SCTE·ISBE CABLE-TEC EXPO 2018
ATLANTA, GA
OCTOBER 22-25

2018 Fall Technical Forum
SCTE·ISBE • NCTA • CABLELABS

The Emerging Impact and Use Cases of Blockchain Technology in the Era of HFC Connected People and Things

A Technical Paper prepared for SCTE•ISBE by

Sandeep Katiyar
Senior Consultant
Nokia Bell Labs Consulting
Bldg. 9A, 7th Floor, DLF Cybercity
Gurugram, India-122002
sandeep.katiyar@bell-labs-consulting.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

Introduction

The number of connected devices in the future is expected to reach into the billions with the advent of the IoT, 5G, and the continued proliferation of smart devices. The extensive footprint of Multiple System Operator (MSO) Hybrid-Fiber Coax (HFC) networks will play an important role in rapidly expanding the connectivity of these devices across the globe. While virtualization and Software Defined Networking (SDN) reduce the network architecture complexity and provide a better way of processing and routing data, the security of such architectures to support these billions of devices, data integrity, and content privacy are still under question and will remain a key concern in upcoming years. Blockchain is emerging as a new way to address such security concerns through decentralizing the security construct and letting each connected device fundamentally become part of an overall security architecture.

Given the constant source of interest due to its decentralized secure way of transferring value or information with help of smart contracts or major industry sectors (i.e., telecom, banking, education, health-care, government, etc.), organizations are evaluating the ways in which Blockchain can be adopted in their areas of influence. The first ones are mostly financial organizations where highly-secure transactions play an important role. The core premise of Blockchain is to distribute the whole aspect of application or operation, where the operator[1] provides a simple convenient way to organize, manage and provide services to its subscribers. Figure 1 illustrates the concept of decentralization, where the left side shows a star topology with centralized authority for the network nodes, and the right side showing network nodes with a decentralized and a distributed configuration. Further, topology, network complexity and its applicability pave a path for the type of Blockchain implementation an operator decides to implement: Private (Enterprise), Semi Public or Public. The reason for opting for a Private Blockchain in communication networks is that mostly all the operations inside a network will greatly impact the transactions between network nodes and will have lesser amount of interaction with an end subscriber until the enterprises use cases like SDWAN gather . That is broadly, until Public Blockchain implementations for uses cases such 3rd party storage services and content services are offered by the operator and need to make the 3rd party provider and subscriber part of the Blockchain.

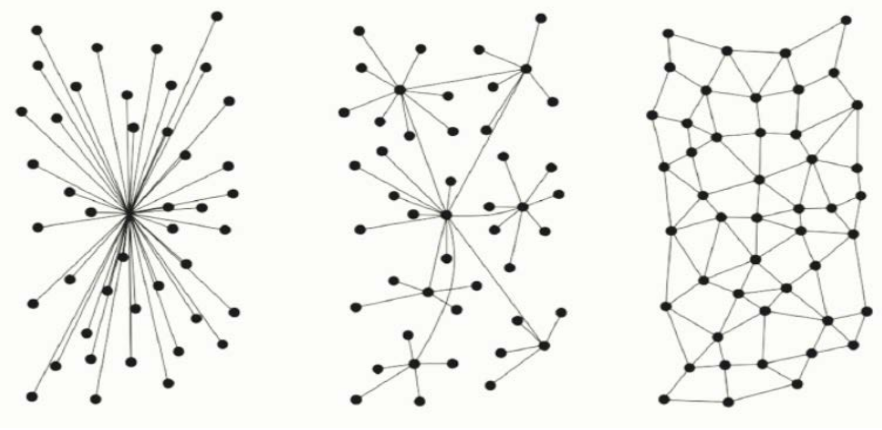

Figure 1 - Nodes & Links in Centralized vs. Decentralized vs. Distributed Environment

This paper discusses the impacts and use cases of Blockchain technology in cable architectures and broadly outlines the mechanisms on how Blockchain distributed ledgers and trust mechanism can help protect the integrity of the network.

[1] The one who owns the Blockchain.

Background

This section provides a basic overview of the key Blockchain and SDN concepts and technologies.

