MeshBox

MeshBox®
HyperMesh^{TM} Building Block

Whitepaper Version 4.0.1

2020.10.14

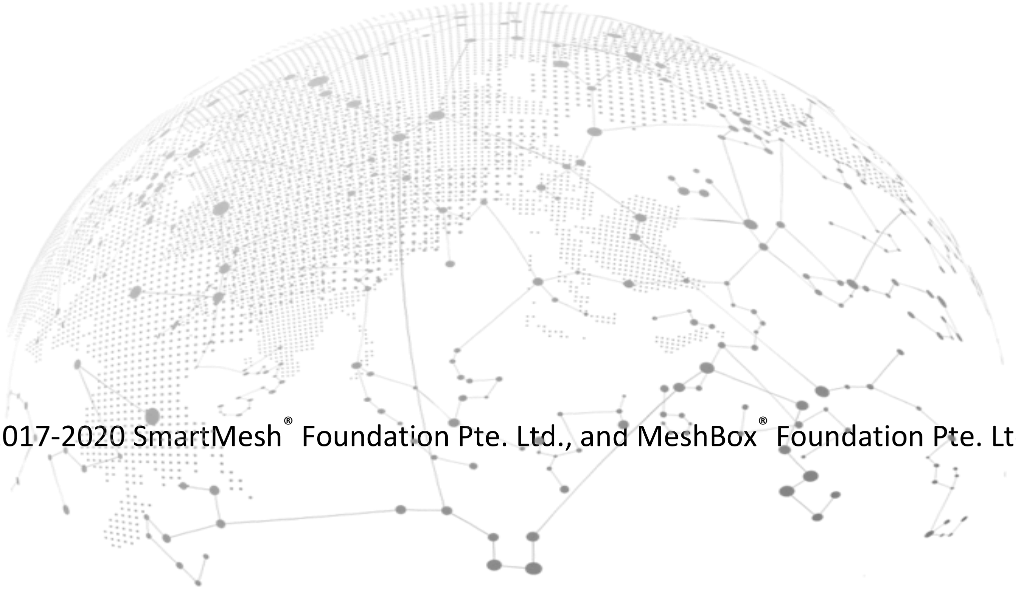


Table of Contents

1. Executive Summary

Our current Cyber-Physical Infrastructure is a technological marvel, gifting mankind with tools to innovate at an ever-increasing exponential rate. We depend on such innovation if we are to survive and thrive as a species.

However, the need for faster, ubiquitous, exchange of information and value continues to expand in scope, even bringing in everyday objects and machines. The current infrastructure, which was built by corporations focusing on maximizing share-holder profits, is flawed, due to the centralized nature of the business model, and by the resulting centralized networks which have been created.

In March, 2018, the world-wide-web turned 29 years old. In an open letter to mark the 29th anniversary of his invention, Berners-Lee made some sharp criticisms on how the technology has been deployed:

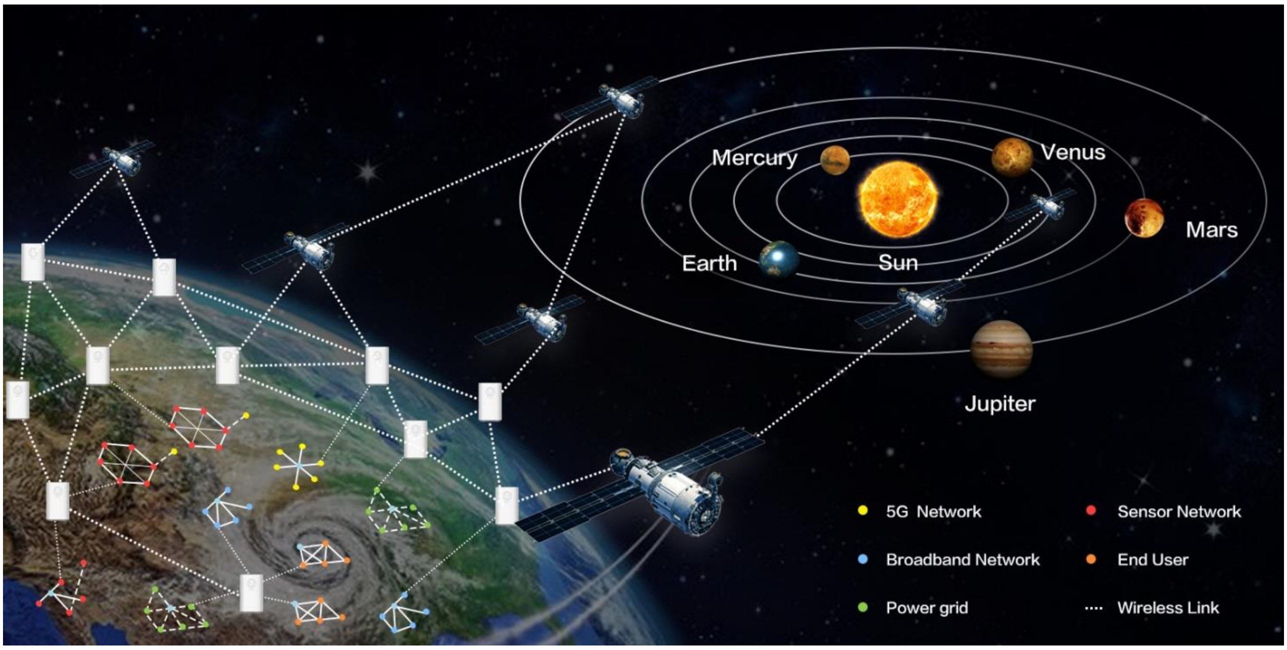
> *In recent years, we've seen conspiracy theories trend on social media platforms, fake Twitter and Facebook accounts stoke social tensions, external actors interfere in elections, and criminals steal troves of personal data.*
>
> *These problems have proliferated because of the concentration of power in the hands of a few platforms – including Facebook, Google, and Twitter – which control which ideas and opinions are seen and shared.*

Furthermore, centralized data in the hands of a few corporations constitute single-points-of-failure and are susceptible to a myriad of internet attacks such as DDOS, malware, etc.

While many in the developed countries enjoy advanced technology, there is a growing divide with the rest of the world. There are currently 3.9 Billion people without internet access, 2 Billion people who are unbanked, and 1.2 Billion without access to electricity [Paygo]. The current system cannot effectively address such needs. A new paradigm is needed.

The next generation infrastructure will not be just another iteration on the previous architectures. Rather, it will be a ***HyperMesh***™ architecture, a ***distributed***, synergized blend of networking, computing, content distribution, financial technology, and cyber-physical infrastructures.

The HyperMesh™ Infrastructure is being built from the ground-up, in a distributed fault-tolerant manner, incentivized by blockchain cryptocurrencies, powered by renewable transactive energy, and enabled by a world-wide Satellite Internet with local ***peer-to-peer (P2P)*** Meshed communication on the ground.



Meshbox®, an ecosystem partner of Smartmesh®, is in a unique position to speed up the realization of such a HyperMesh™ Infrastructure architecture. Rather than focus on maximizing share-holder profits and supporting the costly requirements associated with bleeding-edge applications, Meshbox® strategy aims to achieve:

- **Inclusivity**: Provide basic cyber-physical infrastructure for all peoples, including those without access. Provide adequate performance for the most common applications: Support of Wifi communication (which is more prevalent than cellular connectivity); secured, fault-tolerant content and data storage; and low-latency, high-throughput payment network; and renewable energy resources.

- ***Social Entrepreneurship***: Provide a means to bring dignity and a sustainable livelihood to the masses. Enables common people to earn a living by selling ***Internet of Value*** (IoV) services to neighbors and keeping the ROI within the community. People become service providers and have the freedom to deploy infrastructure as they wish.

The key value-propositions being offered are.

- Meshbox® has built ***MeshBox®*** Wifi Routers
    - Indoor and Outdoor MeshBox®es, communicating through Mesh networking to seamlessly cover any application area.
    - Global connectivity with interfaces to various Wide-Area-Networks (WAN)
    - Disk Space for data storage, content delivery, and offline-data access.

- Smartmesh® has deployed a Public Blockchain and Applications
    - ***Spectrum Blockchain*** solution running with Smartmesh® Token (SMT) coin.
    - High throughput, low latency ***Photon Payment Network*** with secured backing on Spectrum.
    - Smartmesh® Wallet and Distributed-Applications for monetized Wifi, Internet, Storage, and Payments.

- Smartmesh® and Meshbox® are optimized to deliver
    - First Blockchain-enabled Communication Infrastructure
    - Offline payments and Content Delivery, via Wifi Mesh Network, with or without Internet connection.
    - Low-cost MeshBox® hardware, plug-and-play operation, unlicensed spectrum, and a blockchain-based monetization mechanism.

The MeshBox® product is an implementation of the above key value-propositions and is an essential building block of the HyperMesh™ Infrastructure.

In the following, key attributes of MeshBox® and differentiation from other technologies are described, with the following interpretation of the various font colors.

- **Expensive, Heavy Technologies**
- Traditional (outdated) Technologies
- **Cost-Effective, Lightweight Technologies (using MeshBox®)**

			Hyper-Mesh$^{\text{TM}}$ Building-Block : **MeshBox$^{\text{TM}}$**
Wireless Communications			
Licensed Spectrum : 1G 2G 3G 4G 5G			
		eMBB	**Supports Streaming Media**
		ULLRC	**Low E2E Latency**
		Machine-to-Machine	**M2M, P2P Communications**
		10Gbps Data-Rate	**1 Gbps Data-Rate**
Un-Licensed Spectrum :			**WiFi 802.11**
Information Communications Technology (ICT)			
	Centralized	De-Centralized	**Distributed**
	Shared-Bus	Switch/Router	**Meshed-Networks**
	Circuit-Switching	Packet-Switching	**Token-Switching$^{\text{TM}}$**
		Information-Internet	**Internet-of-Value**
	Cloud Computing	**Network-Function-Virtualization**	**Edge-Computing**
		Software-Defined-Networking	**Ad-hoc Mesh-Networks**
Highly Scalable Networking			
Satellite Communications			**Space-Ground Integration Network$^{\text{TM}}$**
Hierarchical Networks (Access, Edge, Core, Datacenters)			**FRACTALS$^{\text{TM}}$ Network**
Smart-Cities			**Transactive IoT**
Energy-Efficient-Computing			**LoRa Technology for IoT**

The terms above are described in this whitepaper in more detail.

2. Smartmesh® and Meshbox® Introduction

Meshbox® Foundation has been partnering with Smartmesh® Foundation from the beginning to realize the HyperMesh™ Infrastructure. Smartmesh® blockchain technology has been optimized to run on MeshBox®es.

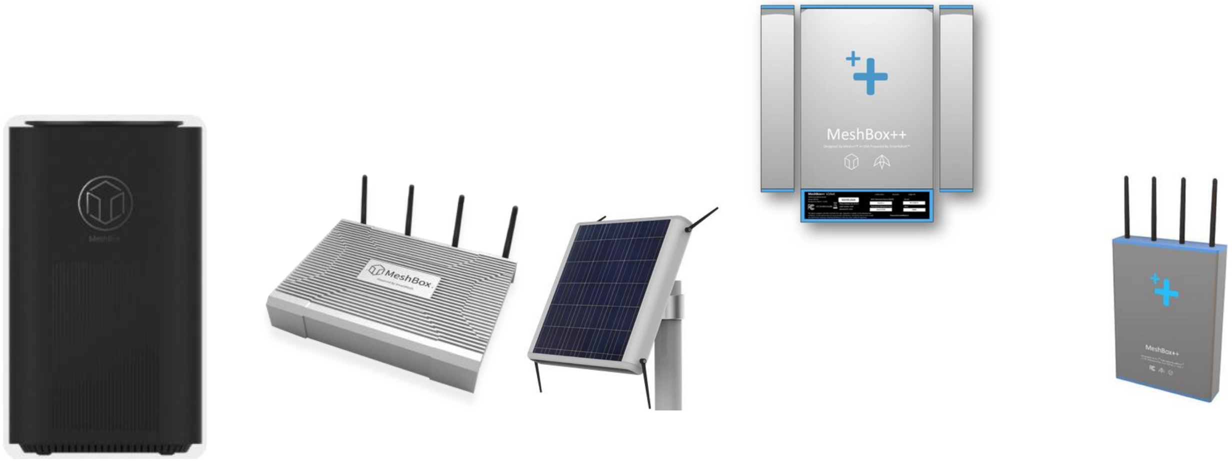
Smartmesh® has deployed the Spectrum public blockchain, which supports the following coins and tokens.

- Smartmesh® Token coin, listed on Huobi.pro and Gate.io, and used for Spectrum blockchain.
- MESH tokens, listed on FCoin.com and HitBTC, and used for the Content Delivery Networks, supporting video streaming.

Meshbox® and Smartmesh® bring about a paradigm shift to enable Infrastructure deployment which is highly robust, yet flexible, due to the ability to operate

- With or without the Internet (or Intermittent Internet)
- With or without a blockchain; with Photon high-throughput Payment Network,
- With or without an electrical grid; with renewable battery and solar technology.

MeshBox®es are used to form large, highly-scalable Wifi Mesh Networks spanning both indoors, and outdoors, over which Smartmesh®'s blockchain technology is layered.



Indoor MeshBox® **Outdoor MeshBox++™ [MB++]**

Hereafter, "MeshBox®" refers to both the Indoor MeshBox® and outdoor MeshBox++™ versions, "Indoor MeshBox®" refers to the indoor version, and "MeshBox++™" refers to the outdoor version.

Indoor applications for Indoor MeshBox® include:

- Company Security
- P2P Banking

- Control Center for IoT devices
- Transactive Energy control
- Special events and gatherings

- Homes & office buildings

- Hotels, Museums, Event Venues
- Shopping malls, Airports

- Transportation

Outdoor applications for MeshBox++^{TM} include:

- Adhoc Mobile Networks
- Internet gateway
- Disaster Stabilization

- Areas without infrastructure

- Dense populations

- Remote Areas, Farms, Fishing ports
- Festivals & Markets

The MeshBox® solution does not require additional wires for communications, since the MeshBox® network nodes are connected wirelessly using Wifi. As long as at least one of the MeshBox®es are connected to the internet (wired DSL/coax/fiber, microwave, or satellite backhaul), all MeshBox®es in the mesh network are also connected to the Internet.

Also, no power cables need to be installed for the outdoor MeshBox++™, which saves the majority of deployment costs, since the Outdoor MeshBox++™ are self sufficient with battery and solar technology.

MeshBox++™, has been deployed successfully in the United States, at the following venues:

- Superbowl 51 February 2017 in Minneapolis, Minnesota : 6 MeshBox++™ nodes
- 50th Special Olympics July 2018 in Chicago, Illinois : 15 MeshBox++™ nodes, 3 gateways.
- Permanent installations of MeshBox++™ networks in San Jose, and San Francisco, California

MeshBox®, as a key component of the HyperMesh™ architecture, works well with several key market trends:

- Wireless communications. MeshBox® provides dense (many users per area), high data-rate coverage, much like Small Cells in 5G Cellular Networks.

- ***Meshed-Networking*** uses distributed, ad-hoc networking to provide fault tolerance to failures, and can be deployed automatically without complicated network configuration tools
- ***Edge-computing***, ***Edge Storage***. MeshBox® supports distributed Data storage through Inter-Galactic-File-System (IGFS). Keeping computations and data local reduces traffic, latency, and energy.
- Peer-to-peer communications (e.g Device-to-Device) through Mesh networking
- ***Transactive-IoT*** with Energy efficient computing and communication. Multi-Core CPUs are used to process both data-routing, data-storage, content delivery, and blockchain-based payment networks. MeshBox® provides a control point for Transactive IoT networks (interfacing to LoRa technology).
- ***Transactive Energy***. The outdoor MeshBox++TM integrates solar panels and batteries for self-sufficient operation. MeshBox® acts as a control point for managing the flow and payment of electricity between Distributed-Energy-Resources.
- Monetization of Infrastructure services with Blockchain and Crypto-currency: Spectrum blockchain and Photon secondary architecture supports peer-to-peer payments. ***Wormhole Universal Channels***TM enable interoperability between various third-party blockchains, using the ***Atmosphere***TM architecture.
- AI and Big Data Services: Applications and services built on MeshBox® support Shared-ROI and double-auction buying and selling of products and services, on behalf of the user.

