Blockchain Convergence with 5G/LTE and IoT

Abstract:

The convergence of blockchain technology with Fifth Generation Wireless (5G), Long Term Evolution (LTE), Internet of Things (IoT) and cloud services fosters in a host of new services that were not possible before. The proliferation of devices in a distributed architecture has many challenges including ensuring the device configuration management and cybersecurity. This paper discusses how smart contracts can be used for configure, operate and protect IoT devices.

Clint Smith, P.E.
csmith@nextgconnect.com

The convergence of blockchain technology with Fifth Generation Wireless (5G), Long Term Evolution (LTE), Internet of Things (IoT) and cloud services fosters in a host of new services that were not possible before. Distributed architectures for providing services in a communication ecosystem is common to 5G, LTE, IoT, cloud services and blockchain. The convergence of these unique technologies facilitates a neutral host environment and network slicing for service delivery that is extended to the industrial, utility, enterprise and smart home environments.

Presently there is a large focus on blockchain solutions, 5G/LTE solutions, IoT solutions and cloud solutions. Some cross pollination between these four pillars are emerging. However, these four seemingly diverse technologies when brought together will enable the next communication system of the future and with added location awareness will foster new services and concepts which are not even imaginable right now.

5G is being deployed as both Standalone (SA) and non standalone (NSA) with LTE as the access method for IoT devices. The virtualization of the wireless network using Network Function Virtualization (NFV) with Software Defined Networks (SDN) is enabling a low latency flat distributed network. The use of Containers for VNFs is being used in a virtual environment to quickly and efficiently scale services enabling logical network slices across multiple domains and technologies.

5G and LTE utilize narrowband, Cat-NB1 (NB) or wideband Cat-M1 (CAT-M) devices as the primary access technologies supporting IoT devices. However, there are other wireless access techniques and protocols that support IoT devices including WiFi and ZigBee.

IoT is often considered the next great industrial revolution and is pervasive with more and more devices being deployed for a vast amount of applications. IoT devices and their supported applications cover a huge range of industries and use cases that scale from a single constrained device to massive cross-platform deployments of embedded technologies and cloud systems connecting in real-time.

IoT devices can be currently found in consumer applications, smart homes, enterprise, infrastructure management, industrial applications, military, agriculture, energy management, environmental monitoring, medical, transportation, food services, insurance, retail, city infrastructure, banking as well as in oil, gas and mining.

Although each of the before mentioned industries has unique IoT applications, the common theme is sensors and devices connected via machine-to-machine, or machine-to-infrastructure to deliver the use case, monitor assets, collect data, analyze processes, and improve efficiency.

The need to have low latency for device to device communication is becoming essential for IoT devices as well as smart vehicles and others. 5G access for IoT devices is still being defined with LTE (4G) having solutions which continue to evolve. Smart vehicles are currently using DSCR also known as 802.11p as well as LTE/5G to facilitate low latency device to device communication.

However, tying the diverse IoT ecosystem together which includes numerous legacy and emerging communication protocols that allow devices and servers to talk to each other in new and more interconnected ways is a daunting task. At the same time, dozens of alliances and coalitions are forming in hopes of unifying the fractured and organic IoT landscape. However, the IoT ecosystem has created artificial barriers either by design or because of the legacy platforms themselves.

IoT devices as part of the Industrial IoT 4 (IIoT) are utilizing wireless as the connectivity method as compared to wired connections. IoT devices use both licensed and unlicensed spectrum for their wireless connectivity. 5G/LTE can use both licensed and unlicensed spectrum. The use of 5G as the wireless connectivity method fosters in a vast array of enhancements from capability, installation ease, and future proofing.

Blockchain and Hyperledger, as its name implies is a collection of blocks. Blockchain while initially known for cybercurrency provides many other key factors. Blockchains are based on a distributed ledger and smart contracts. A distributed ledger is a shared history or record of all previous actions within the blockchain that is immutable due to its cryptographic security. Blockchains also utilize smart contracts which are used to provide information, usually a contract, where all parties associated with the contract interact and record their particular transactions. Smart contracts are also referred to as a transaction-based state. Smart contracts can be proof of work (PoW), proof of stake (PoS), utilize container technology.

However smart contracts can also be used to provide software, configuration, scripts, authentication and other important features used in machine to machine communication.

Figure 1 is a brief illustration of an IoT device using a 5G/LTE network to connect to a data center or cloud service. In Figure 1 the IoT device uses a NB-IoT modem. The NB-IoT modem uses a 5G/LTE wireless network for connectivity to the internet or private network. The IoT device is then able to send and receive telemetry from the control or data center.