A. Blockchain

A Blockchain is a distributed database consisting of a continuously growing set of records which are referred to as “blocks”, each record is list of transactions and each transaction is signed. Cryptography is used to link blocks together through signing (one way hash functions that are encrypted with a key). Blocks include a hash of the previous block, with proof of work (or similar proof, i.e., Proof of Stake, time, etc.) that help verify the integrity of a transaction, transactional data, and a timestamp. This makes an interconnection between the blocks, thus creating a chain of blocks or a Blockchain. Altering any data in a block retroactively cannot be done unless all subsequent blocks are altered. Any unauthorized alteration of a block or transaction is easily identifiable as corrupted.

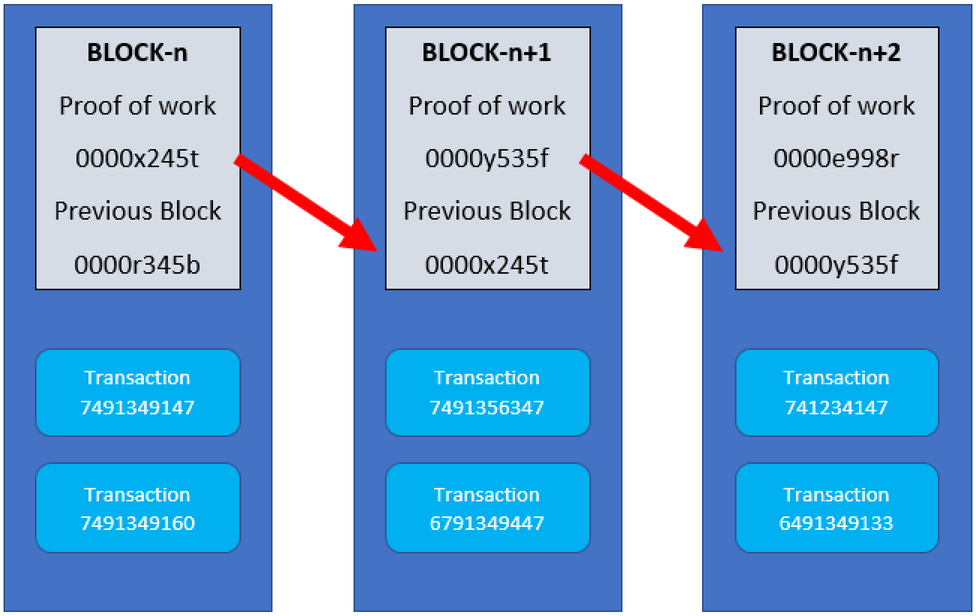

Figure 2 - Example Blockchain Showing a List of Cryptographically Verifiable Records

As previously mentioned, the three classical main pillars that Blockchain stands-on are, Transaction, block mining and distributed ledger, Transaction among network nodes is a transfer of modified configuration or a status change value that is broadcast to the network and is collected into blocks. Block mining is the process of adding earlier transaction records to the ledger of past transactions or Blockchain. Distributed ledger is a database which is shared and synchronized across the network. The Blockchain eco-system is enabled by these pillars to provide a holistic trust-based approach to secure transactions and the networks, largely reducing the barrier between trusted and untrusted aspects of networks. Translating these pillars to Telco network requirements the main pillars are transaction integrity (e.g., transactions are signed using asymmetric key cryptography), blocks are compiled that include a hash (may or may not be a signature) of the previous block, and the resulting blockchain is distributed amongst a sufficiently large network.

While Blockchain adopts the decentralized concept among peers for transparent information transmission, some characteristics of Blockchain, such as using all network entities to distribute Blockchain, might not be fully applicable to telecom networks. Blockchain might be helpful in securing SDN, cloud storage, virtualization, IoT and billing in MSO networks.

B. Software Defined Networking (SDN)

SDN decouples the network control plane and forwarding plane functions and enables network control to be programmable. The underlying network infrastructure is abstracted to both applications and network services. Control, decoupled from hardware, is implemented in software within SDN controllers. To illustrate this concept the following is provided. In traditional non-software defined networks, a data packet arriving at a switch or router is forwarded to a destination based on decisions made in firmware.. However, in SDN, such packet forwarding decisions are made by SDN controllers. For each packet entering a switch or router node, the SDN forwarding plane decides what to do with the packet. The SDN controller defines the flows which denotes the data itself. A set of packets transferring from source to destination (or set of endpoints) is characterized by a flow. Internet Protocol (IP) address, TCP/UDP port pairs, Virtual Local Area Network (VLAN) endpoints, layer three tunnel endpoints and input ports, etc. define the endpoints in SDN. The forwarding action that the SDN devices take into decision is determined by one set of rules which apply to all packets belonging to that flow. A flow is unidirectional in that packets streaming between those same two endpoints in the inverse direction could each constitute a separate flow. The Open Flow protocol helps to periodically collect information from network devices concerning their status along with commands involving how to handle traffic. Furthermore, an Orchestrator provides overall management of the different domains of a network from an end-to-end perspective. Refer to Figure 3.