3. HyperMeshTM versus Traditional Communications

MeshBox®es are used to build a HyperMeshTMed Infrastructure, which incorporates a newly emerging networking paradigm.

In First-generation Circuit-Switching, each connection between communicating parties receives dedicated (reserved) Bandwidth, even when not being used. Examples include Plain-Old-Telephone System (POTS), SONET/SDH, and DWDM for fiber communications.

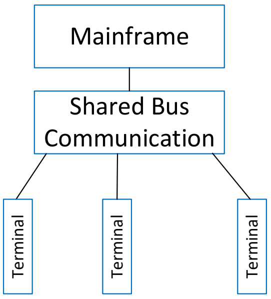
Second-generation Packet Switching is comprised of storing-and-forwarding of message-segments (packets) in routers, which dynamically arbitrate/schedule which packets are transmitted on shared transmission lines. This sharing provides better resource sharing of shared resources and makes use of buffers (memory) to temporarily store packets, thus greatly improving the utilization and efficiency of networking resources. Examples are Switched Ethernet, Internet Routers, and Voice-over-IP.

The newly emerging Third-generation is called ***Token-Switching***TM and is enabled by Blockchain. In this new paradigm the scope is greatly expanded from information exchange to a self-sustainable Internet of Value (IoV), represented by the exchange of tokens. Tokens can represent not only monetary value (e.g. Ethers, SMT, MESH), but also non-monetary entities such as a car or house title, personal identity, medical records, a vote in an election, and can even be linked to physical objects in a supply chain.

The following shows the progression of networking and computer architecture from the mainframe era to today's HyperMeshTM infrastructure, which supports the Internet of Value.

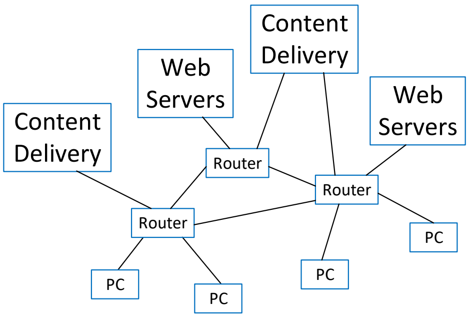
Mainframe Computers and Voice-Communications

Centralized
Circuit-Switched
Cellular 1G 1980s ; 2G 1990s



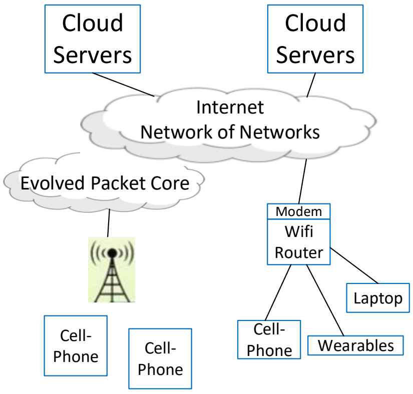
Internet : Personal-Computers, Data-Communications

Centralized
Cellular 3G 2000s
Circuit-Switched Voice
Packet-Switched Data



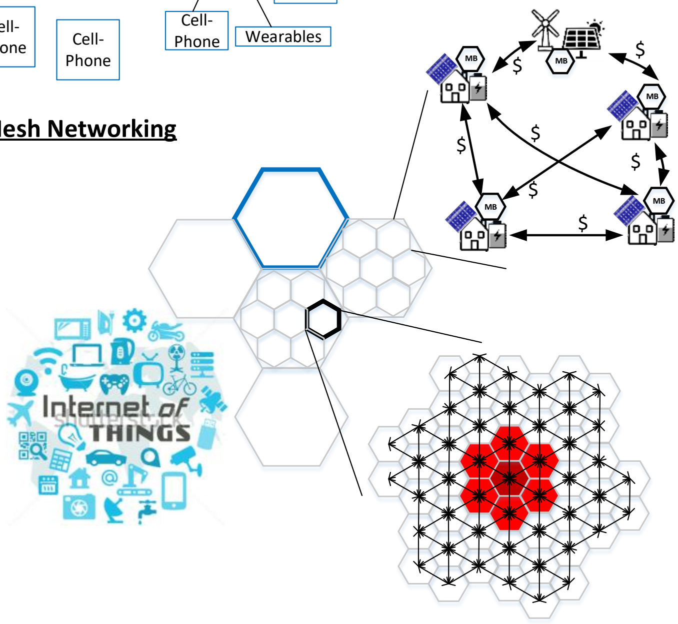
Cloud : Software defined Networking/Computing/Storage

De-Centralized
Cellular 4G 2010s
Packet-Switched Voice
Packet-Switched Data



Hyper-Mesh : Internet of Value with Mesh Networking

Distributed
Cellular 5G 2020s Interoperability
Packet-Switching
Peer-to-Peer Communications
Token-Switching and Blockchain
Transactive IoT
Transactive Energy



3.1 HyperMesh™ Infrastructure and 5G Cellular

In Wireless Communication, the next generation of cellular technology is 5G. Emerging 5G applications and performance Targets include

- ***eMBB*** : Enhanced Mobile-Broadband for high-speed Internet, supported on fast moving vehicles. Dense user support with high data-rates, up to 100x of 4G rates, supporting 10 Gbps within a Small-Cell (about 300 meters radius).

- ***ULLRC*** : Ultra-Low-Latency-Reliable-Communications using 0.1 msec TTI compared to 1 ms TTI in 4G. This is required for self-driving cars, interactive virtual reality, and remote surgery. [WSJ].

- ***Machine-to-Machine*** type communications (IoT)

In order to achieve 10s Gbps data-rates, 5G makes use of New Radio technologies including

- Millimeter-Waves (30 GHz to 300 GHz Spectrum)
- Small-Cell
- Massive MIMO
- Beam-forming and beam-tracking
- Full-duplex

5G extends the wireless spectrum to higher frequencies such as 28 GHz and 60 GHz using millimeter waves. The challenge with such high frequencies is that the range is limited and attenuation through obstacles (including rain or smog) is much more severe. Whereas a 4G macro-cell can cover a 10 miles radius, 5G with high data-rates covers up to 300 meters, and suffers from poor performance in Non-Line-of-Sight (NLOS) deployments.

Thus, to cover a dense urban environment, dense configurations of Small-Cell antennas are needed. Massive-MIMO increases the number of Antenna ports from about 10s to 100s. However, interference is a major problem with Massive-MIMO if signals are broadcasted omnidirectionally. Beam-forming and beam-tracking help to reduce such interference by focusing data-streams to each user. Full-duplex makes more efficient use of the Spectrum by allowing for simultaneous transmission in both directions.

The cost of such New Radio technology is that operators must spend Billions of dollars to license the wireless Spectrum, and also Billions of dollars to deploy the new 5G technologies. For instance, 10,000 Small-Cell antennas are needed, just to cover New York city. This is a large number, compared to the total of 70,000 Macro-basestation cell sites in the entire United States [WSJ].

Wifi is part of the overall network solution for 4G and will also be leveraged in 5G, due to Wifi's low-cost and ubiquitous deployment. However, in the 5G network architecture, Wifi is used only as an access network, to funnel all traffic to a 5G basestation (Small-cell, Pico-cell, Macro-cell), since all of the billing, traffic analytics, and value added services for the operator (over just the basic communications pipe) are done in the basestation and small-cells. In such a network architecture, Wifi meshing is undesirable since local traffic in the Mesh is not seen, and therefore not monetizable to operators deploying the basestations and small cells.

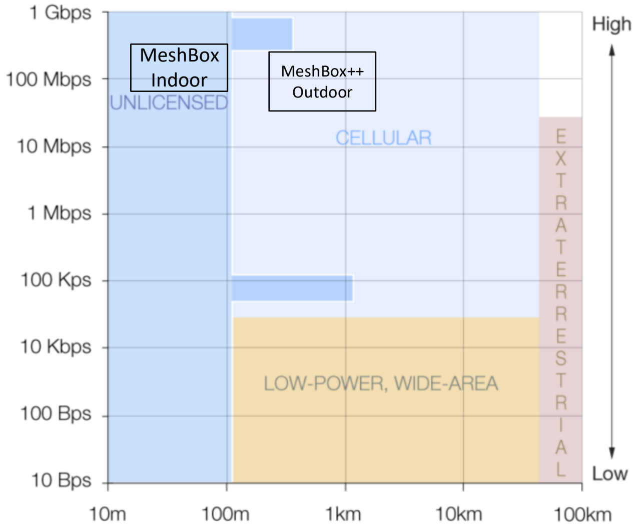
However, Smartmesh® and Meshbox® are bringing a disruption to the convention 4G/5G network architecture by supporting billing, analytics, and value-added services INSIDE THE MESH network. Thus, network operators can deploy Wifi equipment for the Access network, and support many of the functions which were previously supported only in the basestation/small-cell. This allows the operator to dramatically reduce costs for access networks, and still retain the capability to monetize value-added services.

In additional, Smartmesh® and Meshbox® have optimized the mesh network to support new services (much like Cloud RAN), leveraging Smartmesh®'s Spectrum blockchain and Photon Payment network to support electronic-banking and Machine-to-Machine payments; content delivery and encypted data storage (via Inter-Galactic-File-System) using a built-in Disk Drive; and providing gateway functions for LoRa-based IoT networks. Such features are also available even when the MeshBox® Mesh network is NOT connected to the Internet, which is something which 5G cannot support.

MeshBox®es are positioned to cover the vast majority of applications such as web accesses, streaming media, and financial technology. For instance, streaming video accounts for 80% of all internet traffic. MeshBox® supports such streaming media by offering high data-rates, up to 1 Gbps, within a 100-meter to 200-meter radius per MeshBox® for a much lower deployment cost.

5G's strategy is to deploy a Network-of-Networks, and includes technologies such as Millimeter wave, Wifi, Lifi, and 4G, with seamless switching between such technologies. MeshBox® thus complements 5G by providing a cost-effiective solution for Wifi Mesh networks, covering both Indoor and Outdoor sites. In addition, since MeshBox® uses un-licensed Wifi spectrum, deployment cost is much lower than that for 5G, which has to recoup the billions of dollars cost for Spectrum licensing and New Radio equipment somehow.

MeshBox® provides greater geographical coverage and higher bandwidth compared to most Wifi routers with multiple hops and patent-pending low-loss routing algorithms.



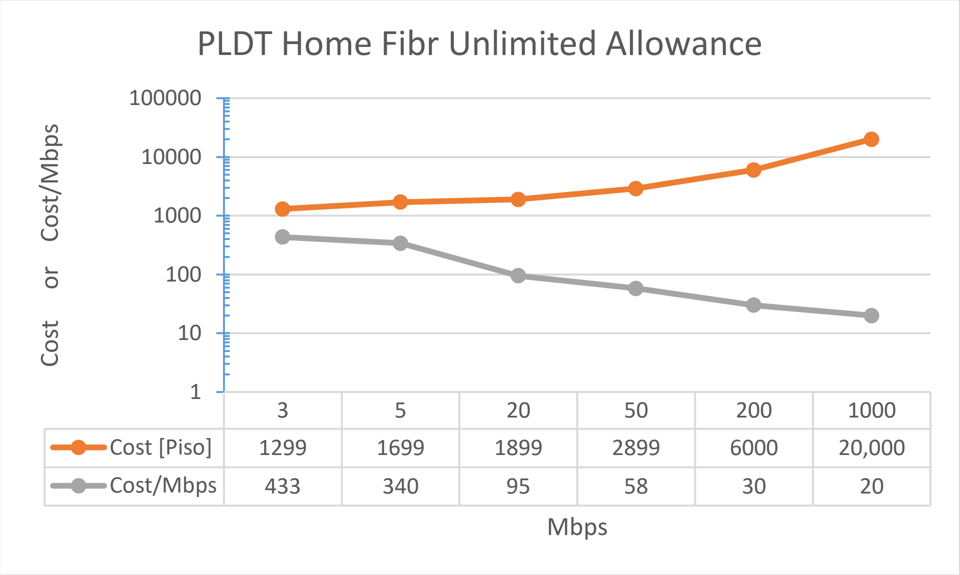
MeshBox®es are also equipped with backhaul internet interfaces including Ethernet (which can connect to various DSL / Coax / Fiber modems, as well as Satellite Dishes), and Cellular networks (via SIM card).

3.2 MeshBox® HyperMeshTM Economy of Scale Benfits

As discussed above, as long one or more MeshBox®es are connected to the Internet, all MeshBox®es in the HyperMeshTM network can share this connection. Thus, the HyperMeshTM network takes advantage of this sharing to leverage Economy-of-Scale benefits.

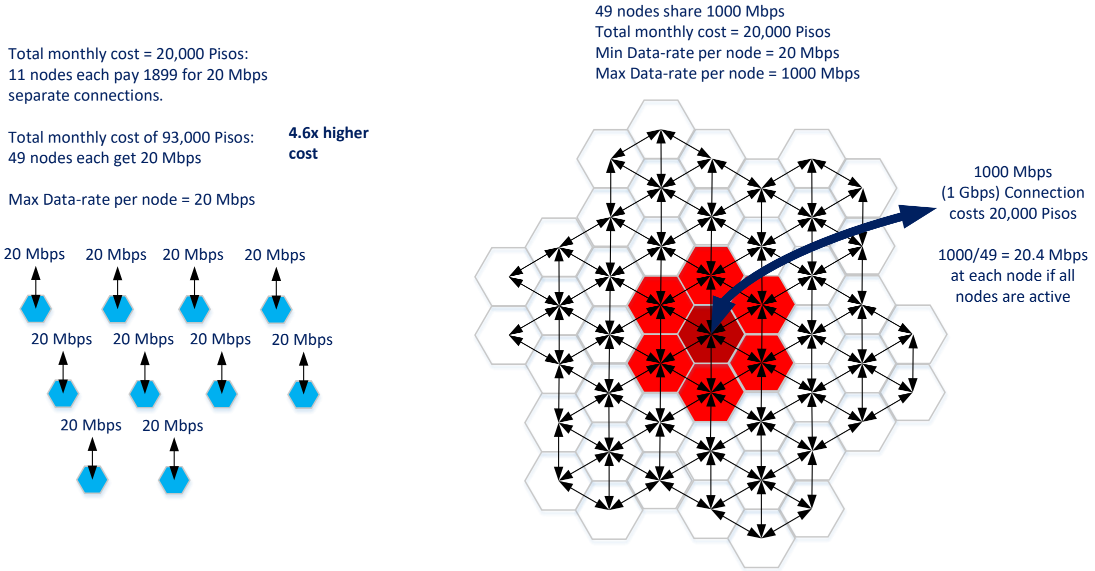
An initial locations for trial network deployment of the MeshBox® HyperMeshTM network include China, Southeast Asia, Africa, and Europe. The economic advantages of deploying a MeshBox® network, as compared to using traditional telecom wireless networks is explored, using a Philippines telecom, PLDT, as an example. PLDT is one of three major Telecoms in the Philippines.

Consider PLDT Home Fibr [PLDT] service plans, plotted below. Note that as in most systems, due to Economy of Scale, the Cost per Mbps declines as the Data-rate [Mbps] increases. For instance, the cost for a single 1000 Mbps connection is only 20,000 Piso, which is approximately equal to the cost 16 separate 3 Gbps connections, which costs 20,784 Pisos (=1299 Pisos * 16) for only 48 Mbps total.



	3	5	20	50	200	1000
Cost [Piso]	1299	1699	1899	2899	6000	20,000
Cost/Mbps	433	340	95	58	30	20

Thus, it is more economical to purchase a high-speed speed connection, and then share it with the entire community, which the MeshBox® network facilitates.


Total monthly cost = 20,000 Pisos:
11 nodes each pay 1899 for 20 Mbps separate connections.