However, security and especially cybersecurity have and continues to be a major concern not only in all aspects of telecommunications but of unique concern for IoT. The threat of a cybersecurity attack on IoT devices continues to be a serious concern for governments, industry and consumers. The current method of detecting a cybersecurity attack is to utilize monitoring for post intrusion detection as illustrated in Figure 1.

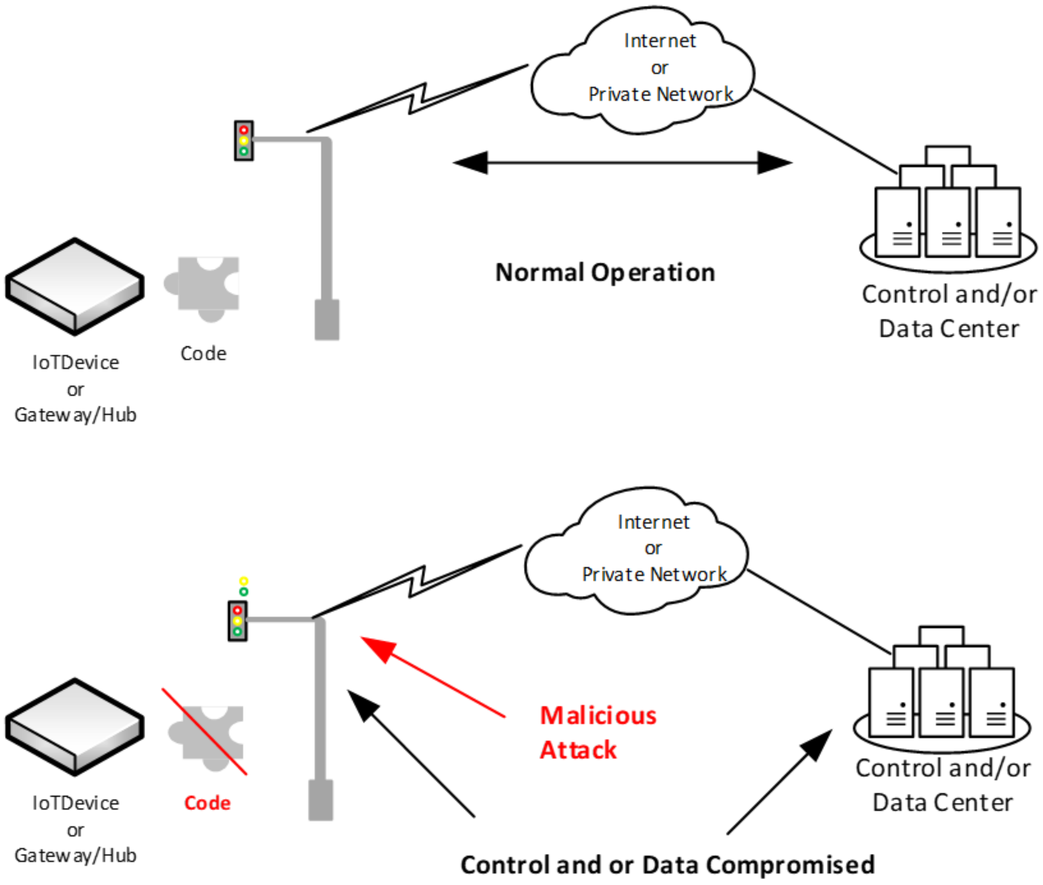

Figure 1: IoT Malicious Attack

In Figure 1 the IoT device code is compromised leading to upstream contamination. The current detection methods commonly used are post detection using pattern detection methods which may or may not prevent damage from the intrusion.

However, a more robust method is needed involving a proactive method whereby the cybersecurity breach and or intrusion attempt is stopped from the onset. Blockchain technology utilizing smart contracts can be used to robustly secure IoT devices. Smart contract is a piece of software that resides on the blockchain to enforce a contract. The use of blockchain smart contract technology can involve both wired and wireless technologies that communicate with either a private, public or a consortium blockchain.

Smart contracts can also be used to deliver or run software and or configuration files for IoT devices. Because smart contracts in a blockchain are immutable they can be used for a more effective way of delivering and verifying contracts which can also include the software code and or configuration of an IoT device. Smart contracts can also be used to provide automated configuration changes where the network is dynamically changed in near real time meeting particular service, performance or contract requirements.

With 5G and LTE, smart contracts can also be used to facilitate dynamic roaming or network selection either between operators, between assets or a particular radio spectrum that is allowed to be used. This can also be used by subscribers to determine their network of choice by utilizing smart contracts to select which operator to use and provide a method of payment or authentication for payment enabling their use of the network without having to utilize a third-party clearing organization.