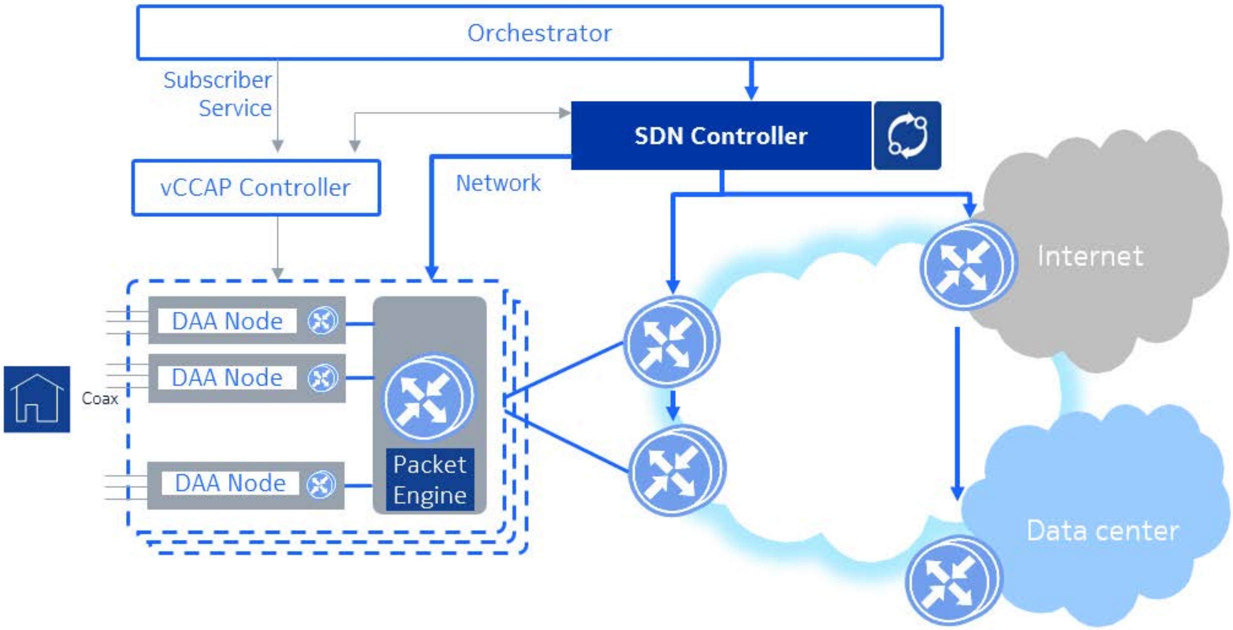

Figure 3 - MSO SDN Architecture

MSOs will move from a centralized Integrated Converged Cable Access Platform (I-CCAP) to a virtualized Distributed Access Architecture (vDAA) over time. Various Data Over Cable System

Interface Specification (DOCSIS®) functions will be disaggregated and distributed in a vDAA. In a Remote PHY (Physical) vDAA architecture, the MAC (Media Access Control) layer will be centralized in a cable hub/data center and the PHY layer will be distributed to a vDAA node located deep within the HFC Network. In a Remote MAC/PHY vDAA architecture, both the MAC layer and the PHY layer will be located at the vDAA node. SDN will enable greater flexibility and programmability of this emerging architecture. One such example is automatically configuring and administering complex DOCSIS profiles based on the network condition, with further possibility to have an end to end process by integrating together with Transport-SDN which automatically optimizes the transport network, based on varying characteristic in networks .