Total monthly cost of 93,000 Pisos:
49 nodes each get 20 Mbps

4.6x higher cost

Max Data-rate per node = 20 Mbps

49 nodes share 1000 Mbps
Total monthly cost = 20,000 Pisos
Min Data-rate per node = 20 Mbps
Max Data-rate per node = 1000 Mbps

1000 Mbps
(1 Gbps) Connection
costs 20,000 Pisos

1000/49 = 20.4 Mbps
at each node if all
nodes are active

For a 49 node MeshBox® H(4) Domain, a high-speed link (such as 1000 Mbps) to the Internet can be provisioned with a Gateway MeshBox® in the middle (which is connected to the Internet).

Then, the 49 nodes can share the bandwidth using the Mesh Network, with each Node receiving about 20 Mbps of service (=1000/49) for a total cost of 20,000 Piso's per month, plus the CAPEX cost for 49 MeshBox®es. This translates to 409 (=20,000 / 49) Pisos for each 20 Mbps of service at each MeshBox®.   Compare the 409 Pisos to 1899 Pisos for a 20 Mbps connection from PLDT to understand the significant cost savings due to Economy of Scale.

Similarly, to buy 49 connections of 20 Mbps each, the total cost would be 93,000 Pisos, compared to the single 1000 Mbps connection which costs only 20,000 Pisos.

The CAPEX cost for the 49 MeshBox®es must be considered. However, since the operation of MeshBox®es provides the owners with tokens, which can be converted to Fiat currency, the cost of the 49 MeshBox®es is re-couperated after several months, to a year, so this CAPEX cost is returned to the owners.

4. HyperMesh™ Highly Scalable Network Architecture

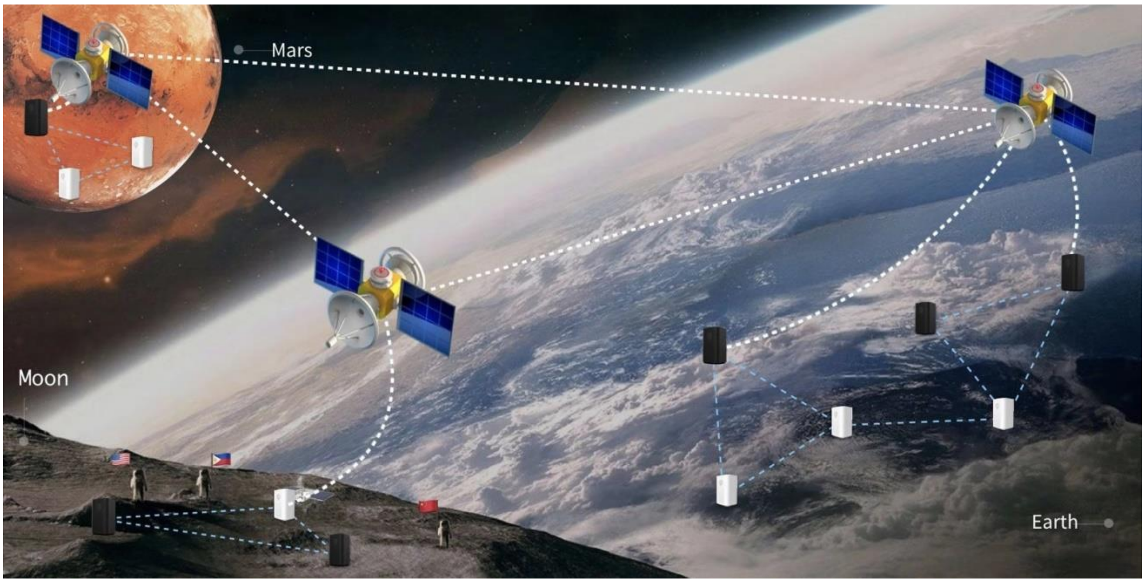
MeshBox®es are engineered to interoperate with other technologies in order to form a highly scalable HyperMesh™ Infrastructure.

- Wide-Area-Network (WAN) technologies, optimized with large-area WiFi meshed communications spanning both indoors and outdoors.
- Space-Ground-Integration-Network (SGIN): Economy of Scale benefits using high-bandwidth satellite links, connected to low-cost ground-based Wifi Mesh networks for localized, last-mile deployment, even to far-flung locations and developing countries.
- Fintech applications for blockchain and payment networks to bank the unbanked.
- Transactive Energy applications layered onto the HyperMesh™ network, leveraging Blockchain applications.
- Interworking with LoRa and Narrow-Band IoT (NB-IoT) technology for IoT connectivity, covering a wide-area, with low-power, but with low bandwidth.

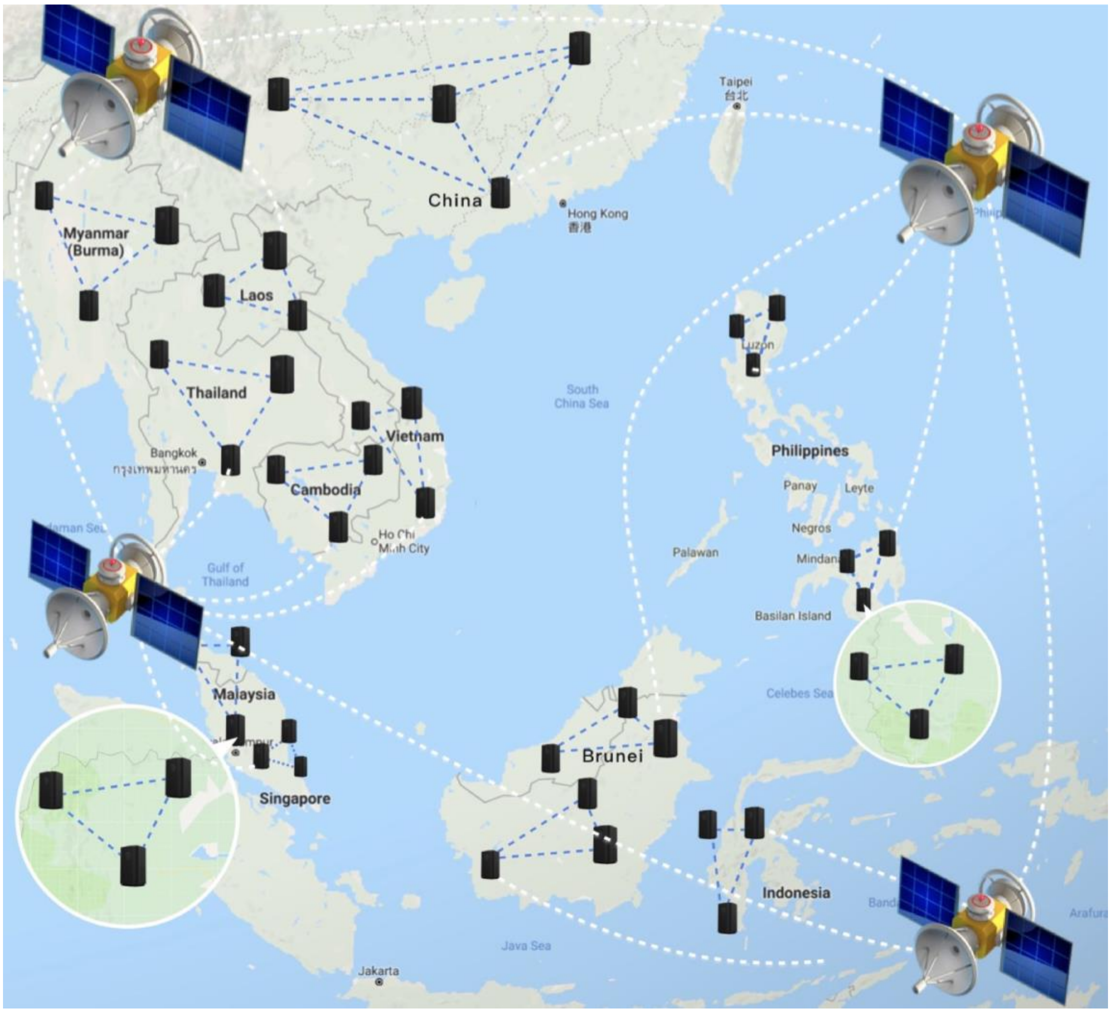
The following shows a Fractal architecture which is used to scale the HyperMesh™ architecture. Scalability spans from the lowest-level Domain of IoT devices, all the way to a Universal Domain.

The hierarchical levels are defined as follows:

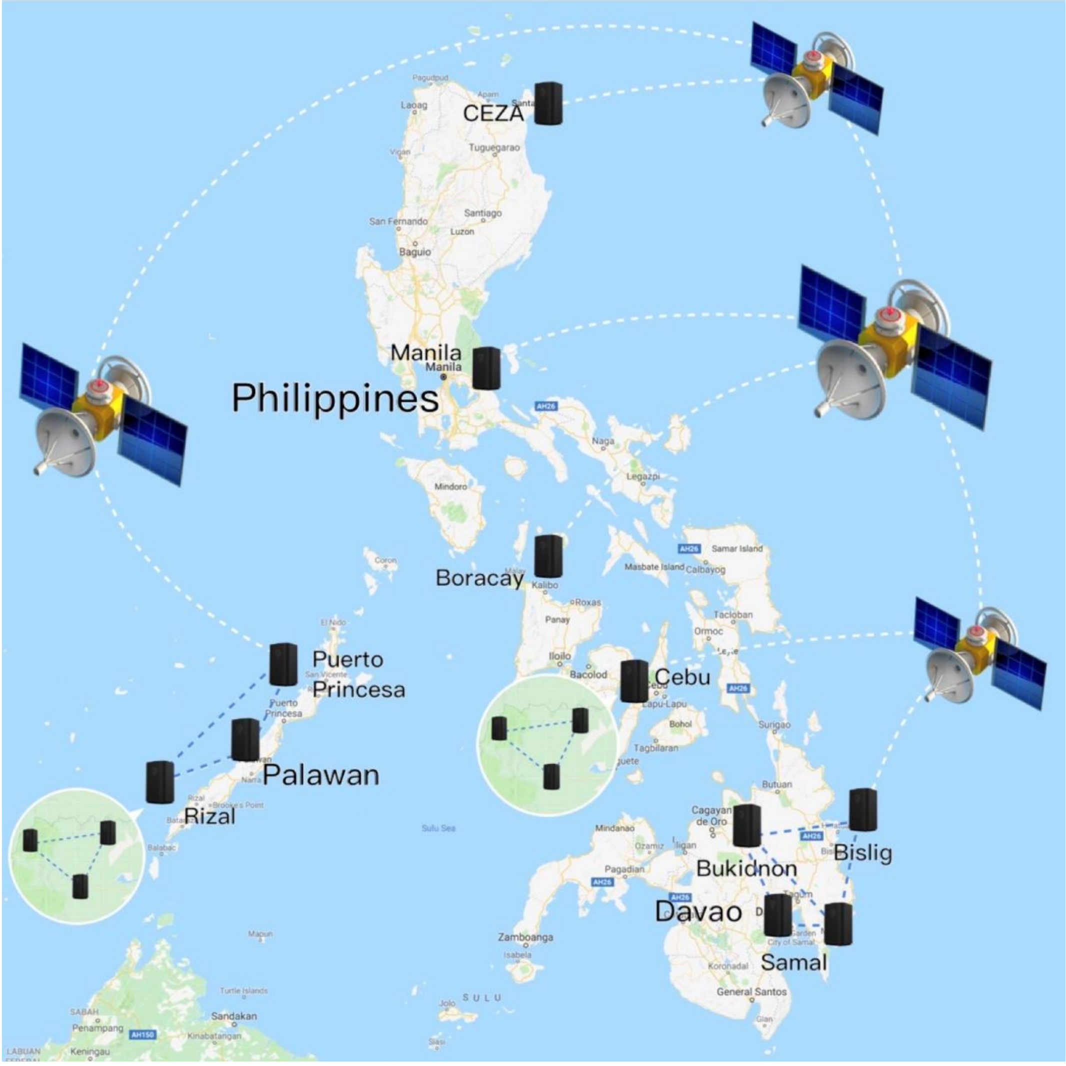
- H(11) = Universal Domain = Domain which spans to beyond the Earth, including networks to the Moon, Mars, and beyond.



- H(10) = International Domain = Span multiple countries. For instance, as shown below, China and the Association of South East Asian Nations (ASEAN) countries: Philippines, Indonesia, Brunei, Malaysia, Myanmar, Laos, Vietnam, Cambodia, Thailand, and Singapore.



- H(9) = Country Domain = Spans a Country, such as the Philippines, shown below.

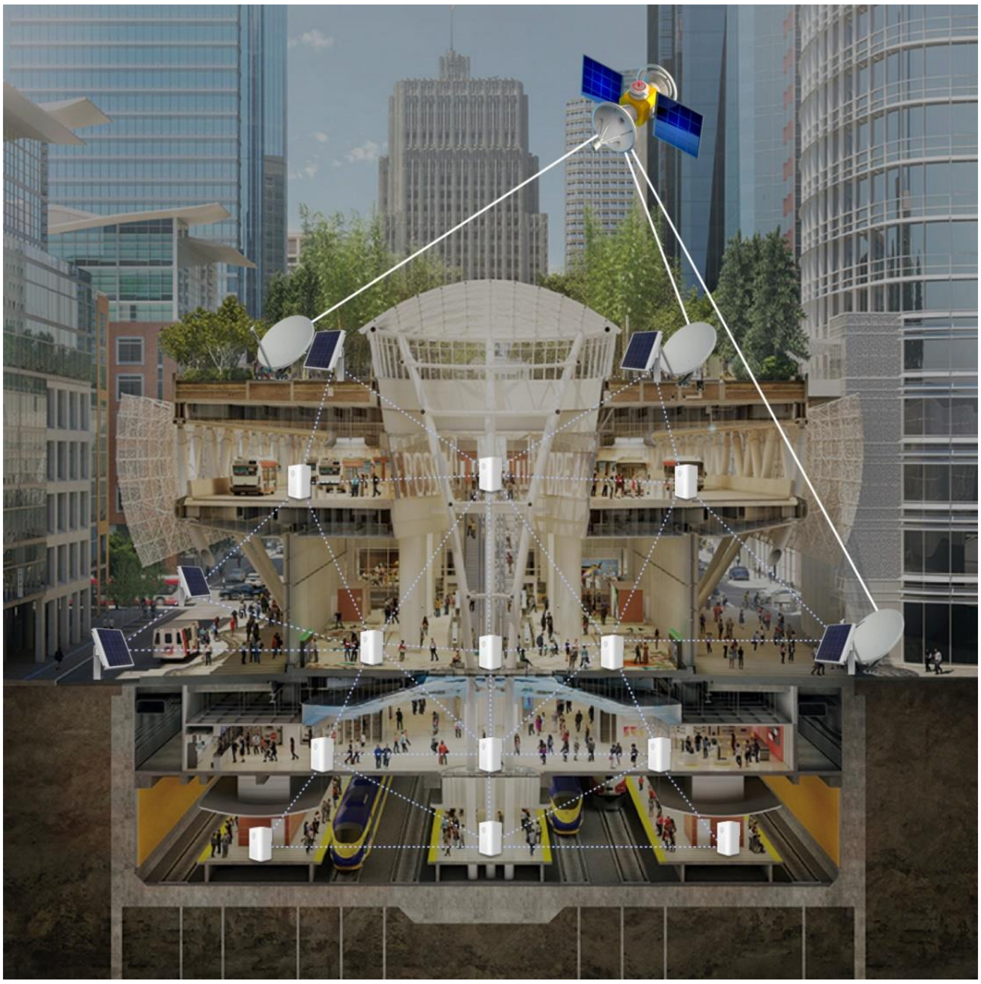


- H(8) = Region Domain = Spans Region (State or Province)
- H(7) = City Domain = Spans a City or Village
- H(6) = Community Domain = Spans a community within a City
- H(5) = Outdoor Domain using MeshBox++TMes = Spans a Community, which can be a block or a group of buildings managed by one entity, or jointly owned by a community.
- H(4) = Building Domain using MeshBox®es = Spans a building (or several inter-connected buildings)
- H(3) = Single MeshBox® Domain
- H(2) = Smart IoT Domain : IoT Access Points, Smartphone
- H(1) = Basic IoT Domain : IoT Terminals

