Next G Connect (NGC)

Blockchain Overview

August 1, 2019

Blockchain

- Blockchain is essentially a decentralized and distributed ledger that is used for recording transactions.

- Blockchain is primarily associated with cybercurrency however this powerful technology that has many other applications (i.e. IBS).

- There are several types of blockchains, however all of them are based on recording a transaction in a block and the block can not be changed once written.

- Blockchain therefore is a collection of blocks and each block is a record of a transaction that can be monetary, contract, or something else.

- Blockchain's distributed ledger is replicated amongst nodes providing a record of all previous actions which is immutable, not changeable.

The information contained in this presentation is provided by Next G Connect LLC. ("NGC") to you as is.   Any reproduction, dissemination or onward transmission of this presentation or the information contained herein is can be done provided you reference its origin, www.nextgconnect.com.

Blockchain

- Blockchain's distributed ledger is shared between nodes providing a history or rather record of all previous actions which is immutable, not changeable, due to the unique cryptographic security that blockchain uses .

- Once the transaction is recorded on the blockchain it can not be altered which is very important for protecting your data.

- The blockchain ledger is visible to every node in the network and transaction can involve anything.

- However transaction and smart contracts do not have to be visible to everyone.

What is Blockchain

- All blockchain networks regardless of protocol used can be implemented in one of three basic configurations.
  - Public blockchains: a blockchain that is public allows anyone in the world to read, send transactions, and participate in the consensus process (mining).
  - Consortium blockchains: a blockchain where the mining process is controlled by nodes which have predefined relationships such as a bank, insurance companies, REITS, healthcare. The right to read the blockchain may be public, or restricted to the participants. These blockchains may be considered “partially decentralized”.
  - Private blockchains: a blockchain where write permissions are kept to one organization.

Blockchain

- Blockchain use nodes called miners/verifiers to verify and approve every transaction that takes place in the blockchain

- Blockchains do not always need to be run on the internet, they can be private, public or consortium based blockchain networks

- Three major blockchains currently are Bitcoin, Ethereum, and Hyperledger:
  - Bitcoin is purely a cybercurrency blockchain
  - Ethereum blockchain uses cybercurrency and smart contracts
  - Hyperledger uses smart contracts

- A smart contract is a program residing in the blockchain that can be executed by sending a transaction to the smart contract

Blockchain elements

- The main components of the blockchain are:
  - Blocks
  - Hashing
  - Keys
  - Nodes
  - Miners/Verifiers
  - Smart Contract

The information contained in this presentation is provided by Next G Connect LLC. ("NGC") to you as is.   Any reproduction, dissemination or onward transmission of this presentation or the information contained herein is can be done provided you reference its origin, www.nextgconnect.com.

Blockchain elements

- **Blocks**: Is a record of a transaction that can be monetary, contract, or something else. Each block is linked to the previous block that contains a cryptographic hash of the previous block. When the new block is created is has the previous block's cryptographic hash, its own cryptographic hash, a timestamp and of course the transaction data. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

- **Hashing:** Hashing is a method of encryption called cryptographic hash. Most cryptographic hashes use a secure hash algorithm (SHA). The SHA size in blockchain is referred to as either SHA2 or SHA256 which means it's a fixed length of 256 bits in size. The fixed size makes the hashing deterministic and is required for the miners to verify the transaction.

The information contained in this presentation is provided by Next G Connect LLC. ("NGC") to you as is. Any reproduction, dissemination or onward transmission of this presentation or the information contained herein is can be done provided you reference its origin, www.nextgconnect.com.

Blockchain elements

- **Keys:** In blockchain there are is a private key and public key. The public and private key for each user or device is created by an algorithm which encrypts a password that is created by the user. The output of the algorithm produces a private and public key which is a 256bits in size, SHA256.
  - The public key is an address that is made public for all to see.
    - The sender uses the recipients public key to encrypt the transaction
  - The private key
    - the sender uses its private key to sign the transaction
    - the recipient uses its private key to decrypt the transaction

- **Node:** Is a device that is part of the block chain. The node can either be the sender, recipient or a passive observer of the blockchain transactions. As part of the blockchain process every node has the same information as all other nodes which makes it secure and resilient.