Blockchain Impact and Benefits on the HFC Network and Services

Blockchain technology may benefit future HFC architecture and services provided by an MSO. Future HFC architectures may enable decentralized business models. This may seem an odd assertion for access networks. However, consider that emerging HFC networks, particularly with new DOCSIS 3.1 technology standard, bring massive bandwidth businesses. In the WAN market place, we’ve seen dramatic adoption of virtualization technologies. Enterprises in terms of size and locations are getting more dependent on connected resources every day to tackle the customer expectations and dynamic management of WAN bandwidth and resources is becoming critical to their everchanging game for their business networks. For example, if we look at the growth of virtual operators to Slicing concept in the Mobility world we can relate the same here with our HFC networks, given that complete Virtualization and cloudification of the networks is ongoing and achievable, where once its enabled a HFC owner that has deployed Slicing could offer an tenant a dedicated slice of its network for carrying traffic, but further this tenant is also enabled to deploy its own VNF's (virtual network functions), helping both the operator and virtual operator achieve better flexibility, reliability & savings.

As HFC scales, we should anticipate similar technologies and business solutions. This leads to defining a new plane in our access infrastructures, the business plane, which together with the existing management, control and data planes, will provide secure and automated service enablement. In such architectures where an MSO interacts with other operators or content providers, it will be useful to manage incentives using consensus processes, such as proof of work, to support a variety of distributed network functions. This results in and access platform for new business services. Some examples are shown below.

- Media Content services: Leasing content from the content provider.
- Storage as a Service: Leasing storage to another enterprise.
- Platform as a Service: Leasing solution stack to enterprise.
- Infrastructure as a Service: Leasing necessary hardware, storage etc. to enterprises.
- SD-WAN: Overlay connectivity option for enterprise using SDN or similar concepts.

Apart from the business services, which will have a major impact/influence of how the client is enabled and managed, the HFC network will be impacted due to ongoing virtualization of the headend, IOT infrastructure creation, and SDN enablement. The last two are more practical and have larger influence in terms of Blockchain implementation.

A main aspect of Blockchain on the network side which makes it suitable for HFC networks is the provisioning and feedback mechanism performed in a better way. Though we have 2-way feedback mechanisms with SNMP, NETCONF, etc., considering the way SDN works (i.e., depending on network status), changes triggered by SDN controller might impact multiple nodes to ensure the integrity of a configuration across the addressed nodes.