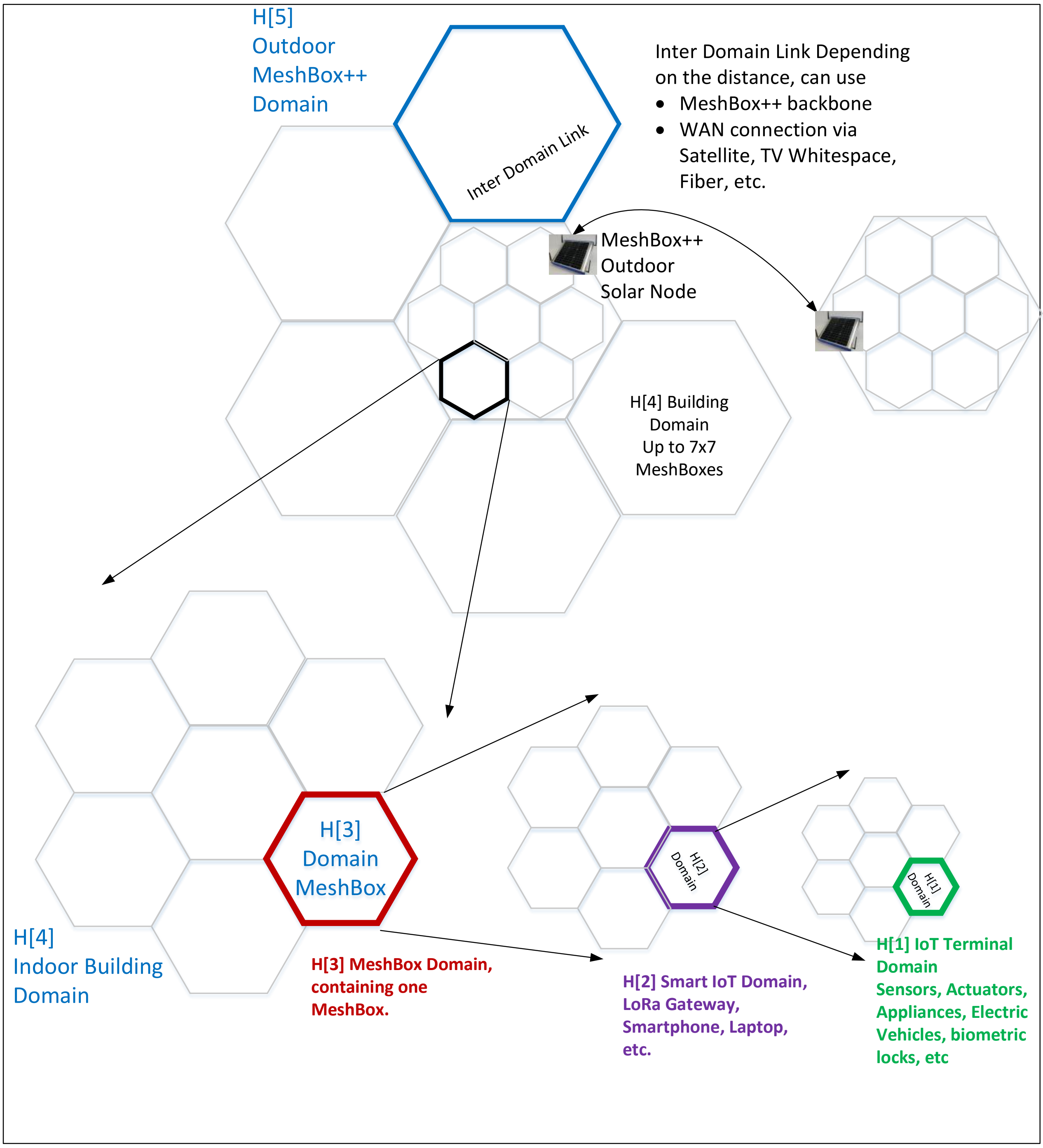
Satellite and WAN Internet can be used at hierarchy levels H(11) down to H(4), while the MeshBox®-based Mesh networks can cover from H(7) down to H(1).

Satellite Internet, Smartmesh® and Meshbox® technology are synergized through the following:

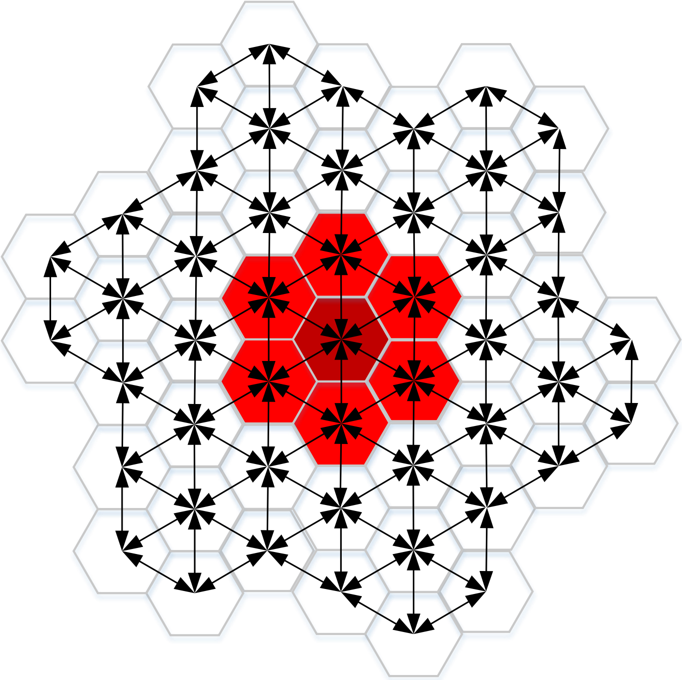
- Satellites provide world-wide internet coverage, which is especially useful for non-urban, islands, rural, in-accessible, on-sea, and in-air locations.
- Satellites can use fewer, higher-speed Satellite links, connected to fewer MeshBox®es on the ground.
- MeshBox® ground-based Mesh-networking to provide high-bandwidth, high-density, local coverage, for both Indoor and Outdoor coverage.
- MeshBox® scales the Satellite data-rate significantly through the use of Edge computing, Edge storage (caching), leveraging time-locality and space-locality of content accesses.
- Mesh network covers Non-Line-of-Sight (NLOS) locations, which Satellite signals do not cover well, due to higher carrier frequencies providing higher data-rates, but more susceptible to attenuation from physical obstacles.



In the figure below, the Hierarchies from a Building Domain (H[4]) down to an IoT domain (H[1]) are shown.



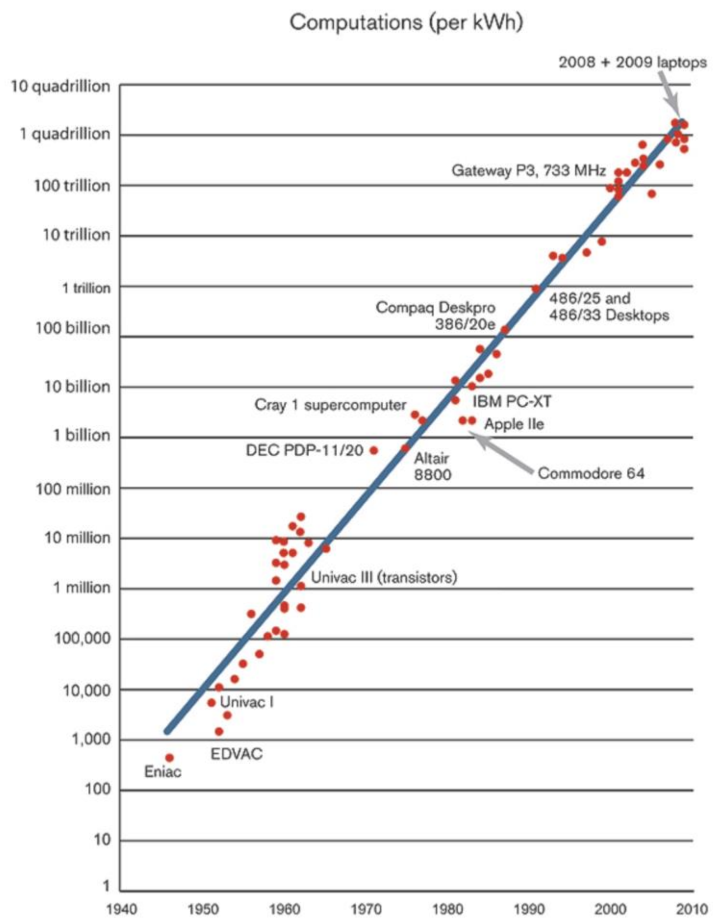
Each Hierarchy Domain is shown with 7 Sub-Domains. However, the number of such Sub-Domains can be up to 49 (=7x7) as shown below.



On such a Fractal network architecture, various networks are overlaid, including communication, Photon™ peer-to-peer payments, Wormhole Universal Channels™ for multi-blockchain token exchange, Energy Internet (Enernet), etc. The exchange of various tokens, both fungible (monetary) and non-fungible (non-monetary, cyber-physical), are supported.

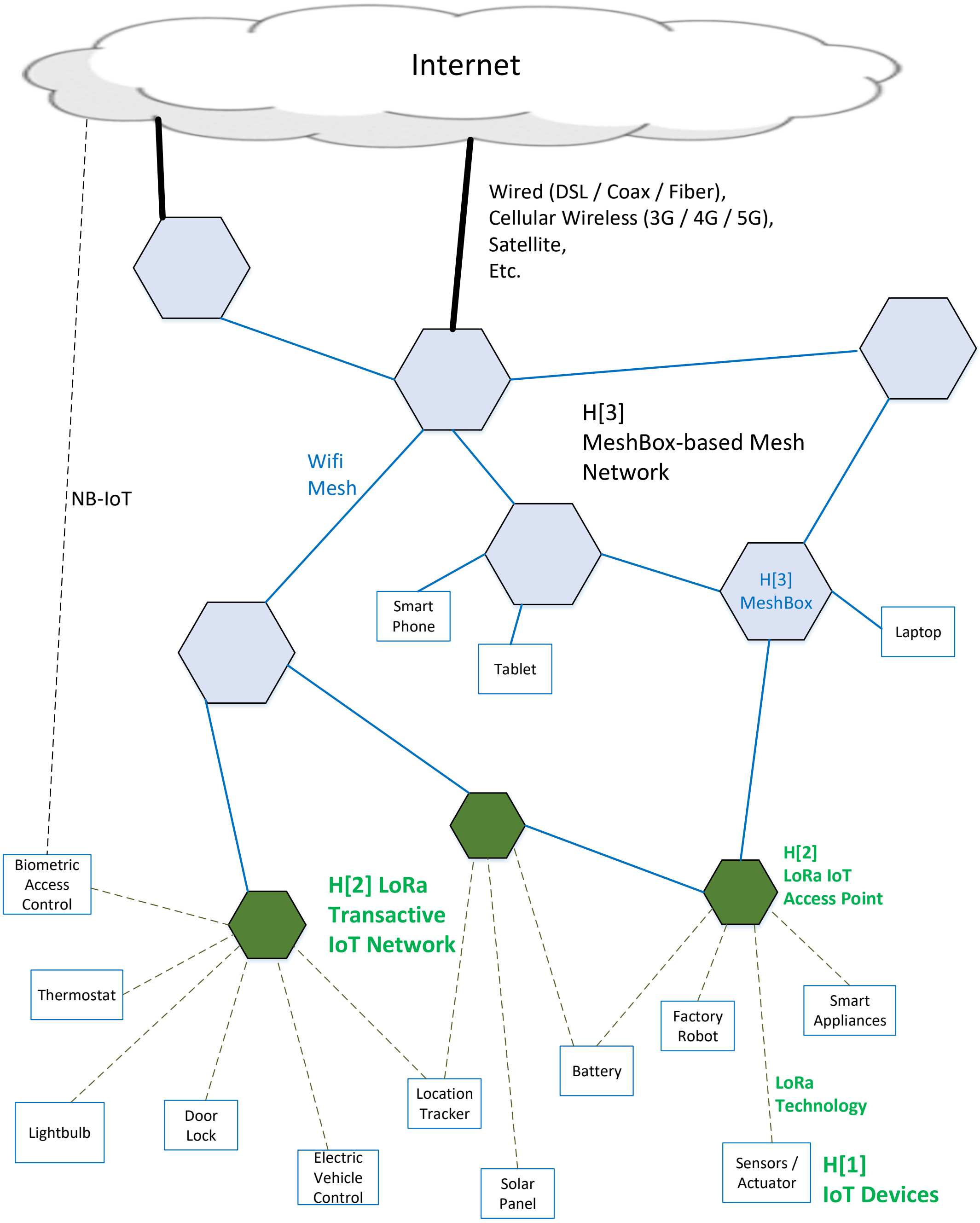
At the lowest Hierarchy levels of the HyperMesh™ network, is the coverage of IoT devices. The proliferation of IoT is driven by energy-efficient computing, which leverages the following technology trends.

Following Moore's law, transistor count on an Integrated circuit doubles every 2 years for the same cost. Data Storage prices drop by 1/10 every 5 years. In Energy Efficient Computing, the energy needed to perform a task requiring a fixed number of computations will continue to fall by half every 1.5 years (or a factor of 100 every decade), as illustrated by the graph below [EEN].



The above shows that IoT devices will proliferate since computing and communication will be so cheap that they can be embedded into everyday items with little energy draw.

One technology which is well suited for IoT is LoRa Technology, and is being integrated into the HyperMesh™ architecture with MeshBox® as a gateway between the Internet and the IoT world, as shown below.


Internet
Wired (DSL / Coax / Fiber),
Cellular Wireless (3G / 4G / 5G),
Satellite,
Etc.
H[3]
MeshBox-based Mesh
Network
Wifi
Mesh
NB-IoT
Smart
Phone
Tablet
H[3]
MeshBox
Laptop
Biometric
Access
Control
H[2] LoRa
Transactive
IoT Network
H[2]
LoRa IoT
Access Point
Thermostat
Lightbulb
Door
Lock
Electric
Vehicle
Control
Location
Tracker
Solar
Panel
Battery
Factory
Robot
Smart
Appliances
LoRa
Technology
Sensors /
Actuator
H[1]
IoT Devices

5. MeshBox® Token Distribution plan

There are several Stakeholders involved in deploying a HyperMesh infrastructure, which uses MeshBoxes as a fundamental building block. Such Stakeholders have several lucrative ways to earn revenue through rewards for providing services to the community. These include

(1) The MeshBox HyperMesh Investor (MHI) pays for some of all Capital Expenditure (CapEx) of the MeshBox itself.

(2) MeshBox Business Channel Partners are sellers or re-sellers of MeshBoxes, such as distributors in particular countries or regions.

(3) The MeshBox Local Operator (MLO) maintains the MeshBoxes in the HyperMesh, and pays for the Operational Expenditures (OpEx) costs. MLOs can be a Telecom, Internet service provider, or even local merchants. Such costs could include installation, maintenance, warranties, and insurance (in case of theft).

(4) Deployment venue, which are businesses (Micro, Small, and Medium Enterprises (MSME)), public areas, or residences, which host the MeshBox, and run applications to generate revenue and provide services to their community. Such businesses may pay costs such as electricity, and security for the MeshBoxes.

