SatyaSpeak

IAFI-5th ISMC,2025

15th Dec. @New Delhi,Bharat

6GHz powered Decentralised WiFi(DeWi)-

"Unlocking the Potential of Wi-Fi Hotspots as Phygital Public Good"

Dr Satya N. Gupta, NGNguru

PhD (CVU), CEng. DIISc. DRP, IRSSE(VR)

Chairman- Blockchain for Productivity Forum

Adjunct Professor of Practice- South Asian University

Secretary General- ITU APT Foundation of India

Evolution of Wi-Fi Standard (IEEE802.11) - 1997-2025

IEEE 802.11 Protocol	Release Yr.	Frequency Band(s)-Ghz	Ch. Width (MHz)	Max Throughput
802.11	1997	2.4	22	2 Mbps
11b	1999	2.4	22	11 Mbps
11a	1999	5	20	54 Mbps
11g	2003	2.4	20	54 Mbps
11n (Wi-Fi 4)	2009	2.4/5	20/40	600 Mbps
11ac (Wi-Fi 5)	2013	5	20/40/80/160	6.8 Gbps
11ax (Wi-Fi 6)	2019	2.5/5	20/40/80/160	9.6 Gbps
11ax (WiFi 6E)	2020	2.5/5/6	20/40/80/160	9.6 Gbps
11be (WiFi 7)	2024	2.5/5/6/60	20/40/80/160/320	36 Gbps

Key Performance Benefits

Advantages of Wi-Fi 6E Technology

Better efficiency

40% higher throughput

Pristine band

0 legacy interference

Reduced congestion

75% less interference

Lower latency

As low as **2ms**

Longer battery life

30% power savings

Wi-Fi 6E Performance Metrics

2Gbps+	2ms	1200MHz	7x
Maximum Speed	Ultra-Low Latency	Additional Spectrum	160MHz Channels

Speed Enhancement

> Single connections can exceed 2Gbps rates, excellent for video and AR/VR gaming applications

- Doubles effective throughputs with 160MHz channels
- Enables 10Gbps+ networks for future generations
- Perfect for high-bandwidth applications

Interference Reduction

> Legacy-free 6GHz band eliminates interference from older Wi-Fi protocols

- No legacy device interference in 6GHz band
- Fewer collisions between adjacent networks
- Consistent low-latency performance

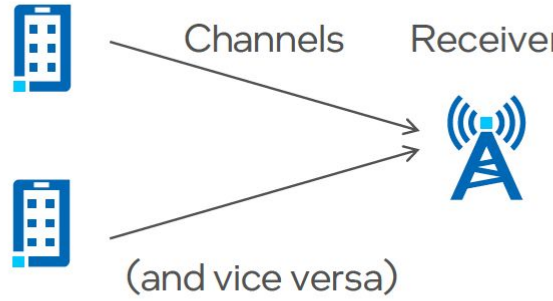
Capacity Increase

> Supports more simultaneous Wi-Fi clients in dense and congested environments

- More than doubles available spectrum
- Additional non-overlapping channels
- Better performance in crowded areas

Efficiency Gains through Multi-Level Innovation

OFDMA and MU-MIMO Efficiency Gains



Capacity = Channels x Bandwidth x Log (1 + Signal/Noise)