What is Blockchain

- **Miner**: Any node in the blockchain network can take part in securing the network through a process called "mining". Nodes which have opted to be miners compete to solve math problems which secure the contents of a block. The miner is the entity that verifies the transaction between the sender and recipient. The miner typically receives a transaction fee for verifying that the transaction is valid , this is paid by the sender of the transaction.

What is Blockchain

- **Smart Contract**: A smart contract is a list of actions and conditions that need to be completed in order to fulfill the contract. The smart contract can be a single function or multiple step function involving two or more participants.

- Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman

- A smart contract is also 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 smart contract is stored on the blockchain and is triggered by blockchain transactions. A smart contract can also reference other smart contracts.

The information contained in this presentation is provided by Next G Connect LLC. ("NGC") to you as is.   Any reproduction, dissemination or onward transmission of this presentation or the information contained herein is can be done provided you reference its origin, www.nextgconnect.com.

How Blockchain works

- To begin both the sending and receiving parties need to have both a public and private key.
  - Both sender and recipient create their own private and public keys
- Nothing happens until someone requests a transaction.
- When a transaction is requested
  1. To initiate a transaction the sending party obtains the public address of the recipient
  2. The transaction is then encrypted by the sender, called signing, and is used to confirm this is indeed a desired transaction
  3. The requested transaction is broadcast to all the nodes in a blockchain. However the transaction is not added to the blockchain at this moment.
  4. The miners then begin the process to verify the transaction is valid
  5. For a transaction to be verified by the minors, a simple majority is needed, then the transaction is allowed to proceed
  6. The miner then posts the new block to the block chain
  7. The recipient of the transaction reads the block chain that is addressed to it based on its public address
  8. The recipient then decrypts the block using its private key
  9. The transaction is now complete
  10. The rest of the nodes in the network also receive the transaction details when their local blockchain copy is synchronized

The information contained in this presentation is provided by Next G Connect LLC. ("NGC") to you as is.   Any reproduction, dissemination or onward transmission of this presentation or the information contained herein is can be done provided you reference its origin, www.nextgconnect.com.

How Blockchain Smart Contracts work

- Smart contracts follow a similar process for a blockchain transaction however there are some distinct differences
- The smart contract is created using commands that tell the blockchain this is a smart contract and not a transaction
- To create a smart contract the author of the smart contract, sending party, needs to have both a public and private key
- Creating a Smart Contract:

  1. The smart contact contents are created
  2. The smart contract is then signed using the private key of the smart contract creator
  3. The requested transaction is broadcast to all the miners in a blockchain
  4. The miners, which also can be nodes, then begin the process to verify the transaction
  5. If the transaction is verified by the miners, a simple majority is needed, then the transaction ,smart contract, is allowed to proceed
  6. The miner then posts the new smart contract block to the blockchain
  7. The transaction is now complete
  8. The rest of the nodes in the network receive the smart contract address when their local blockchain copy is synchronized
  9. Only invited recipients can use the smart contract

IoT and Smart Contracts

- There are many uses for smart contracts.

- One unique use of smart contracts is for IoT.