Smart contracts therefore can be used to manage devices whether they are IoT devices, small cells, or macro cells. Figure 2 is a depiction of how a smart contract, associated with block 84, references other smart contracts for delivery of the software, configuration scripts or any other function. The smart contract can also be updated referencing other blocks to facilitate code updates, bug fixes, configuration changes and other items.

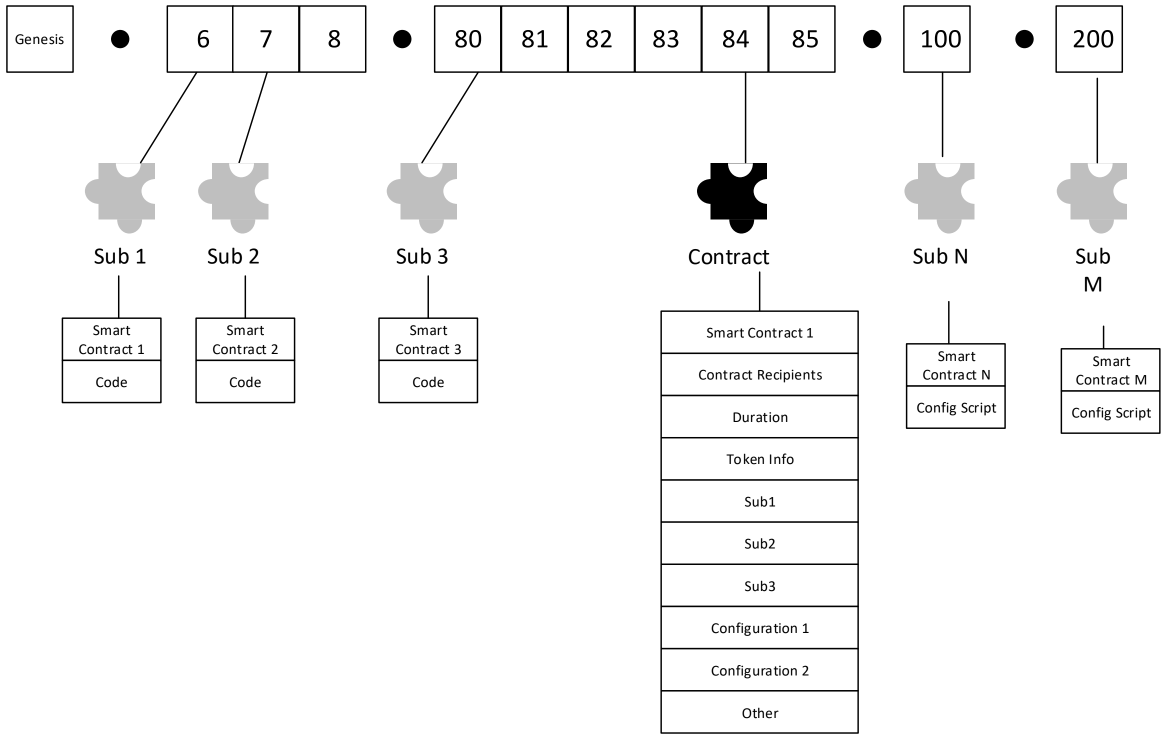

Figure 2: Smart Contact Blocks

In Figure 3 the device uses the master smart contract in block 84 and then assembles its required configuration and software from the various other blocks, smart contracts, as instructed in the master smart contract.

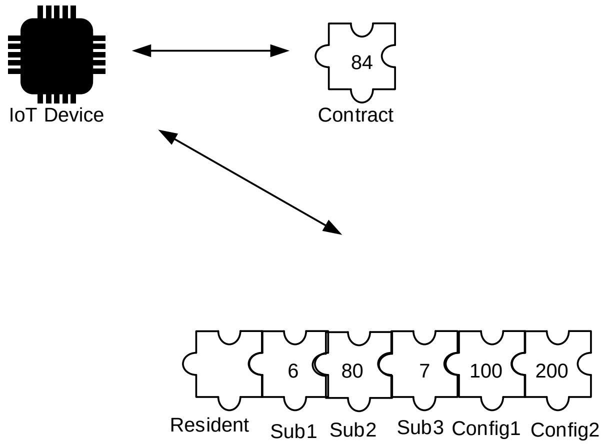

Figure 3: IoT Device Configuration and Software using Smart Contracts

The proliferation of IoT devices has fostered the big data phenomena where the mining of mega data is being promoted as essential for any business. However, having all the data available for third parties is not necessarily a good thing.