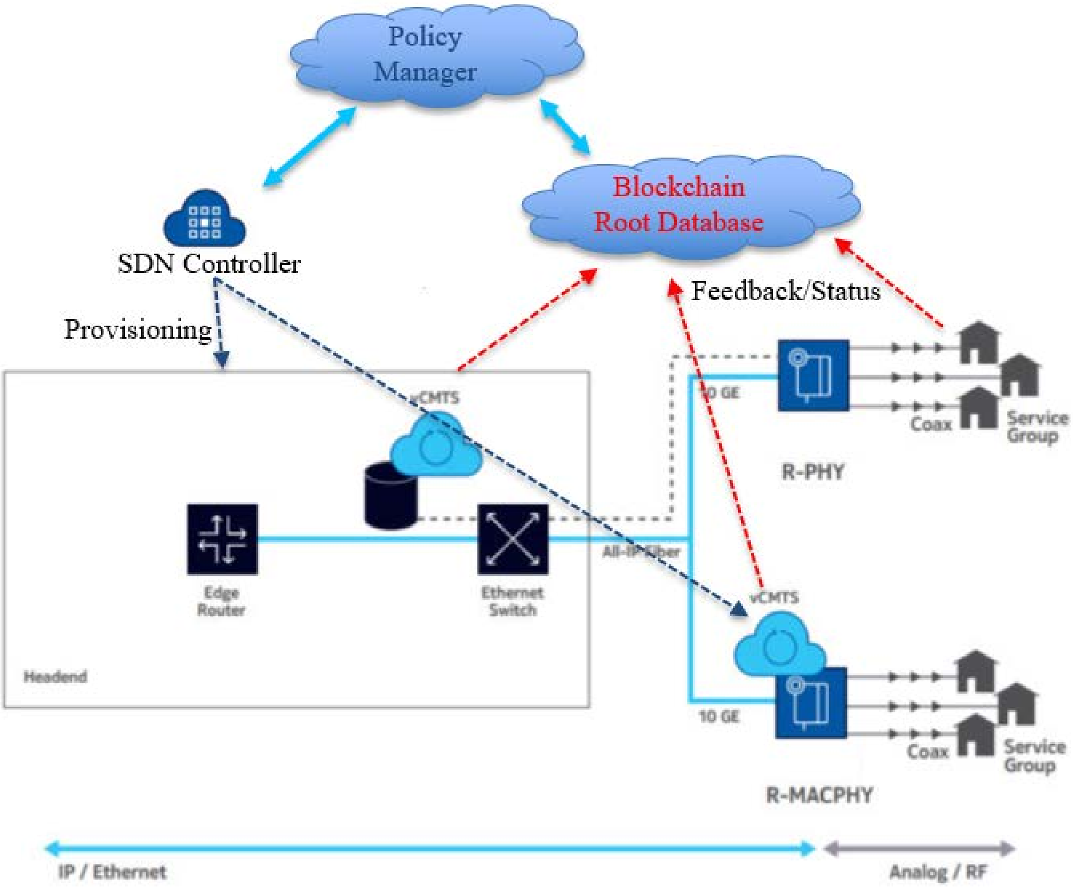

Figure 4 - Example MSO Blockchain Architecture

Similarly, in case of the business services, the resource configuration for the enterprise or subscriber can be provisioned based on the feedback/status principles of Blockchain to link heterogeneous resources with heterogeneous needs in a digitally enabled world. This in turn means that Blockchain provides a more secure and transparent way to manage the network and services benefiting the network owner and the end user.

As depicted in Figure 4 above, the architecture brings two new nodes into the network, the Policy Manager and the Blockchain Root Database. The Policy Manager sends direction to the SDN Controller or SDWAN Controller or Access Controller, to act on the given requirement i.e, setup circuit between NodeA and NodeB with so and so bandwidth, it will help program automated behaviors in a network to coordinate between the required hardware and software elements to support different applications and services. The Policy Manager role can be integrated with the Orchestrator (Figure 3), and whenever any change in configuration is triggered across a network between multiple nodes, the Policy Manager queries the Root Database for the last hash value to confirm the integrity and authorizes an action. The change it will have in comparison to normal flow is that, here after successful execution of the command, the triggered changes and participating nodes generate a top hash between them and that gets stored in root database for a particular time t and is queried each time before executing a new command to ensure the integrity of network, the generally, The Blockchain Root Database contains the hash values for referred transactions at particular time intervals using a Merkel tree. This concept in further explained in the next section.

The high-level benefits that Blockchain provides to an MSO are:

1) Decentralized Network data: The HFC network data is stored off-chain in a distributed way facilitating multi-party trust, and a participating node i.e., router, vDAA can easily find the storage address through the Blockchain i.e, quicker response, minimal impact during failure of one or more nodes.

2) No Centralized Trust based mechanism: The access to HFC data is controlled by the majority of the Blockchain enabled network entities (modems, RPDs, CMTSs that can originate or relay transactions as part of a blockchain network), without any intervention from single trusted source i.e., rather than single source of trust mechanism, whole network works in sync mode as trust enabler.

3) Traceability and Accountability: Activities such as accessing and modifying the HFC network configuration data, can be recorded by the Blockchain. No malicious attempts can go undetected.

4) New Business Services: Considering Multi-tenant reality over period of time, BC will help operators in ensuring their network integrity and ease of operations.

Blockchain Design for SDN Implementation

As SDN is steadily being deployed, various security attack vectors could also penetrate SDN implementations, examples of known ones are listed below:

- Malicious SDN applications.
- Malicious controller creating entries in the flow tables of the network elements, thus gaining complete control of the network.
- Malicious network element, or a hacker posing as an administrator.
- Unauthorized access to an SDN framework.
- Unauthorized configuration, network or topology change.
- Attack on SDN function causing service disruption.

While the Open Networking Foundation (ONF) provides several recommendations including ONF TR-511, TR-529 and TR-530 for securing SDN, Blockchain can help strengthen it further and mitigate the threat created by SDN’s centralization of control - a key security concern with the SDN model. SDN’s centralized control model raises security concerns as described below, given it can become a single point of security attacks that can have disastrous results. Blockchain can improve security and mitigate threats using hash-values

Trust
Identity Assurance
Configuration Mishandling
Participation proof

Figure 5 - Security Factors Concerned with SDN Implementations

and binary trees, irrespective of where an asset is located or where data is stored. Every node (vDAA router, switch, etc.) and its related configuration, operator, or via automatic function can be tagged, tracked and located with real-time verification independent of trusted administrators. Blockchain provides a system wherein the need for trust can be eliminated.

