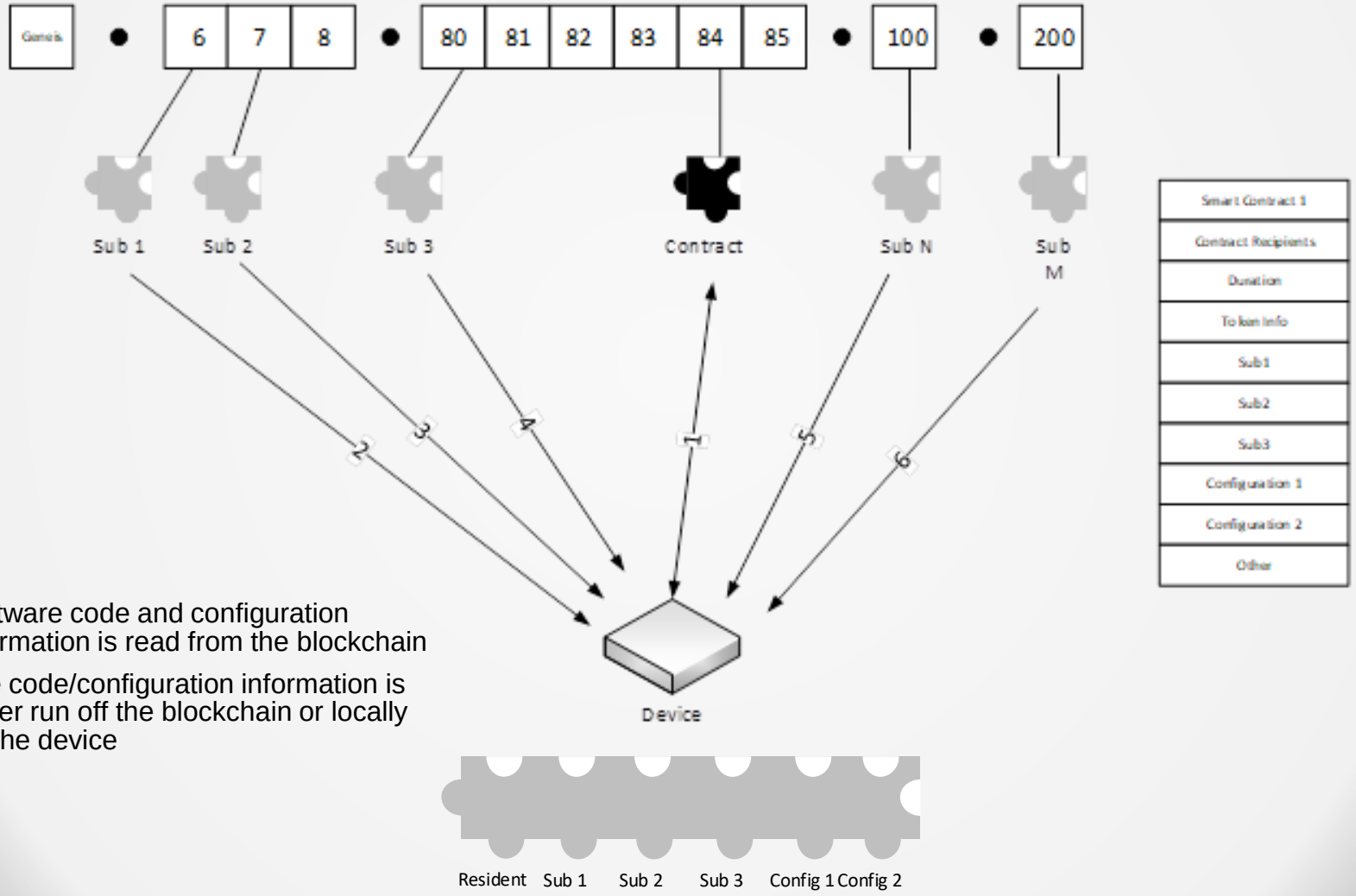
    1. Deterministic. if it gives the same output to a given input every single time
    2. Terminable. Means it does not operate forever
    3. Isolated. – can not be changed

- The immutability of the smart contract used by IBS ensures that the IoT device is running the correct code, and operates as desired

IoT Device Software and Configuration components located on blockchain



Device reads contract and obtains the software and configuration from the blockchain



- Software code and configuration information is read from the blockchain
- The code/configuration information is either run off the blockchain or locally on the device

NGC IBS Solution

- NGC's solution, IoT Blockchain Solution (IBS), prevents malware and other security breaches.

- The IBS solution using smart contracts will:
  - Delivery the IoT device Code
  - Deliver the IoT device configuration
  - Deliver updates to the IoT device software and configuration
  - Protect IoT device integrity from malware
  - Ensure code that IoT devices are using has not been tampered with

- IBS utilizes a zero trust environment providing an additional layer of security by:
  - Verifying the code authenticity on the device for each transaction
  - Securing the communication channel between the device and the blockchain
  - Preventing Man in the Middle (MITM) attacks and Denial of Service (DOS)

- The IBS Solution is portable to any blockchain implementation that accommodates smart contracts including hyperledger.

Who we are:

NGC is a consulting team of highly skilled and experienced professionals. Our background is in wireless communications for both the commercial and public safety sectors. The team has led deployment and operations spanning decades in the wireless technology. We have designed software and hardware for both network infrastructure and edge devices from concept to POC/FOA.

Our current areas of focus include 4G/5G. IoT and security.

The team has collectively been granted over 160 patents in the wireless communication space during their careers. We have also written multiple books used extensively in the industry on wireless technology and published by McGraw-Hill.

Feel free to utilize this information in any presentation or article with the simple request you reference its origin.

If you see something that should be added, changed or simply want to talk about your potential needs please contact us at info@nextgconnect.com or call us at 1.845.987.1787.

Thank you