There are two main types of networks which are supported by MeshBox:

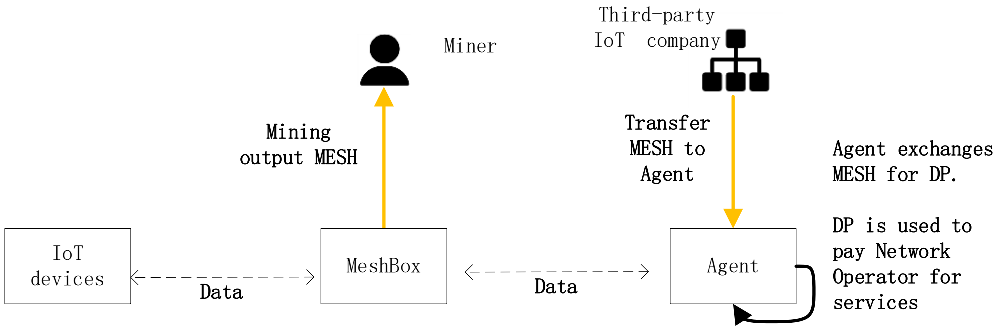
- Wireless Broadband Networks, which support high data-rate, at higher power requirements, and with limited geographic are of coverage (few hundred meters omni-directional). The current network which MeshBox supports is Wifi Mesh, with various Internet backhaul interfaces.
- Wireless Narrowband Networks, such as Low-Power WAN (LPWAN) networks, which support low data-rate, but a larger geographical area of coverage (several kilo-meters omni-directional). The current such network supported are LoRaWAN Access Points, which can be stand-alone machines, or integrated into MeshBox in a miniPCIe board form-factor.

There are three types of machines in an IoT application: IoT devices, MeshBox and Agent.

- **IoT devices**: communicate with MeshBox through wireless networks such as Lora or WiFi, and send or receive data to the Internet.
- **MeshBox**: Provides wireless Access Network, through Wifi, to various Internet Backhauls. Can connect to; or integrate internally, a LPWAN Access Point (such as LoRaWAN). For LPWAN applications, MeshBox supports the transport of data between IoT devices and Agent.
- **Agent**: A software application deployed on the Internet. An Agent receives data from IoT devices through a network of MeshBoxes and routes them to their corresponding destinations (where the data is processed).

A MeshBox Local Operator (MLO) deploys one or more MeshBoxes, and earns MESH rewards. The MLO thus becomes a Miner, by deploying MeshBox to participate in network construction and data transport. Third-party IoT application companies, which want to collect the IoT data, exchange MESH for Data Points (DP) which is a pre-paid amount. Users use DP to pay for MeshBox services such as receiving and sending IoT data. The transaction for DP payment uses a pre-paid mechanism, in which the IoT Application company pays upfront for the "Load"on their account, which is then deducted as IoT transport services are used to transport such IoT data to the intended destination.

The MESH tokens, which the IoT Application companies pay, are then deposited to the MeshBox's wallet account, which can be transferred to the stakeholders as a reward and ROI.



MeshBox provides the following services to the community, which generates ROI for the stakeholders.

- MeshBox nodes use Wi-Fi and WiFi Mesh to provide users with Internet services which will receive a certain number of Token (MESH) rewards. If users share their own broadband at the same time, they will also receive a part of Token (MESH) rewards.
- MeshBox nodes use Lora/NB-IoT to provide users with IoT services which will receive a certain amount of Token (MESH) rewards.
- MeshBox nodes contribute hard disk space and caches data resources to the entire network system, which will get MeshBox Token (MESH) rewards corresponding to MeshBox.

REMOVE THE FOLLOWING:

The total number of Mesh tokens to be issued is 10 billion, and will stay constant. The allocation will be as follows.

Mesh Allocation	**% MESH Allocated**
Mining (for MeshBox Owner or Operator)	40 %
MeshBox Foundation Holding	15 %
Marketing (partly for Exchange)	7 %
Team Rewards (MeshBox Employees)	10 %
International Standard Setting	3 %

Pre-sale and Private Equity Investment (partly for Exchanges)	20 %
Advisors	5 %

MESH will be issued on the SmartMesh Spectrum Blockchain in the form of ERC20 tokens.
The specific distribution rules are to be determined by the SmartMesh Foundation.

5.1 MESH Introduction

5.1.1 MESH Overview

MESH network has designed three tradable symbols, digital currency

- MESH token : A utility token on Spectrum with gas fees paid in SMT
- Narrowband Data Points
    - (previously called: NDP (Thing Data Point))
- Broadband Data Points
    - (previously called: BDP (Internet Data Point)).

5.1.2 What MESH Is Used For

MESH is a digital token, which can be transacted between parties through the Spectrum Blockchain. MESH is can also be used to purchase DP (Data Points).

5.1.3 How To Obtain MESH

(1) Purchase MESH from other MESH holders

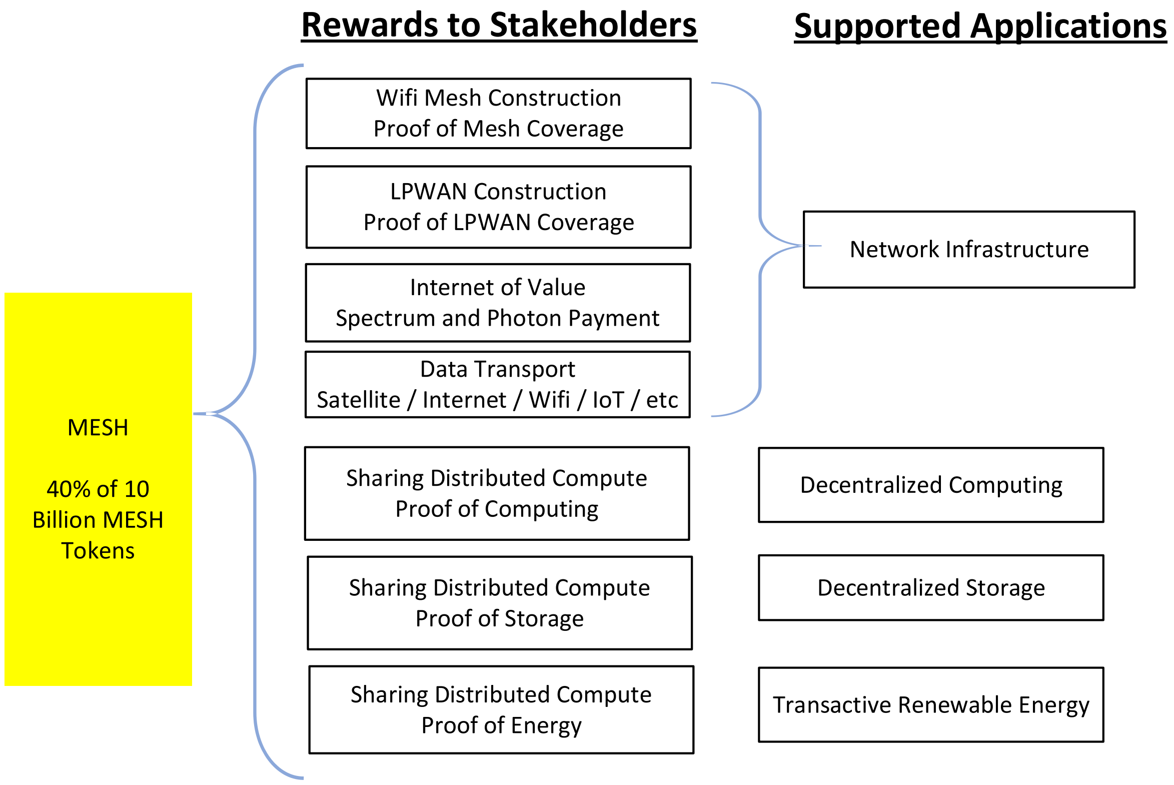
(2) After purchasing a MeshBox, the MeshBox operator can mine MESH tokens by operating the MeshBox, which participates and verifies the MeshBox Wifi mesh network coverage. Also, when MeshBox is co-located, or has an integrated LPWAN Access Point (e.g. GTI LoRaWAN miniPCIe board), MeshBox also participates and verifies LPWAN IoT network coverage.

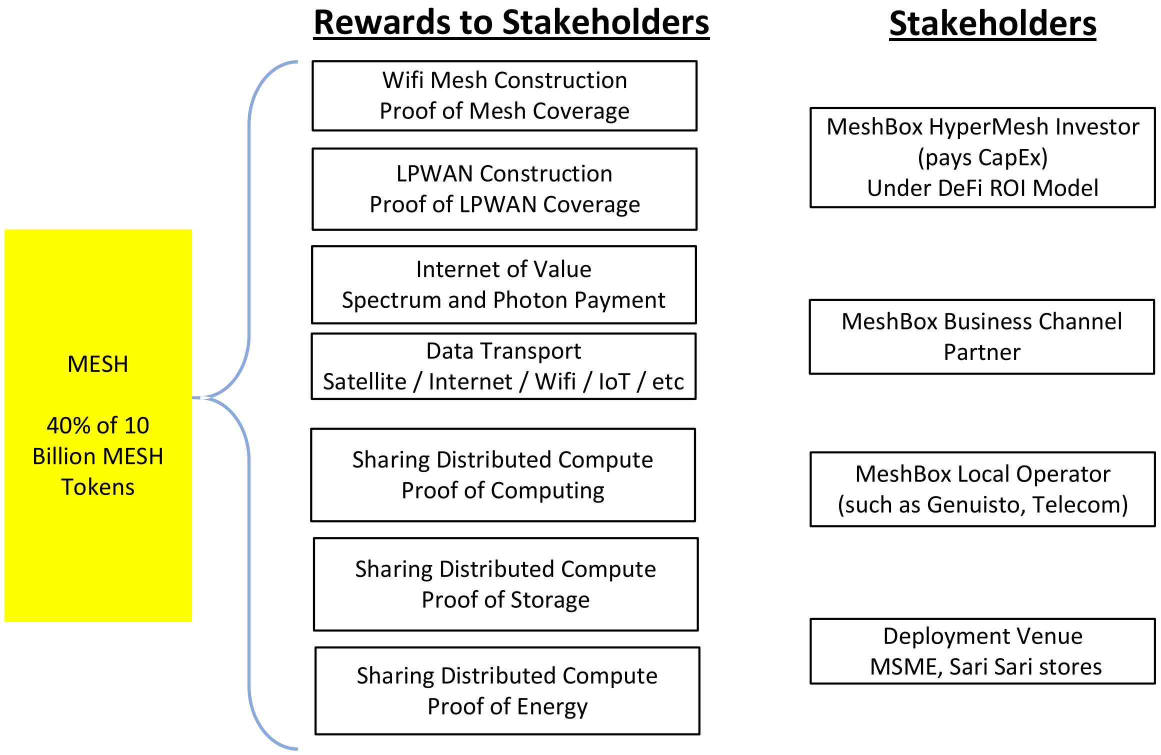
(3) The MeshBox Local Operator can also run applications on the MeshBox which provides distributed computing and distributed data storage resources to users connected to the Mesh Network. In return, the MLO earns additional MESH tokens.

5.2 MESH Mining

5.2.1 MESH Reward

The total number of MESH token issued is 10 billion, 40% (= 4 Billion Total) of which is used for mining rewards. These rewards are further divided into the following parts:




Rewards to Stakeholders
Stakeholders
MESH
40% of 10 Billion MESH Tokens
Wifi Mesh Construction
Proof of Mesh Coverage
LPWAN Construction
Proof of LPWAN Coverage
Internet of Value
Spectrum and Photon Payment
Data Transport
Satellite / Internet / Wifi / IoT / etc
Sharing Distributed Compute
Proof of Computing
Sharing Distributed Compute
Proof of Storage
Sharing Distributed Compute
Proof of Energy
MeshBox HyperMesh Investor (pays CapEx) Under DeFi ROI Model
MeshBox Business Channel Partner
MeshBox Local Operator (such as Genuisto, Telecom)
Deployment Venue MSME, Sari Sari stores

Network Construction Rewards

Network (including Wifi and LPWAN) construction rewards means that MeshBox autonomously participates in, and verifies the Wifi coverage of the MeshBox network through the Internet coverage certification protocol. Therefore, the rewards obtained are called Internet construction rewards, and the rewards are distributed to the owners of MeshBox.

Data Transport Rewards

Data transmission (including Wifi and LPWAN) rewards refer to the rewards that MeshBox receives for providing Data communication services, with the reward amount depending on the amount of data transmission. The rewards are distributed to the owner of MeshBox.

Storage Sharing Reward

Storage sharing rewards means that MeshBox gets rewards for sharing storage space, and the rewards obtained are related to the size of the shared storage space. The rewards are distributed to the owner of MeshBox.

Computing Power Sharing Reward

Compute power sharing reward means that MeshBox gets rewards for sharing computing power, and the rewards obtained are related to the shared computing power. The rewards are distributed to the owner of MeshBox.

6. MeshBox® Proof of HyperMesh Connectivity

SmartMesh Foundation and MeshBox Foundation is developing a Proof of HyperMesh Connectivity protocol, based on the Spectrum blockchain, Mesh side-chain, MeshBox-based Wifi Mesh network, LPWAN, and Space-Ground Integration Networks. The end goal is to deploy a solution for inclusive Internet connectivity.

Some of the Proof of HyperMesh Connectivity architecture is borrowed, with thanks, from the Helium Proof of Coverage mechanism [Helium], which is a decentralized protocol to secure IoT data transport against Sybil and alternate reality attacks.

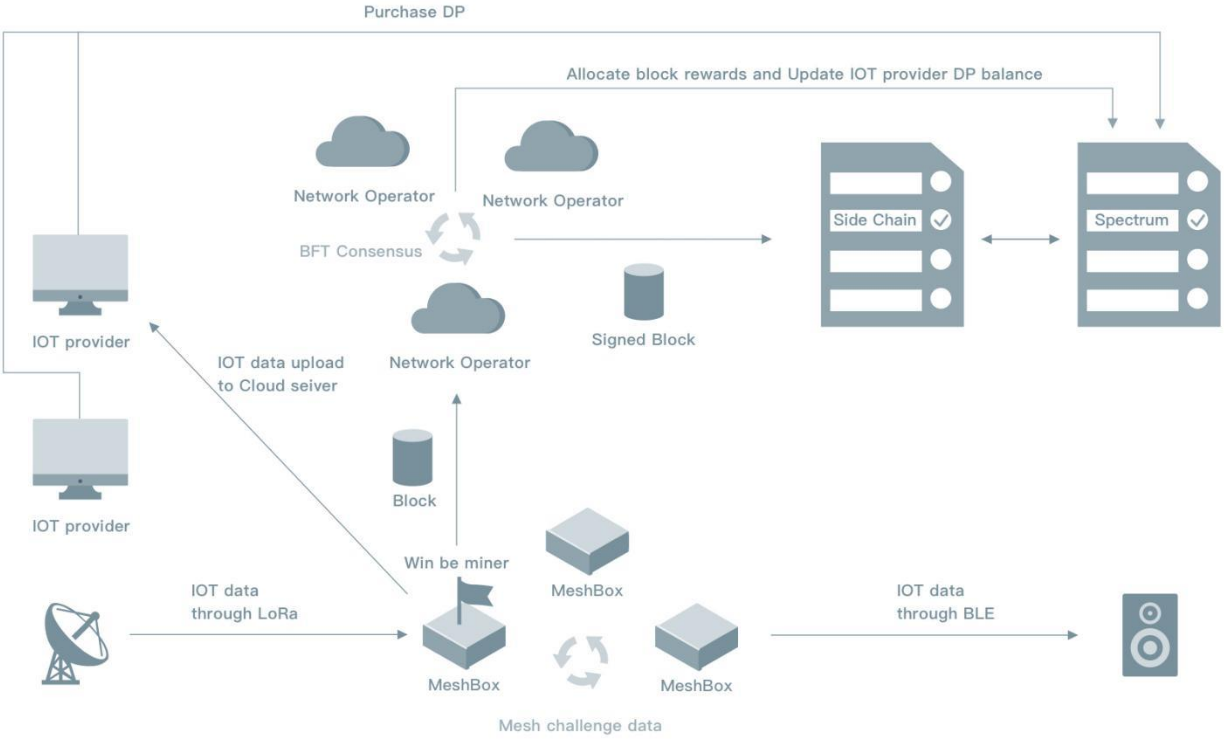
6.1 Proof of HyperMesh Connectivity Overview

MeshBox implements both Wifi mesh router and LPWAN Access Point technologies as follows.

- LPWAN (LoRaWAN from Ecosystem Partner GTI) with miniPCIe Access Point card integrated into MeshBox.
- Wifi Mesh with various Internet backhauls (RJ45 Ethernet modems including satellite, 4G Cellular SIM)

In terms of blockchain technology and tokens, the HyperMesh uses the following.