Using a Merkle tree implementation as shown in Figure 6, a distributed binary tree can be periodically generated using hash-values of data generated in the MSO network. Two input values, along with required parameters, are concatenated and run through a hash function. This process is iterated, resulting in a single root hash value. Shared secrets are still used for authenticating clients during the signature validation process, keys are not needed every time for the signature verification itself. The integrity of the signatures is protected using hash functions thus reducing the repetition of key exchange and need of the signature verification each time.

Finally, the root hash is calculated and stored in top database or root database which consists the hash output of top chain for any changes propagated by policy manager at given time t and is broadcasted to all other nodes (vDAA node, router, switch, etc.). For every hash value included in the tree, there is a unique hash-chain, or series of hash-values that allows the root hash-value to be recreated. This hash chain is returned and stored as the signature. A signature identifies the node or configuration through the hash tree, from the node’s own hash value, up to the root database consisting of a complete transaction record. With access to the root database, anyone (nodes), anywhere (any part of the network), can receive data and verify the signature, which includes indications of time, identity and integrity. The process is unique and one of concepts in which the integrity of the transaction i.e., the change propagated to the network nodes gets covered with hashing and in case of subsequent changes in the network where the policy manager queries the node and root database gets verified with policy manager private key and Nodes public keys in turn providing the non-repudiation.

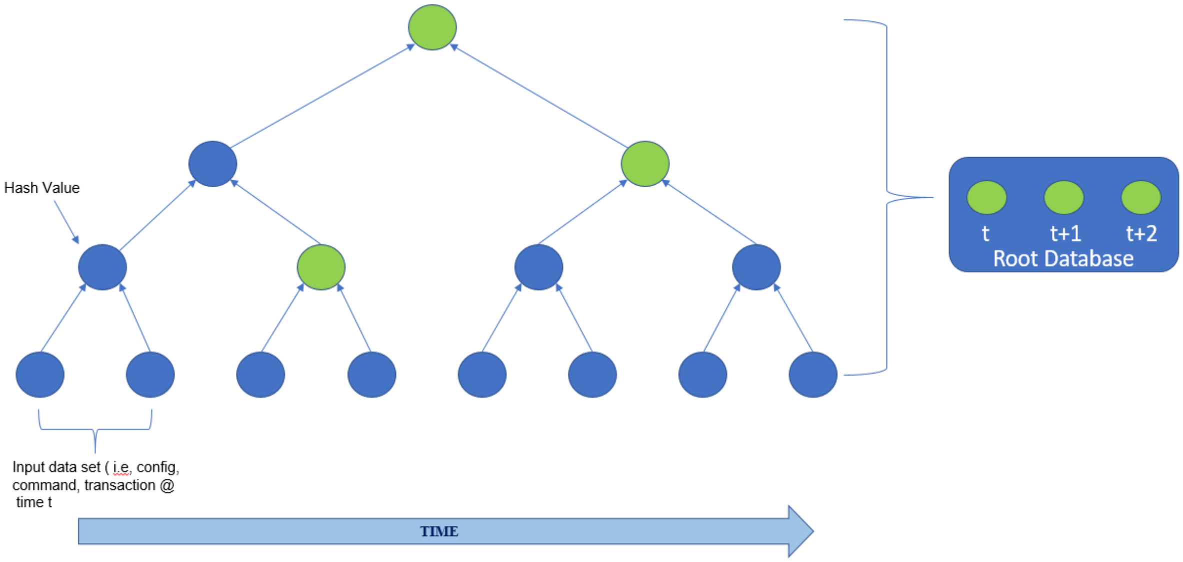

Figure 6 - Hash Block Chain & Merkel Tree

By integrating a Private Blockchain model, the components of an MSO SDN network will be able to sign and verify data as it moves between components. This provides the MSO with a data integrity infrastructure in which data can be verified in near-real time. The data residing in the configuration storage is regularly monitored for its consistency and verified against the associated signatures that were created upon the creation of the configuration data. The design of this chain can be implemented using the hierarchical model used in the current generation of networks, where the hashes at different layers of network are aggregated and processed at each layer and the top database (Database holding computed hash values of the chain relevant to specific portion of network for a time intervals) is settled and stored at the MSO datacenter.