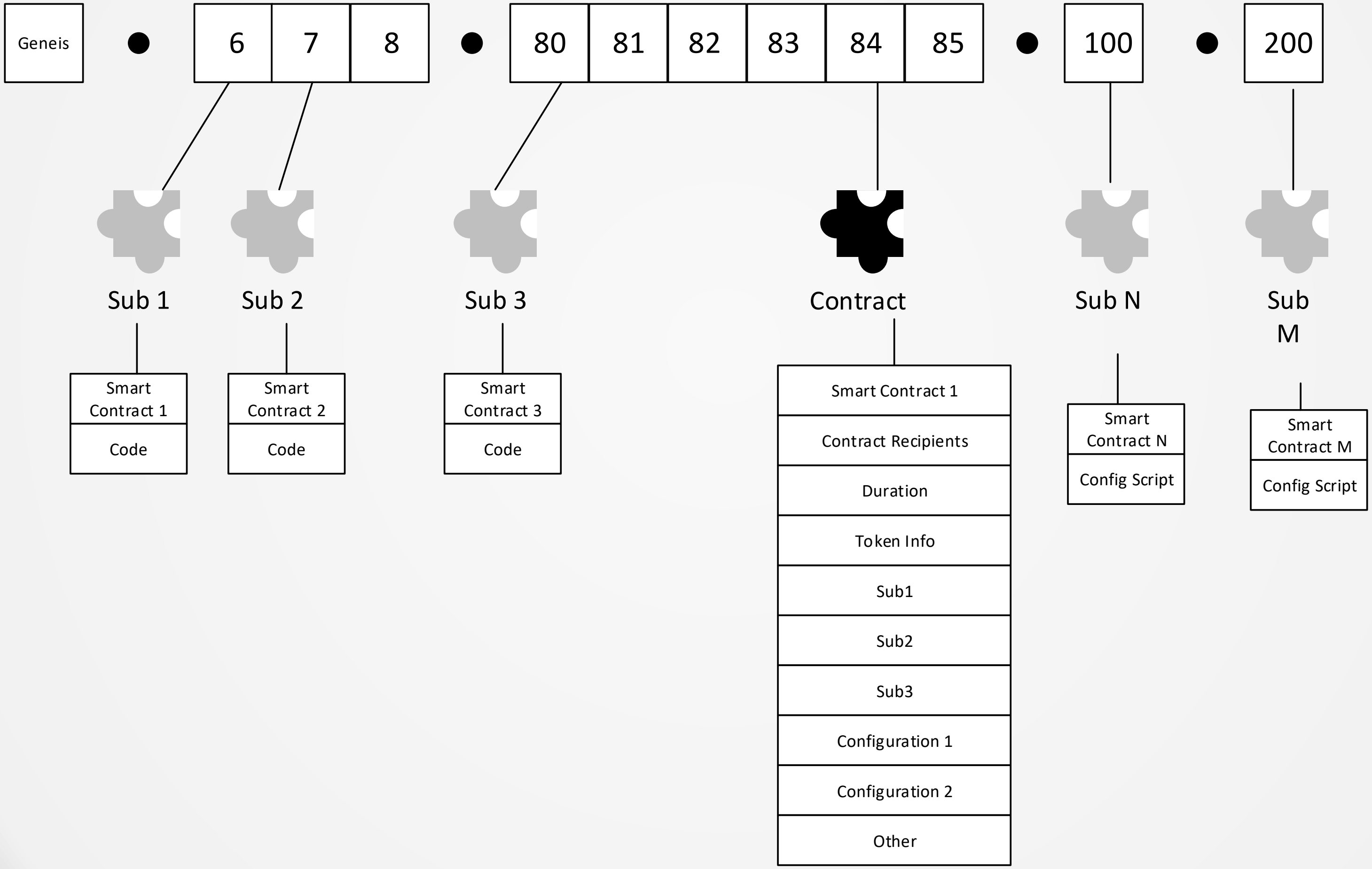
- The NGC IBS solution uses smart contracts to deliver software code and configuration scripts to the IoT device