- Spectrum public blockchain with publicly traded SMT tokens.
- MESH tokens as rewards for MeshBox-provided services.
- Mesh side-chain from Spectrum main-chain.
- MESH tokens exchanged for Broadband/Narrowband Data Points, which are then used to pay for transport services.



In order to build a HyperMesh network with wide-area coverage; simplify the connectivity between people, between people and machines, and between machines; and reward MeshBox owners by providing various services, a Proof of HyperMesh Connectivity is being developed. This is composed of two parts:

- Proof of LPWAN (focusing on LoRaWAN) coverage or Proof of LPWAN
- Proof of Wifi Mesh coverage (referred to as Proof of Mesh coverage, or Proof of Mesh)

MeshBoxes which participate in the two-level Proof of HyperMesh Connectivity protocol will be rewarded with MESH tokens by providing correct and verifiable proofs, which provides a steady source of ROI for the stakeholders.

Proof of HyperMesh Connectivity, by MeshBoxes, is secured by a side-chain to the Spectrum Main-Chain. The Mesh Sidechain is a new blockchain, implementing a type of BFT consensus, with the Proof of HyperMesh Connectivity consensus mechanism. The Mesh side-chain tracks and secures the Proof of HyperMesh Connectivity protocol information and the communication of related consensus verification data.

The transactions (sending and receiving) of MESH tokens are not carried on the Mesh side-chain, but, rather are all done on the Spectrum main chain

Two tokens are introduced on the Spectrum main-chain.

- **Narrowband Data Points (NDP)** Points are used by IoT applications to pay for IoT Data traffic fees. NDP can only be purchased using MESH and cannot be traded. NDP is anchored to the U.S. dollar.
- **Broadband Data Points (BDP)** are used for Internet users to pay traffic fees. BDP can only be purchased through MESH and cannot be traded. It is only available to the buyer. BDP is anchored to the U.S. dollar.

6.2 Proof of LPWAN Coverage

The Proof of LPWAN coverage is mainly used to verify whether the MeshBox, with the integrated LPWAN Access Point (developed by GTI IoT Technologies), at a certain location is providing a certain level of LPWAN RF coverage for IoT devices.

The ability to prove whether MeshBox has carried out LPWAN coverage is based on the following characteristics (as also stated in [Helium]) :

(1) Radio frequency (RF) propagation distance is limited
(2) In the first-order (i.e. simple line-of-sight scenarios), the strength of the received RF signal is inversely proportional to the square of the distance from the transmitter
(3) RF propagates at nearly the speed of light (in air)

The Proof of LPWAN coverage will be stored on the Mesh Sidechain, and the wireless coverage of its location (GPS) will be verifiable by miners with certainty to confirm its authenticity, and generate rewards for the Stakeholders.

6.2.1 Participants in Proof of LPWAN Coverage

The following algorithm for Proof of LPWAN Coverage borrows heavily from [Helium] and is essentially an interactive Challenge protocol. During this Challenge, there are three main types of participants

(1) Challenger: An independent MeshBox node that can create a Proof, which is submitted to to the Mesh Sidechain consensus miners group for verification. Challengers will be rewarded for submitting valid challenges. Currently, each MeshBox node can submit a challenge every 30 blocks (a time period of the sidechain).
(2) Target: Any MeshBox node (also referred to as the “challenged”) selected to respond to the challenge is called the Target. In each challenge, considering the efficiency and cost, the number of Targets should be between three and seven. These Targets must be located in close proximity each each other, geographically, so they can communicate with each other through RF. At least one Target can be connected to each other, otherwise it is impossible to effectively carry out the RF broadcast to transmit the Challenge data. To

prevent collusion, the Challenger and the Target MeshBoxes must not be in the same geographic area.

(3) Witnesses: At any stage during the challenge, adjacent MeshBox nodes (witnesses) in the same proximity can also receive the broadcasted RF data, and help validate that the challenge data has been received and broadcasted by radio frequency signals, which indirectly proves the coverage.

The Proof of LPWAN Coverage, implemented in the form of a Challenge protocol is realized by the interaction between MeshBoxes playing one of the three roles above. The goal is for the Challenger to obtain the Proof of Mesh coverage by the Targets, through an interactive protocol, in which the entire process can be reconstructed and verified by other miners in the consensus set.

6.2.2 Construction of Challenge Proof

The Challenger can challenge multiple Targets at once (under the premise that they are connected through the LPWAN protocol).

The Challenger builds a multi-layer data packet, the Challenge packet, which is transferred to the multiple Targets to be challenged, and confirms that multiple Targets have covered the LPWAN operation area by receiving feedback packets (point-to-point).

Since the Challenge requires multiple interactions, conditions for the Challenge are pre-set for efficiency.

The Challenger and the Target must not in the same geographical LPWAN RF area (Target is not reachable from Challenger via LPWAN RF). In this case, the Challenge packet is sent to the first Target via the internet.

The Challenge packet is layered and encrypted, in the form of "envelope within an envelope" (similar to onion routing). Except for the first Target, other Targets do not know their own layer, and can only decrypt data at their own layer. The first Target can only decrypt the outermost layer.

For each Challenge packet layer, a Target, after decrypting the data belonging to its own layer, will sign a receipt, record the time and signal strength of the received RF, and feedback this information to the Challenger through the Internet. The Challenger combines the received receipts in order to construct the Proof for the Targets.

Witnesses play a role starting at the second Challenge packet layer, because there is no RF broadcast corresponding to the first layer. The witnesses cannot decrypt the Challenge packet at any layer, but can receive the RF broadcast Challenge packets. Witness can thus re-simulate the entire Proof of LPWAN coverage process, verify the signed receipts by each of the Targets, sign the recorded time and signal strength, and feed back the Witness data to the challenger.

The Challenger selects the Witness Proof of the corresponding layer according to the statistical witness list (available from the GPS information on the Mesh side-chain). Such Witness protocol information are combined by the Challenger as Witness Proofs. The proofs from the Targets and Witnesses are combined to form a complete challenge proof.

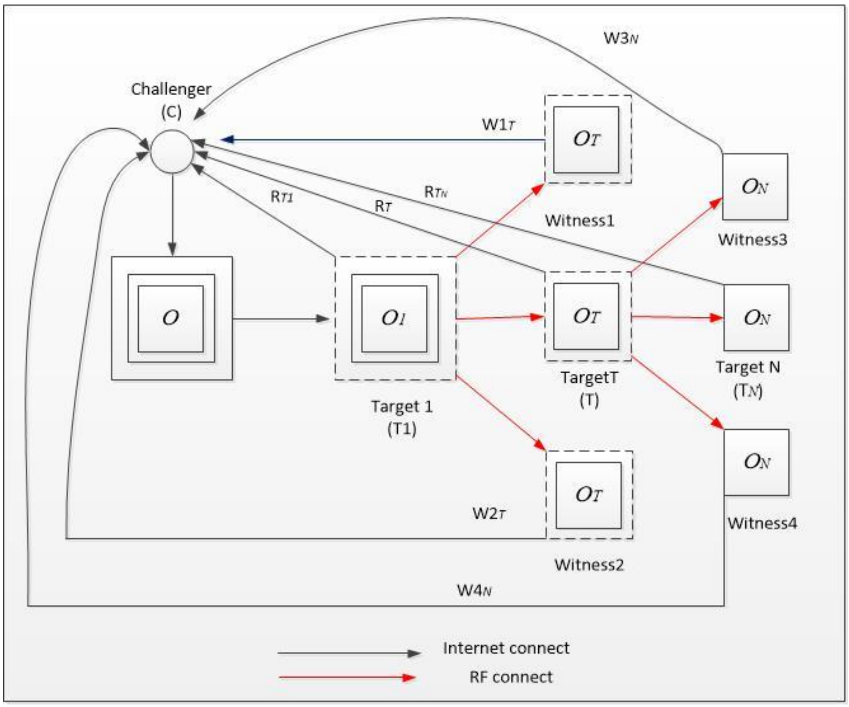


Figure: Multi-layer Challenge packet construction

In the above construction process, choosing the intended Target (center) is the starting point of the construction. Determining the intended Target is equivalent to determining an RF coverage area. A Target in this area may be selected to challenge.
The choice of intent Target T has the following considerations:

(1) It is necessary to construct a probability distribution of trusted of MeshBox nodes, and give each node a Trust score according to the Challenge. Meshbox nodes with low scores have a higher probability of being selected as Targets, which also gives such nodes a higher chance to improve their trust scores by participating in the Challenges. Nodes that first join the network are given an initial score of 0.25, with the score ranging between 0 and 1. The score will dynamically decrease and increase with time and participation in Challenges. The Challenger with the highest score may participate in the consensus group to verify the challenge.

If a score drops below 0.15, then such nodes cannot challenge, but can be challenged. Only nodes with a Trust score of 0.15 or more are eligible to challenge other Nodes, in order to minimize the interference of the dishonest node to initiate challenges.

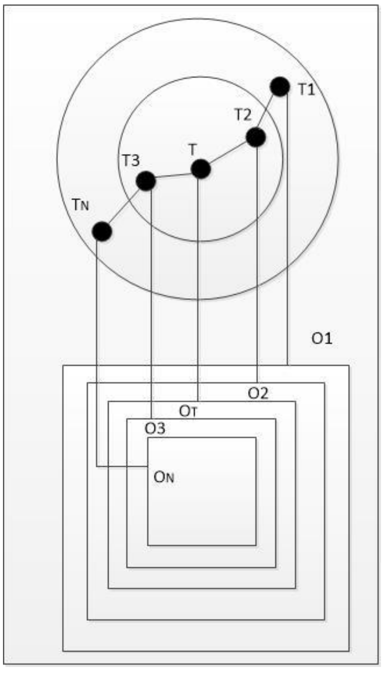
(2) A verifiable entropy is required. The preliminary plan is to use the Challenger's temporary public key and the block hash accepted by the challenge request. Thus, Entropy = Secret + block hash. Then, the Challenger generates a random number from this entropy value, combined with the score from the probability distribution, and selects the initial Target (followed by the set of other Targets in the proximity.

The Target selection process, determined according to the above conditions, can be deterministically reproduced by other miners, so the determination of the Targets is repeatable.

6.2.3 Constructing a Multi-Layered Challenge Packet

Although we have determined the intentional Target through the combination of conditions, a single Target does not enable us to obtain proof of the coverage of the Target. It is necessary to confirm that the true coverage is achieved through interactive feedback between the Target and other MeshBox nodes. As in real life, proving a person's identity requires confirmation by a third party; here, there can be one or more third parties.

From the perspective of safety and efficiency, the verifications can be linked in the form of a chain of evidence to verify each other, which can achieve the purpose of verifying the Target. At the same time, the coverage behavior of neighboring nodes can also be verified together to realize the idea of challenging the coverage of multiple Targets at once. Thus, a multi-layered challenge is specified to achieve this multi-tasking solution.



The following describes how to build a Multi-layer Challenge packet O, which can be broadcast through the Narrowband network and received by a geographically close Target group T_n. Geographically close here indicates it is within viable RF radius of the intended Target T, expressed by Tradius. Since RF is a radio frequency broadcast and can be relayed, it forms a concentric ring with the intended Target T as the center, and a maximum radius of Tradius. The hot spots on the ring can receive the radio frequency between each other directly or indirectly.

Obviously, there may be multiple nodes that will receive Challenge packets, which will form a Target set. Then, which MeshBox node should be chosen as the Target?

For people, it is easier for everyone to believe in the proof provided by a person with high credibility and not directly related to the person being certified. Therefore, in the first round of candidate Targets,

(1) In the first step, select a node T_1 with the highest score in the Target set according to the Trust score, and then select a T_N node that also has a high score, which is the farthest node (in the Target set) from T according to geographical distance. Nodes T_1 and T_N are the start and end point of the proof chain.

(2) In the second step, select additional nodes in the Target set and determine a path from T_1 to T and from T to T_N, so that the Challenger will require a shorter time to receive feedback. According to the score of each node, define the weights of the edges between nodes (preliminary consider edge weights as 1-(score(Ta)-score(Tb))), and calculate the weighted graph Tg, which is used to calculate the shortest paths from T_1 to T, and from T to T_N, according to Dijkstra's shortest path algorithm. As shown in the figure above, a shortest path is calculated as T_1—T_2---T—T_3—T_N.

(3) The third step is to ensure that the data is not tampered with. The Challenger needs to encrypt the data and generate a temporary public and private key pair E_k and E_{k-1}

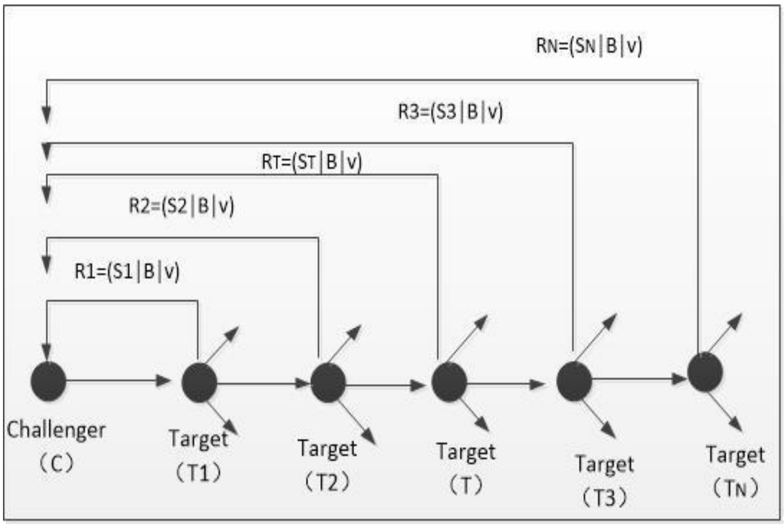
(4) In the fourth step, construct the innermost Challenge packet, that is, the Challenge Packet layer for end point T_N is created, as O_N, as part of the Challenge packet O. Here, the public key of node N and a shared secret (obtained through ECDH negotiation through a temporary public and private key pair E_k and E_{k-1}) are used for symmetric encryption to ensure that only Challenger C and Target T_N know the key.

(5) In the fifth step, repeat above steps to construct O_3, O_T, O_2, and O_1 layers, and add them to Challenge packet O. The outermost O_1 data is O, and O can be used for multi-layer challenges.

In this process, in order to enhance privacy, padding is performed so that the sum of the lengths of each layer of data are consistent, so that, except for the first node, all other nodes do not know which stage of the challenge path they are in, and also don't know which node is the last.

6.2.4 Building the Proof of Narrowband Coverage

After the Challenge packet is constructed, Challenger C sends the packet O to T_1 via the Internet. The process is as follows：



6.2.5 Coverage Proof Process

(1) After T_1 receives O, decrypt the outermost data, record the arrival time B and signal strength v, broadcast the remaining data, and return the signature receipt R1 to the Challenger.

(2) The node T_2 in the middle layer tries to decrypt the received Challenge packet, using the previously negotiated shared key Secret (calculated by the temporary private key pk) and its own public key combination for symmetric decryption.

(3) T_2 records the arrival time B and signal strength v of O_2.

(4) If decryption is successful, T_2 creates a signed receipt R_2, which is signed by T_2's private key, R_2=(S_2|B|v).

(5) T_2 submits receipt R_2 (via the Internet), removes the outermost data, and broadcasts the remaining part of O.