Dealing with multiple services, deploying SDN, network slicing, and virtualization makes this ideal for MSOs.

Blockchain Design for IOT Implementation

Unlike SDN, in the IOT Implementation of Blockchain, subscriber CPE at the originating point of the Blockchain can be used to manage the IOT device configuration, maintain integrity of the received sensor data, possibly enable micro payments (payments triggered for using any specific content, or storage) based on need. The utmost concern that had been shown by operators is how to leverage the Blockchain as service, With IOT, the constraints are much more varied and misunderstood. Blockchain can be enabled as a service on the end IOT platform running over the HFC networks.

While implementation can be achieved with the previously explained SDN model, a key question arises, where should the Blockchain be hosted? Hosting the Blockchain directly on IoT devices is not possible due to resource constraints, although this requires implementation and a need to deploy better computational resources in the network. These resources will cater to the need of the IOT application host. The host collects a consistent set of IOT sensor data for analytics, which preferably can be implemented at various boundaries of network layers as well as implementation of cloud datacenter for this data hosting.

An IOT application provider will look for opportunities to create/store/transfer digital assets inside any practical MSO network, adding value for the provider, and potentially providing a new business stream for the MSO.

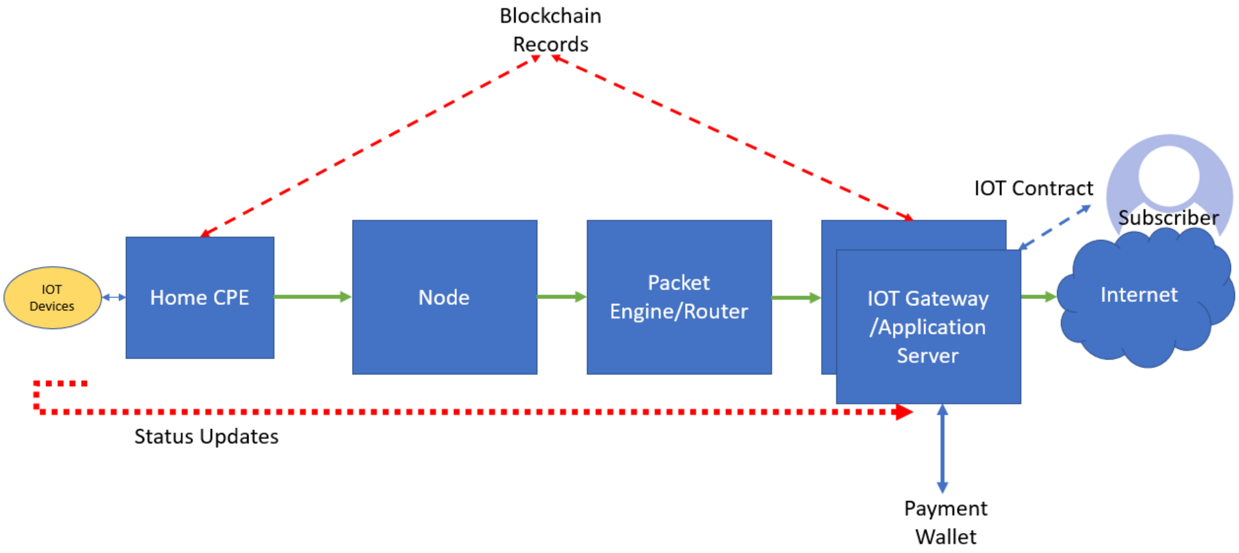

Figure 7 - HFC IOT Blockchain

Possible High-Level Transactions or Use Cases over the Blockchain enabled HFC network includes:

- Smart contracts (a digital contract which facilitates, verifies or enforce the negotiation or performance of a contract between two parties).
- IOT provisioning.
- IOT management.
- On demand service/update sharing.
- End user security.