Any IoT enabled device, regardless of its function, is meant to collect, send and or receive telemetry. It is essential from the onset, that it is understood by all relevant parties involved what is the telemetry, data, that the IoT device will collect, send and receive. In particular what needs to be understood is how the device manufacturer plans to protect the IoT device and its data from being compromised and or how it is going to be used. The voracious volume of data that these devices generate can lead to cyber criminals stealing it and hold it hostage for ransom or use it to run subsequent schemes, such as identity theft.

However, relying on the manufacturer to provide the protection since they are potentially collecting and using the data for their own purposes has many reservations and is not practical from a security perspective. It is not practical due to the company and or manufacturers desire to monetize metadata and the low cost of the IoT devices which makes following more stringent security tampering requirements not cost effective because the price can easily make the IoT devices unattractive.

The other issue about security being embedded on the devices is manufacturing copycats which have spread in many sections of the electronics industry.   Stenciling and other markings make the device appear it is legitimate however it can be a rogue device that has other purposes.

Smart contracts however can also be used to provide a unique level of security preventing unwanted and unintended actors from disrupting those devices and their intended functions. Specifically, smart contract technology can also be used to robustly secure IoT devices due to its immutability.

Figure 4 is similar that shown in Figure 1 with the inclusion of a blockchain using smart contracts. In the depiction shown in Figure 4 the IoT device is using a smart contract which prevents the intrusion in a proactive method.

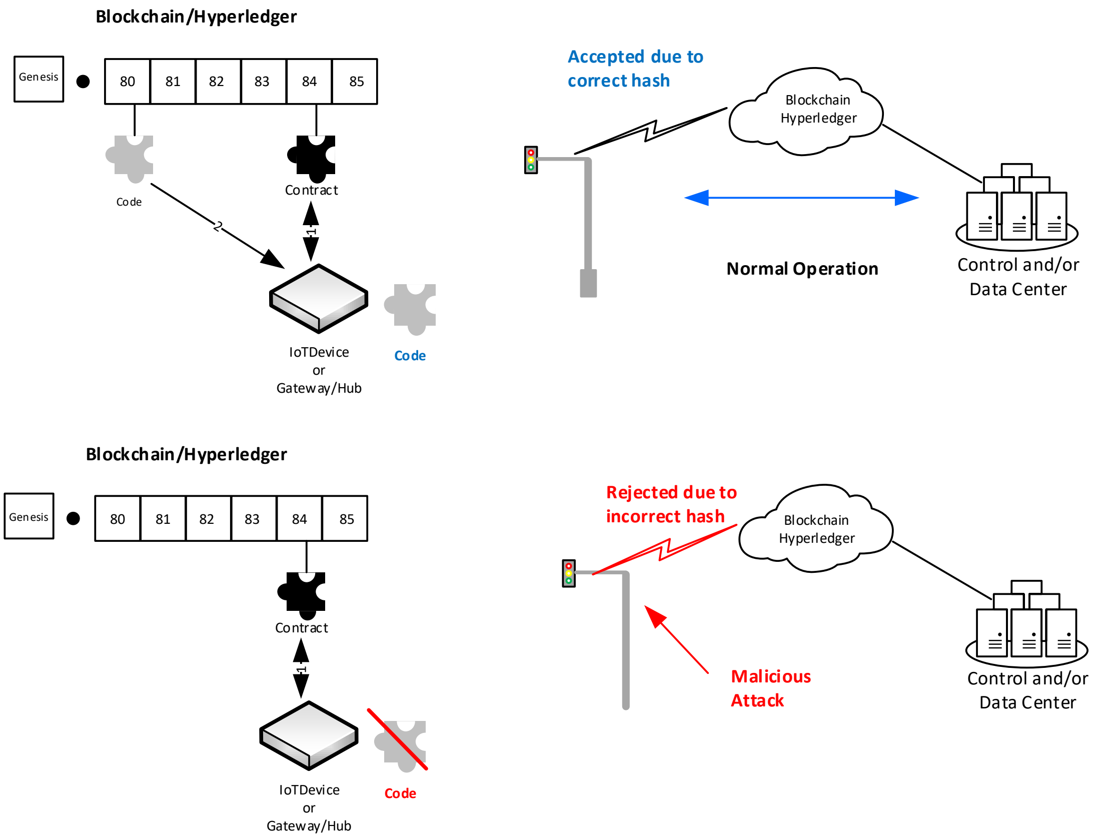

Figure 4: IoT devices using Smart Contracts.

In conclusion 5G/LTE and IoT devices leveraging blockchain coupled with cloud services provides a wholistic ecosystem that enables low latency applications in a secure manner.

I trust that you found this article useful.

Clint Smith, P.E.
Next G Connect
CTO
csmith@nextgconnect.com

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.