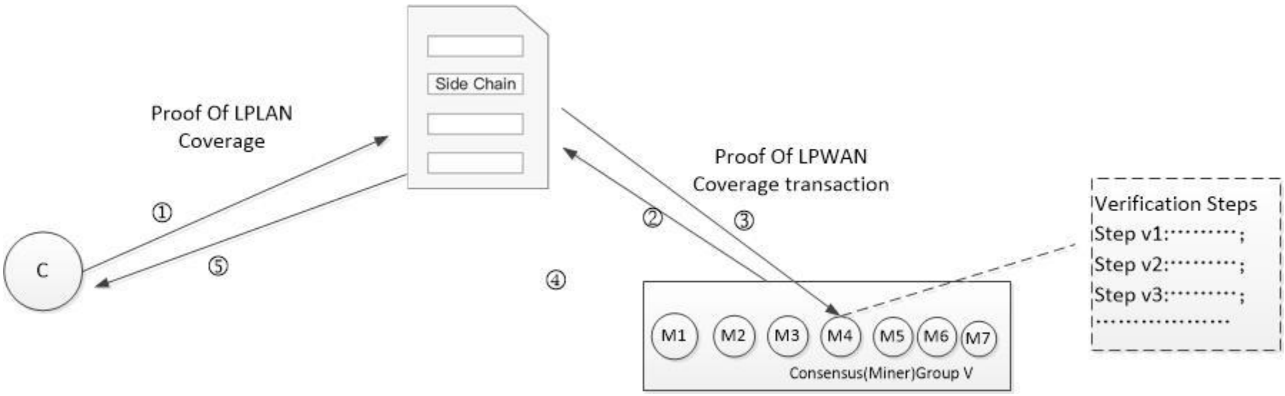
(6) Repeat the above process until the receipt of T_N is sent to C.

In order to improve the efficiency of the challenge, an upper threshold time λ is set for the challenge process. Once the Challenger C receives the receipt from T_N or this threshold time expires, the challenge is considered complete. The signed receipt set R_S is a part of the coverage proof.

The other part of the Witness' proof (W_S) is obtained from the Witnesses in a similar way, and the entire coverage proof (including the Proof from the Targets) is sent to the Mesh side-chain consensus group for verification through a transaction.

6.2.6 Verification of the Proof

When Challenger C submits the proof through a special transaction, all the steps that C took to construct the Proof are deterministic (and have verifiability and randomness). Thus, the other nodes in the consensus group, are able to reconstruct the original process and verify the Proof.



The nodes in the consensus group observe the Proof transactions, and are able to reconstruct and verify the process as follows:

- [Step v1] The consensus group miners V, rebuild the Target group T_n;
- [Step v2] Verify the entropy value through C's temporary private key
- [Step v3] Through Engtropy and probability distribution, determine the intention Target T and the corresponding set T_n
- [Step v4] Determine the start and end points of T_1 and T_N from the set T_n.
- [Step v5] Rebuild the Tg weight map and use the Dijkstra algorithm to determine T_1,...T,...T_N
- [Step v6] Consensus group V verifies the Rs signed by the private key of T_1,...T,..T_N, as well as the the corresponding Rs signed by the Witnesses W_s (using the witness' private key).

If the above processes are successfully completed and verified, then C's challenge is considered successful, and the corresponding participants (including the Target and witnesses) will be motivated proportionally and the score will be increased.

6.2.7 Scoring Mechanism

In order to improve the rationality of node selection, we have introduced a trust scoring mechanism. The design principles are as follows:

When a MeshBox node joins the network, it will be given an initial, basic score ф. Nodes with a trust score greater than the basic score are deemed as honest nodes.

The trust score of the node will dynamically change with the number of challenges and time. The higher the number of successful Challenges passed by a node, the higher the node's score will be. In addition, if a Challenge is not accepted for a long time or the challenge fails, the score for the node will decrease.

In order to prove that the nodes with low scores are also honest, a score probability distribution function is used. The node with the lowest score has the highest probability of being selected, and the scores of the nodes overall are improved through a form of reverse selection.

The scoring algorithm and the node selection probability distribution algorithm will be determined according to the corresponding design parameters of the Mesh side-chain consensus mechanism, which will be described in detail in the subsequent extension.

6.3 Proof of Mesh Network

Mesh networks utilize a distributed structure to construct a dynamic self-organizing wireless multi-hop network, allowing users within the coverage radius of the network to have high-speed wireless access to the Internet to support many applications. MeshBox Foundation has cooperated with SmartMesh Foundation to build a flexible, decentralized, self-healing mobile mesh network. MeshBox Foundation invites global experts to join in building a global mesh network, which has the potential to securely address information security, network congestion, off-internet communication, off-internet payment, inclusive finance and other problems in many application fields.

In order to realize this vision, users around the world need to work together to build a large-scale Wifi mesh network with verifiable coverage being provided by each node. Similar to Proof of LPWAN Coverage, the Proof of Mesh Coverage also needs to incentivize users to increase the density of MeshBox deployments to produce a large-scale network effect. The Proof of Mesh also offers token incentives to participating nodes. MeshBox stakeholders can obtain corresponding rewards by declaring their location and providing corresponding Proof of Mesh.

6.3.1 Design Concept

The Proof of Mesh Coverage is used to prove that a MeshBox has been deployed in its local mesh network, and participating in the routing of Wifi traffic. More specifically:

(1) Prove that the miners, associated with a MeshBox, actually own the MeshBox hardware and enable the mesh network connection.
(2) Prove that the miners are located at their declared geographic location and connected to other MeshBoxes through the local mesh network.
(3) Prove that miners provide mesh network coverage in that area

Different from LPWAN, Wifi mesh has a shorter coverage radius (about 100 meters), and the propagation method is also different from LPWAN. Therefore the Proof of Mesh is introduced. However, considering that LPWAN has a Location Proof (such as Helium's Proof of Location), such a Location Proof will be re-used for Proof of Mesh. Thus, MeshBoxes with a trust score higher than 0.5 or confirmed to have passed the latest LPWAN Challenge is considered to have verified their true positioning, and are thus able to select multiple neighbors around it (within 100 meters) to verify Mesh coverage based on geographic positioning.

Proof of Mesh will be specified, with potential additional mechanisms, in the future, according to the network deployment status. The overall process is as follows：

(1) In the initial stage, the Challenger constructs a many-to-one mesh coverage proof. The Challenger selects the intended Target T as the node to be challenged, and obtains the connection status and MAC address (signature confirmation) of T from the MeshBox node adjacent to its geographic location. The Challenger should obtain a connection confirmation from at least two-thirds of the neighboring nodes (and at least three nodes) within a limited time. The receipts from such neighboring nodes are packaged to construct a coverage proof and sent to the consensus group for verification.
(2) In the intermediate stages, Challenger builds many-to-one, one-to-one and one-to-many fusion Coverage Proofs. After the mesh network is further expanded, there will be two situations:
    a. There are still remote areas where meshboxes become relatively isolated nodes
    b. There are MeshBox groups with a higher degree of concentration.

    In both cases, it is possible that multiple Verifiers cannot be found or the cross-validation efficiency is not high. In this case, a staking mechanism is introduced. Trusted nodes called Hub nodes are deployed, and the coverage of isolated mesh nodes and the multi-mesh nodes connected to the Hub are verified, with associated rewards given to the nodes connected to the Hubs.
(3) At the last stage, the Challenger further constructs a trustless chain broadcast proof, similar to Proof of LPWAN coverage. In the case that the Mesh has a propagation mechanism similar to LPWAN, build a single Challenger, multi-Target, and multi-witness chain broadcast coverage verification, which is integrated with Proof of LPWAN to achieve an even higher level of Proof of Mesh Coverage.

6.3.2 Initial Stage of Proof of Mesh Coverage Construction

In the initial stage the mesh network's characteristics are used.

(1) MeshBox mesh nodes have limited RF propagation distance.
(2) MeshBox nodes are arranged in mesh topology, in which adjacent nodes are directly connected through WiFi signals, and non-adjacent nodes can be indirectly connected through relay nodes.
(3) If any MeshBox in the mesh network is connected to the Internet, the other nodes are also connected to the Internet, via hopping through one or more MeshBox nodes in the same local mesh network.

The goal is to verify whether a MeshBox has truly established mesh network coverage in a physical area. Here, we refer to the LPWAN coverage proof method, and use a similar method to verify the existence of Wifi Mesh coverage in the form of a Mesh Challenge. First, a Challenger node C determines the challenge Target based on the geographic location covered by LPWAN. Each LPWAN Target has a probabilistic statistical trust and instant verification characteristics, and the abilities of Witnesses are different. In order to improve the effectiveness of the challenge, the challenged Target is subject to conditional constraints.

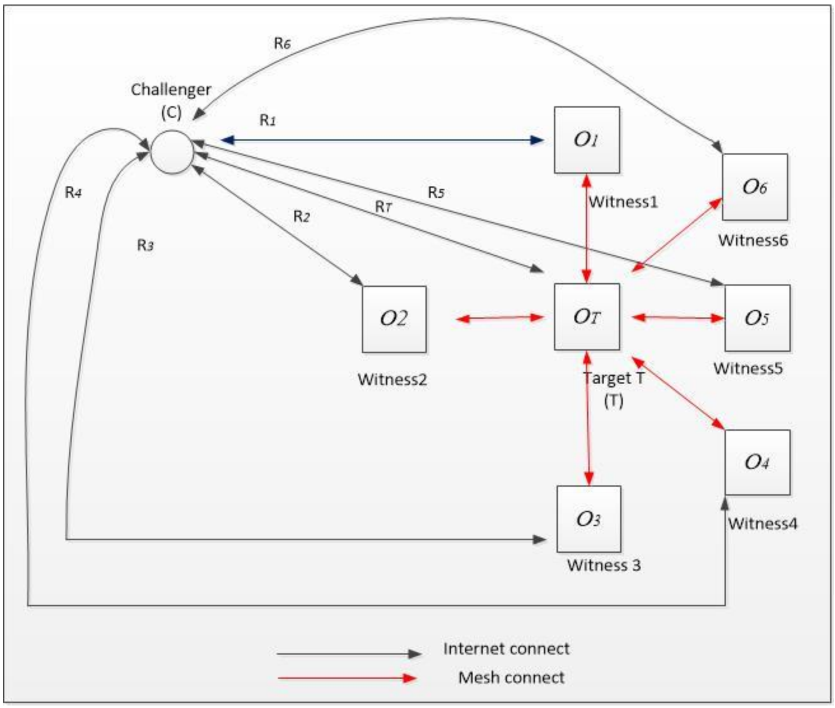
6.3.3 Select the intended Target

The MeshBox node which is selected as a Target should satisfy the following conditions

(1) Nodes that have participated in a Proof of LPWAN Challenge in the latest three Challenge. cycles; Or nodes which have participated earlier than three Challenge cycles ago, and with scores above 0.5.
(2) AND, there are at least three adjacent neighboring nodes.

In order to ensure the uniqueness of the intended Target, similar to Proof of LPWAN coverage, the verifiable entropy value ρ (the current block hash value, which is signed by the private key signature) is introduced. This entropy value ρ is used in the Target node group Z (above condition of more than 3 nodes in the area). The random number thus generated uniquely determines an intention node T as the challenged Target.

6.3.4 Construct the Challenges

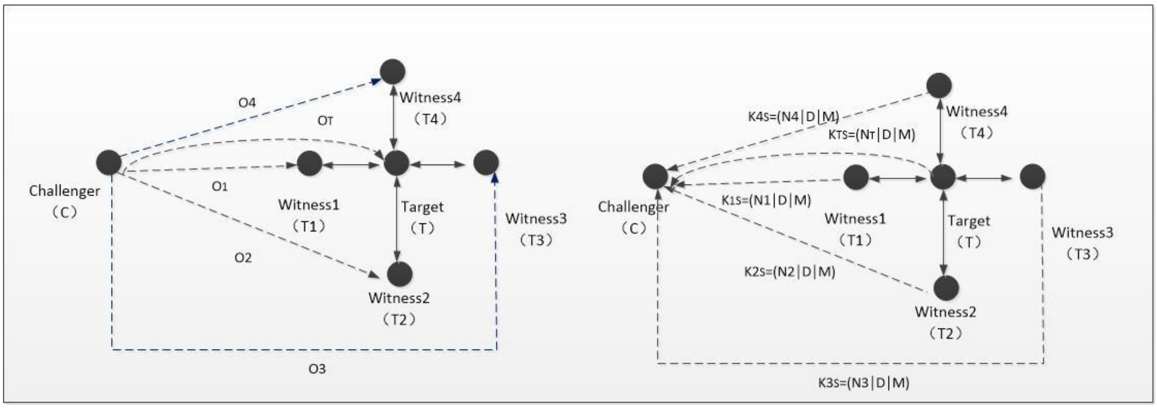


Once T is selected, Challenger C needs to construct a coverage list, and include all nodes I (i from 1 to n) within the mesh propagation radius of $T_{\underline{radius}}$ (100 meters) through LPWAN positioning, and sort by score using ECDH. This results in the construction of multiple Challenge packets, O_i (i, i from 1 to n), in which each O_i contains a two-tuple: E(S, ϕ).

E is a secure encryption function that uses ECDH to obtain a symmetric key , S is a nonce value generated according to the score sorting, and ϕ is the time to send a Challenge packet to the neighboring nodes of T node. Challenger C constructs the logical process of Challenge O as follows:

(1) All T_n within the Wifi signal radius of T are selected as candidate nodes, including the intended Target T;
(2) Sort the nodes according to the score and assign the nonce value in order;
(3) Generate a temporary public/private pair E_k and E_{k-1}
(4) Use Target and Witness node's public keys and ECDH shared key to encrypt directed Challenge packet O_1
(5) Repeat the process 3-4 until all point-to-point Challenge packets O_i are constructed.

6.3.5 Construct Proof of Mesh Coverage



(a) Challenge data transmission (b) Receipt Transmission to Challenger

Once the O_i have been constructed, Challenger C directly sends the Oi to the set of MeshBox nodes via the Internet. Because each Challenge packet is symmetrically encrypted, only the corresponding Target T can decrypt E and feed back a valid receipt to Challenger C.

The process of establishing the Proof is as follows:

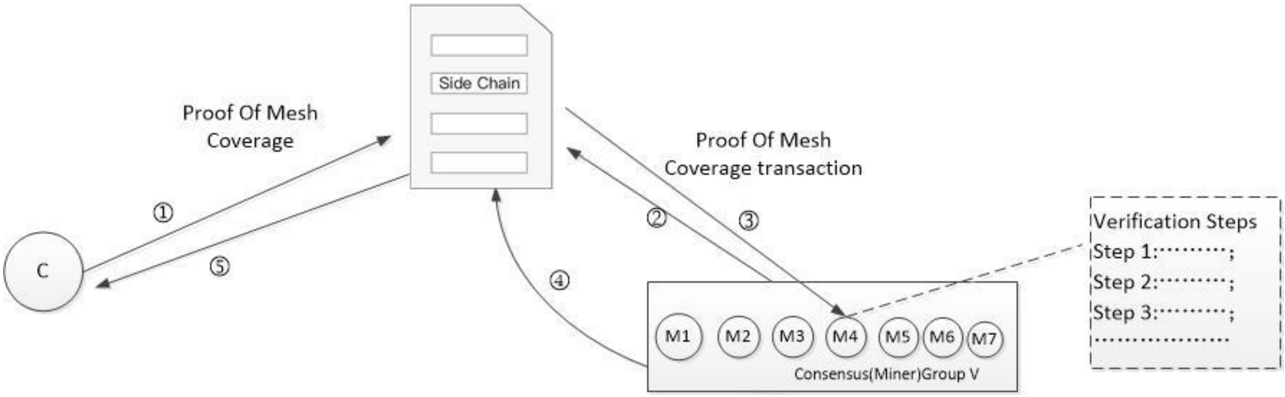
(1) T_1 receives Challenger C's directed Challenge packet O_1 through the Internet
(2) T_1 attempts to decrypt the value of E using its own private key
(3) T_1 records the arrival time of the Challenge packet [GLOBAL CHANGE M1 to t1] t_1
(4) If successful, T_1 constructs a multi-connection receipt set K_s through the following:
   a. T_1 screens out the connected MeshBox nodes according to the special identification of the MeshBox node,
   b. T_1 constructs a connection receipt K_{s1}, consisting of connection state N_1, MAC address D_1, MAC address of a neighboring node, and the time t_1 into a single connection receipt Ks1 = (N1 |D1|t_1),
   c. T_1 sums up the signatures to generate a multi-connection receipt set K_s = (S| K_{s1}|...|K_{sk}), in which there are k neighboring nodes. The "|" denotes the concatenation operator.
(5) T_1 sends K_s to Challenger C via the Internet
(6) Each node that receives the Challenge packet constructs a similar receipt and sends it to Challenger C
(7) Challenger C receives all the Challenge packets and the corresponding K_s receipts or reaches the limited time λ, at which point the collection has been deemed as completed.