Some traditional MSO use cases include:

- Financial settlements (e.g., peering and transit) for backhaul services MSOs provide to MNOs.
- Settlement of MVNO minutes - MSO and MVNO.
- Financial settlements with vendor supply chain.
- Consumer credential mobility – i.e., a Cable customer typically is given free WiFi access in the MSO footprint) requiring log-in and authentication using the MSO credentials. Blockchain can help enable easy and automatic authentication as well as enable mobility between two MSO WiFi networks if they choose to enable such a feature.
- Data Integrity - Of long-term databases, providing protection of subscriber databases from hacking.
- Asset Management – parts and spares inventory tracking and management.

Example HFC enablement for Blockchain

The following table contains a high-level roadmap and impact of Blockchain convergence with HFC networks:

Implications/Period	Phase-1	Phase-2	Phase-3	Phase-4
Key Developments/Enablers	Studying and Leveraging SDN in HFC Networks from operations point of view	SDWAN and IOT Offerings	Key developments and Solution design for Sustained introduction of Blockchain in HFC Networks to secure internal network assets	Introduction of Blockchain as a service Integration with existing ecosystem
Outcome	E2E Management Ease of operations Better fault handling	New revenue potential Surveying the slicing needs for HFC	Improved network security Better compliance to the integrity of services provided and data used for storage and analysis Cost efficiencies due to shared resources & processing	New revenue streams Predictive subscriber needs

Conclusion

This paper explored the combination of Blockchains, SDN and IOT over MSO networks which can be beneficial and help secure the networks in more pragmatic and simplistic way.

While Blockchains provide resilient, distributed peer-to-peer systems together with SDN, IOT and content transactions, it helps in automating workflows with new methods and flow, achieving trust, with significant cost and time savings in the process. The Root Database provided by Blockchain in an SDN network used for a network integrity check makes the transactions in the SDN environment more robust against untrusted members outside the Blockchain. Similarly, together with IOT, Blockchain can be utilized as another service enabler.

Continued research and new implementation models will bring about new business models in the security domain.

Abbreviations

CPE	customer premises equipment
DOCSIS	Data over cable system interface specification
HFC	hybrid fiber-coax
IOT	Internet of Things
ISBE	International Society of Broadband Experts
MAC	media access control
MNO	mobile network operator
MSO	multi service operator
MVNO	mobile virtual network operator
ONF	Open Network Foundation
PHY	physical layer
SCTE	Society of Cable Telecommunications Engineers
SDN	software defined networking
SD-WAN	software defined wide area network
vDAA	virtualized distributed access architecture

Acknowledgments

- Martin Glapa, Partner & Bell Labs Fellow, Bell Labs Consulting, USA.
- R.J Vale, Principal, Bell Labs Consulting, USA.
- Ben Tang, Principal, Bell Labs DMTS, Bell Labs Consulting, USA

Bibliography & References

A Simple Overview of Blockchains, Why They Are Important to the Cable Industry. Steve Goeringer. SCTE-ISBE. 2017 https://www.nctatechnicalpapers.com/Paper/2017/2017-a-simple-overview-of-Blockchains-why-they-are-important-to-the-cable-industry/download

Decentralized access control mechanism with temporal dimension based on Blockchain. Mayssa Jemel and Ahmed Serhrouchni. The Fourteenth IEEE International Conference on e-Business Engineering. 2017

Blockchain in Telcos: A tool for openness. Dimitris Mavrakis. 2017

Introduction to Blockchain. Javier Antich Romaguera, Juniper. MPLS+SDN+NFV. 2018

The Role of SDN in Broadband Networks. Hassan Habibi Gharakheili. 2016

Blockchain basics: A non-technical introduction in 25 steps. Daniel Drescher. 2017

Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis. Georg Becker. Seminararbeit Ruhr-Universit¨at Bochum. 2008

Demystifying Bitcoin and Blockchain. Ganesh Kondal. 2016

A Framework for Determining Blockchain Applicability. Brian A. Scriber, Cabelabs. IEEE. 2018

A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks. Pradip Kumar Sharma; Saurabh Singh; Young-Sik Jeong ; Jong Hyuk Park. 2017

An Innovative Security Architecture for Low Cost Low Power IoT Devices Based on Secure Elements. Urien, P. IEEE CCNC. 2018.

Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. F. Tschorsch and B. Scheuermann. IEEE Commun.Surveys & Tutorials. 2016.

The Blockchain as a Software Connector. X. Xu et al. IEEE/IFIP Conf. Software Architecture. 2016.

Comparing Blockchain Implementations. Zane Hintzman. SCTE-ISBE. 2017