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

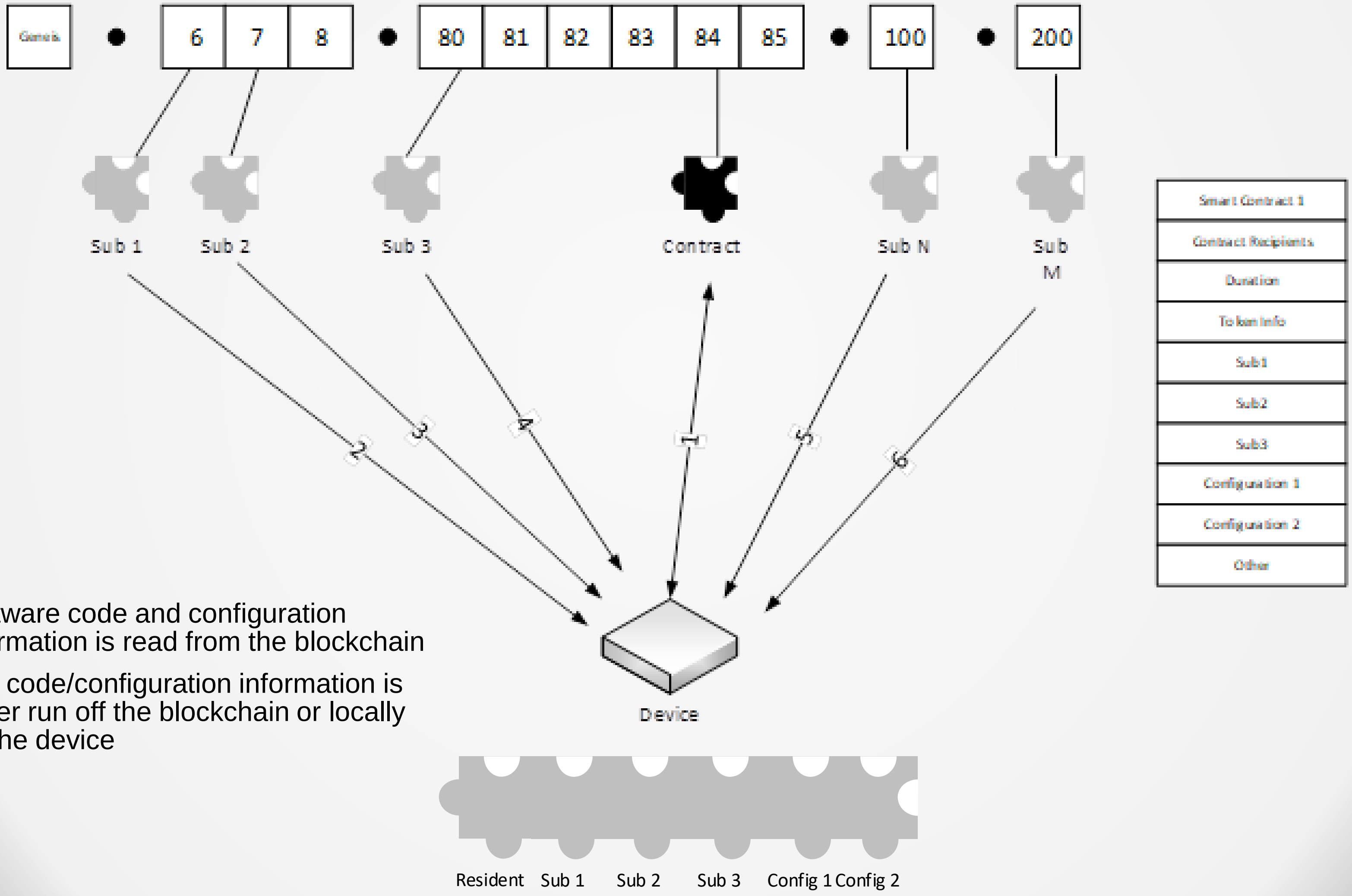
  1. IBS uses smart contracts to proactively detect/prevent malicious devices.
  2. Stores pieces of code in the blockchain which can be invoked by IoT devices or a smart contract within the blockchain.
  3. Addresses provisioning of the device where the device gets its provisioning script from the blockchain.

The information contained in this presentation is provided by Next G Connect LLC. ("NGC") to you as is. Any reproduction, dissemination or onward transmission of this presentation or the information contained herein is can be done provided you reference its origin, www.nextgconnect.com.

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

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 this presentation 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

Thank you

The information contained in this presentation is provided by Next G Connect LLC. ("NGC") to you as is. Any reproduction, dissemination or onward transmission of this presentation or the information contained herein is can be done provided you reference its origin, www.nextgconnect.com.