Because C assigns different nonce values to each of the nodes, the witness nodes T' and the intended node T are processed separately.

Among all witnessing nodes T', Challenger C filters out the single connection receipts K_{sx} connected to T, and sorts them by nonce. Then sequentially match Ksx with the key parameters in the receipt set K_T of the intention Target T. If, at least three matches are satisfied then the coverage of T is deemed as true coverage (otherwise the challenge is considered failed). The Ksx of all witnessing nodes and the K_T of the intended Target T are combined into a Mesh coverage proof and sent to the consensus group.

6.3.6 Verification certificate

Challenger C submits the coverage proof to the consensus group through a transaction [on the Mesh side-chain], and all receipts from the node group will be published on the Mesh side-chain. Because all the steps are deterministic and verifiable, The V verifying miners in the consensus group, reconstruct the steps and verify that the proof is legal.



The process that each Verifier Miner MeshBox takes to reconstruct and verify the coverage proof is as follows:

(1) Verifier miners V, reconstruct the miner set N according to the rules;
(2) Through the challenger's temporary private key, the entropy value ρ is verified and a random number is obtained.
(3) Determine the intentional Target T from the set of miners according to the random number.
(4) Select the node group within the Wifi signal radius of the intended Target T and sort to obtain the Witness node group;
(5) The signature receipts K_{sx} and K_T in the transaction are verified in turn
(6) Assuming that the above steps are successfully completed and the coverage proof is proven, participating nodes will be rewarded proportionally.

6.4 Comparing Proof of Mesh Coverage and Proof of LPWAN Coverage

The Proof of Mesh challenge and verification processes similar in some ways, but also different from that of the Proof of LPWAN.

(1) The similarity lies in the fact that all three interactive modes of Challenger, Target, and Witness are common to both protocols. Also, entropy is used to uniquely determine the intended Target.
(2) The difference is that Proof of LPWAN uses daisy-chain routing to transfer the Challenge packet, whereas the Proof of Mesh uses a Point-to-Point (Challenger to each Target) Challenge packet.

The LPWAN Proof uses time and signal strength as the coverage reference basis, while the Mesh Proof uses time, connection status and mac address (each node feeds back the adjacent connection status and mac addresses) as the coverage reference basis.

In the Mesh Proof, the Challenger needs to perform a secondary matching verification on the data of the intended Target and the Witness (except for the challenger, no node knows who the intended Target is, and the intended Target itself does not know). Then, the Challenger filters the combination of receipts to generate a coverage proof. In terms of the Challenge packet, for the LPWAN Proof, each layer's protocol information is nested (onion). However, in Proof of Mesh, the protocol information is independently encrypted, as separate packets from Challenger to each Target. Both achieve the intended purpose of directional encryption.

In terms of the number of Targets which challenged at the same time, for Proof of LPWAN, multiple Targets can be verified at the same time, while for Proof of Mesh, only one Target can be verified.

The main methods of Proof of Mesh coverage reconstruction are as follows:

(1) Circumstantial evidence: The Challenger can examine the receipts to verify that the Witnesses are connected to the Target, using the MAC address of the intended Target T.
(2) The Challenger can examine the receipt of the Target to confirm the Target's connection with at least three Witnesses with the Witnesses' MAC address.

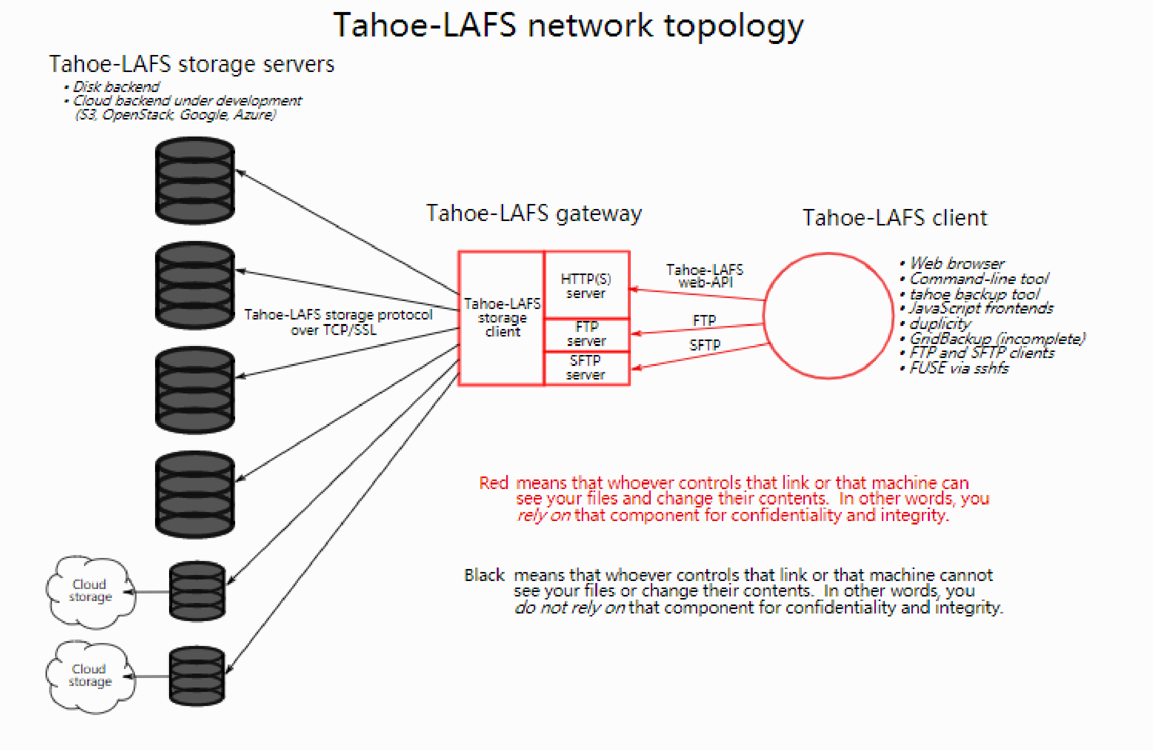
7. MeshBox distributed storage system

7.1 Overview

As a mesh network node, MeshBox does not only capable of supporting network connection, it also have storage and computing functions. Its excellent hardware configuration and the global distributed deployment make it a natural match with distributed storage, which is very suitable for building global distribution storage system, especially for IoT data storage. MeshBox users can easily and safely use the distributed storage system deployed through MeshBox for encrypted storage and sharing files. MeshBox owners can also obtain income for providing storage or storage mining income. In line with the concept of building ecological integration and development, we will support multiple distributed storage protocols such as Tahoe and IPFS at the storage layer of MeshBox, and integrate Tahoe storage solutions in the early stage.

7.2 MeshBox Tahoe distributed storage system

Tahoe-LAFS is a free and open decentralized cloud storage system. It can distribute data across multiple devices. Even if some equipment fails or is taken over by an attacker, the entire file storage will continue to operate as usual, thereby protecting data privacy and security.


Tahoe-LAFS network topology
Tahoe-LAFS storage servers
• Disk backend
• Cloud backend under development (S3, OpenStack, Google, Azure)
Tahoe-LAFS storage protocol over TCP/SSL
Cloud storage
Cloud storage
Tahoe-LAFS gateway
Tahoe-LAFS storage client
HTTP(S) server
FTP server
SFTP server
Tahoe-LAFS web-API
FTP
SFTP
Tahoe-LAFS client
• Web browser
• Command-line tool
• tahoe backup tool
• JavaScript frontends
• duplicity
• GridBackup (incomplete)
• FTP and SFTP clients
• FUSE via sshfs
Red means that whoever controls that link or that machine can see your files and change their contents. In other words, you rely on that component for confidentiality and integrity.
Black means that whoever controls that link or that machine cannot see your files or change their contents. In other words, you do not rely on that component for confidentiality and integrity.

The main technical features of Tahoe are described below:

(1) Tahoe encrypts the data (backup, slice data) before it reaches each storage device

(2) Tahoe uses distributed file storage, that is, the content of the file cannot be viewed and reviewed without authorization.

(3) Tahoe replaces the traditional file access authorization verification with a string of variable length, which has high security, basically cannot be compromised online, and is completely anonymous, without registration and identity verification process.

(4) Tahoe file storage process includes: uploading a file through the client, the file is divided into file fragments before uploading to some storage devices, then upload to a T number of storage devices; each device only retains a part of the file, and there is no complete file backup; the file name is replaced by a encrypted strings; after uploading, Tahoe returns a string through the client, that is, the string is the only credential to access the file, for example:

URI:SSK:234hv34x1t43a6t7ft76iaa3oa:35633ebsf2yrfghn55xo7c5oh3we2rvgi32da930r23sbr7t2s

(5) For the storage service, it only owns part of the file which is encrypted and the file name, source and content of the file cannot be known, so "a certain file" cannot be deleted.

(6) Tahoe distributes files and retrieves (restores) files according to the preset threshold. One file is split into T shares, which are randomly (evenly) distributed among the available storage

nodes. If you need to rebuild files, you only need to return T '(T'<T) shares, that is, if a T-T' storage device fails to retrieve, the file can still be recovered. The more storage nodes means better resistance to failures or attacks, this sharing mechanism is very suitable for remotly and safely store sensitive data while reducing the risk of data loss.

Currently, the MeshBox Foundation and Tahoe-LAFS have established a close cooperative relationship. The two parties have conducted in-depth communication and integration at the technical level, and have successfully built a Tahoe operating environment on MeshBox, conducted performance testing and joint development of APP functions. It can achive the functions of uploading and saving encrypted files, exporting the private key of the files, file import and retrieval via different device, file sharing, etc.

The performance and functions initially built for the distributed storage architecture are described in the following:

（1）Support distributed storage function expansion. Currently, the main function API includes: single file addition, deletion, modification, query, and downloading; directory addition, deletion, modification, query, batch addition of files in the directory, removal/importing of files in the directory, and renaming, etc., also will jointly develop paid storage functions, and support storage nodes use mesh mining to collect miner fees, user upload files (management end) fees and user sharing file download fees etc.

（2）Distributed storage inspection and security. Supports checking the integrity and size of files, preventing manual modification of intermediate data after encryption before storage. The redundancy design of threshold processing is adopted to ensure the security of the backup. As long as the number of damaged devices is less than the threshold number, the file will not be damaged. Except for the provider (or the one he share with), everyone else including those who know the storage device data cannot steal the data.

（3）Distributed file storage performance and resource occupation. Distributed storage computing is faster, and storage devices that need external services must provide independent IP/DNS. When downloading while no one is uploading, the CPU occupies 0.6%-1%, the memory taken up is about 130M (take 3 nodes as an example); when uploading and downloading, the CPU occupies about 1.6%, and the memory is about 350M. The hard disk occupation is based on the file type provided, Take 1M file as an example, if uploaded to 10 storage nodes, the restoring threshold required is 3, and the total file-to-device occupancy will be about 32M.

（4）Network requirements and backup design. According to the purpose, the internal network environment can only be used in the internal network; in the public network environment, the port can be opened for external use under the condition of identified DNS and fixed IP; in terms of network occupation, upload and download are based on the maximum network speed divided by the number of nodes. The number of backups is arranged according to the access middleware.

After the client file is uploaded, even deleted the local file, as long as have the private key, it will be automatically downloaded, or the private key file can be downloaded after confirming the password in another place.

（5）Modification and deletion of storage content design. The data that has been uploaded to the network storage node cannot be modified (unless the file is modified by yourself, the modified file will be automatically synchronized to the storage device, that is, overwritten). The deletion is determined by the storage service node, and the user cannot delete. Other than the user, anyone (invited nodes can be downloaded and viewed), including storage nodes, cannot delete, view, edit, etc. In addition, if the Tahoe node has set a service period, if it expires, the file will be destroyed.

(6) Limits on the number of storage nodes and storage data types. There is no limit to the number of Tahoe storage nodes. In theory, the more storage nodes, the larger the file fragments and backups, which shows a binomial exponential growth pattern. In terms of storage type, whether it is data, pictures or video, there is no difference in distributed storage. Tahoe doesn't care about the file type, it is all through the folder operation, if you want to store 1.exe, 2.jpg or 3.mp4, then put them in one (or more than one) folder.

MeshBox Tahoe has preliminary distributed storage capabilities and is currently developing a MESH token incentive system, so that the MESH token will open up the entire MeshBox distributed storage system and connect various roles in the network including storage miners, block producers, verification nodes, and circulate between these roles.

8. Conclusion

Meshbox®, Smartmesh®, and other ecosystem partners aim to move society in the right direction, by providing a highly advanced Wifi Mesh Network solution with the Spectrum blockchain to enable an Internet of Value.

The proposed solution enables blockchain based Fin-tech, high-throughput wifi-communications, and a distributed content storage system, while operating

- with or without the Internet
- with or without a blockchain; with Photon state-channel secondary architecture,
- with or without an electrical grid; with renewable battery and solar technology.

The production versions of Indoor MeshBox® and MeshBox++TM will be available before 4Q 2019. Pre-production versions of MeshBox++TM have already been deployed successfully in the United States, at the following venues:

- Superbowl 51 February 2017 in Minneapolis, Minnesota : 6 MeshBox++TM nodes
- 50th Special Olympics July 2018 in Chicago, Illinois : 15 MeshBox++TM nodes, 3 gateways.
- Permanent installations of MeshBox++TM networks in San Jose, and San Francisco, California

Together, with partners such as Satellite operators, LoRa technology providers, and Smartmesh®, Meshbox® brings about a paradigm shift to enable Infrastructure deployment with Shared-ROI. Instead of the service provider determining when and where to roll out service, the residents of a community decide when and where to deploy infrastructure such as MeshBox® routers.

This whitepaper highlights how a HyperMeshTM Infrastructure, enabled with Smartmesh® and Meshbox® technology can speed up the realization of an IoV Infrastructure, to bring dignity and a sustainable livelihood for the 3.9 Billion people without internet access, 2 Billion people who are unbanked, and 1.2 Billion without access to electricity [Paygo].

9. References

[Paygo] UN Climate Change Newsroom, Using Pay-As-You-Go Solar Home Systems in Sub-Saharan Africa, March, 2017

[MB++] MeshBox++™ is designed by Mesh++ Inc., a close partner to Smartmesh® and Meshbox®

[PLDT] 3. PLDT Wired Internet Costs https://www.imoney.ph/broadband

[WSJ] https://www.youtube.com/watch?v=9gi_0KR80TQ&t=197s. John Hodulik, UBS Media and Telecom Analyst.

[EEN] Jonathan Koomey, MIT Technology Review The Computing Trend that Will Change Everything, April 9, 2012. https://www.technologyreview.com/s/427444/the-computing-trend-that-will-change-everything/

[Seba] James Arbib and Tony Seba, Rethinking Transportation 2020-2030, The Disruption of Transportation and the Collapse of the Internal-Combustion Vehicle and Oil Industries. May 2017

[GridWise] GridWise Architecture Council, US Department of Energy, GridWise Transactive Energy Framework Version 1.0, January, 2015

[PowerMatcher] Koen Kok, The PowerMatcher: Smart Coordination for the Smart Electricity Grid, Dissertation at Dutch Research School for Information and Knowledge Systems, sponsored by the Netherlands Organisation for applied scientific research TNO, May 13, 2013

[TeMix] Edward G. Cazalet (CEO, TeMix Inc), Business and Regulatory Models for Transactive Energy, GWAC Transactive Energy Conference, www.tea-web.org, December 10, 2014

[FRACTALS] Peter Yan, FRACTALS Realtime Autonomic Control Anti-fragile Layered System Architecture -- Smartmesh® and Meshbox® Ecosystem, September, 2018

[Helium] Amir Haleem, Andrew Allen, Andrew Thompson, Marc Nijdam, Rahul Garg, Helium A Decentralized Wireless Network, Helium Systems, Inc. Release 0.4.2 (2018-11-14)