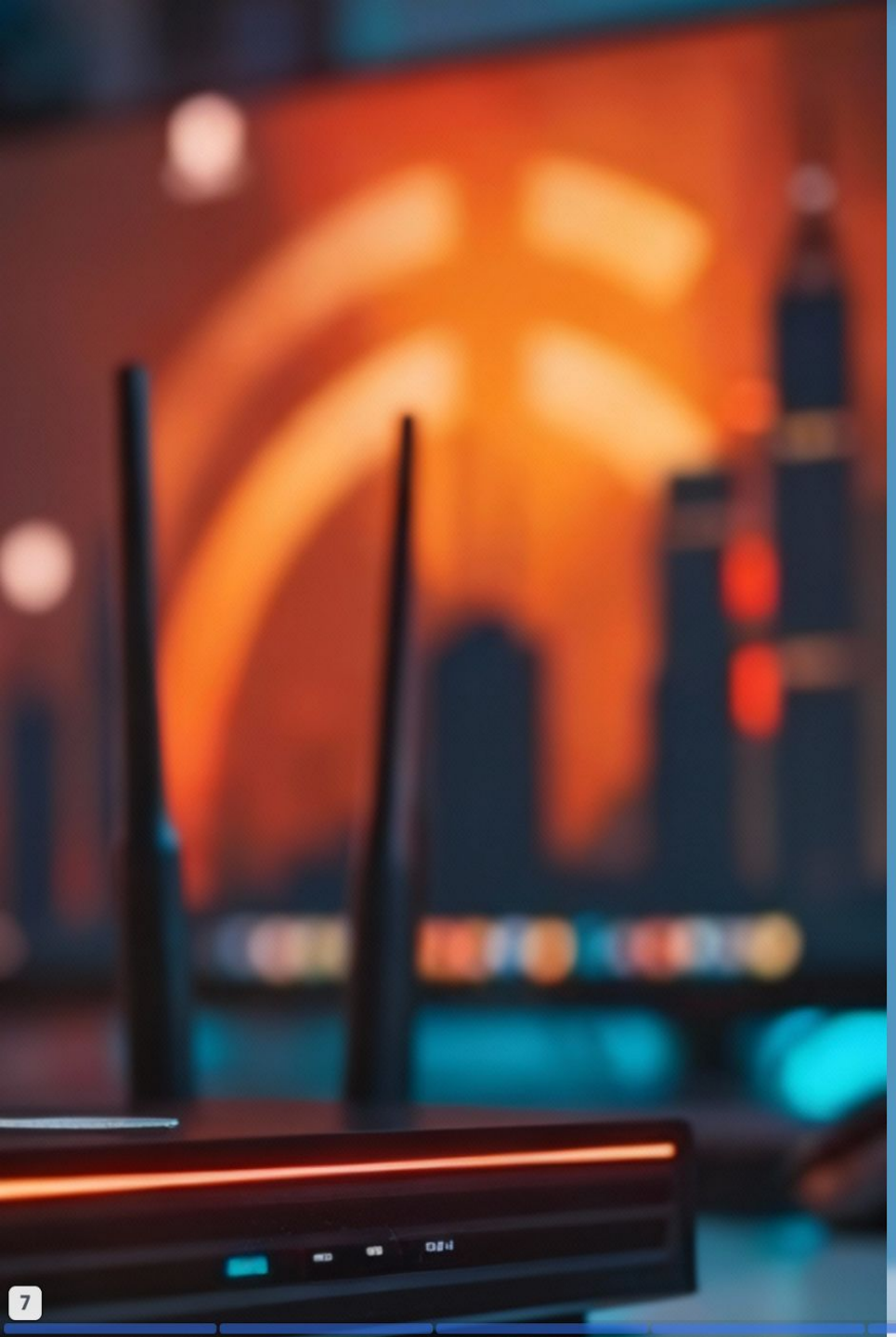
MU-MIMO increases the number of channels

Max bandwidth is unchanged with respect to 11ac

With multiple transmitters the total transmit power is increased

With UL OFDMA there is some cross-user leakage, but it is more than made up for by total power gain

With MU-MIMO cross stream noise increases, but it's inside the log function



Technical Implementation

Advanced Features and Technologies

MU-MIMO Technology

Multi-User Multiple Input Multiple Output enables simultaneous data transmission to multiple devices, significantly improving network throughput and reducing latency in high-density environments.

Scheduling Techniques

Advanced **time-division scheduling algorithms** minimize packet collisions by intelligently allocating transmission slots, ensuring optimal channel utilization and reduced interference.

OFDMA Efficiency

Orthogonal Frequency Division Multiple Access divides channels into smaller subcarriers, allowing simultaneous transmission to multiple devices with different bandwidth

Applications and Use Cases

Where *Wi-Fi 6E Makes a Difference*

Dense Environments

Stadiums, airports - Delivers reliable connectivity in high-density scenarios with thousands of concurrent devices

High-Bandwidth Applications

8K video streaming, VR/AR gaming - Supports ultra-high-definition content and immersive experiences with low latency

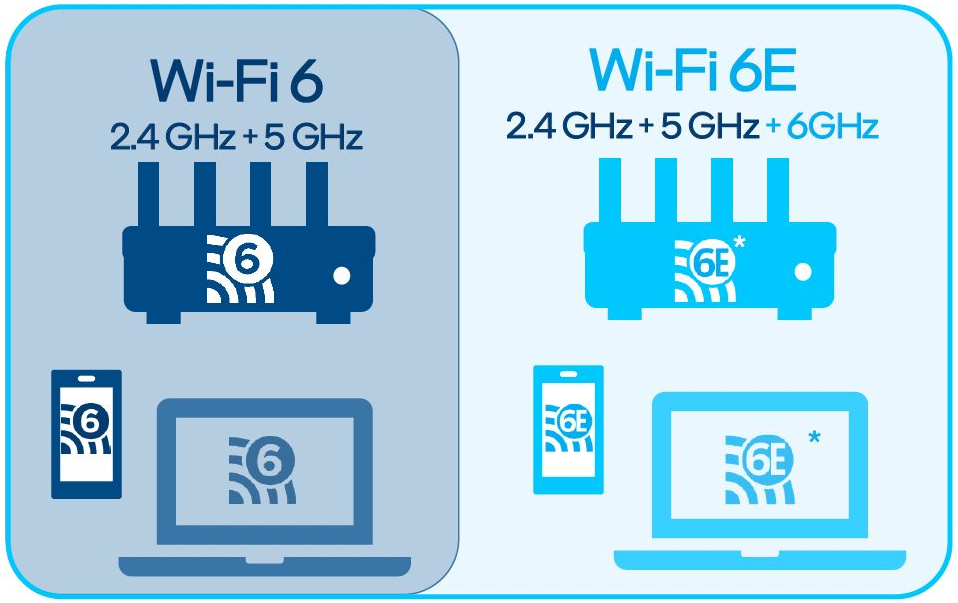
Enterprise Deployments

Offices, campuses - Enables seamless connectivity across large corporate networks with improved efficiency

Moving Beyond- WiFi 6e

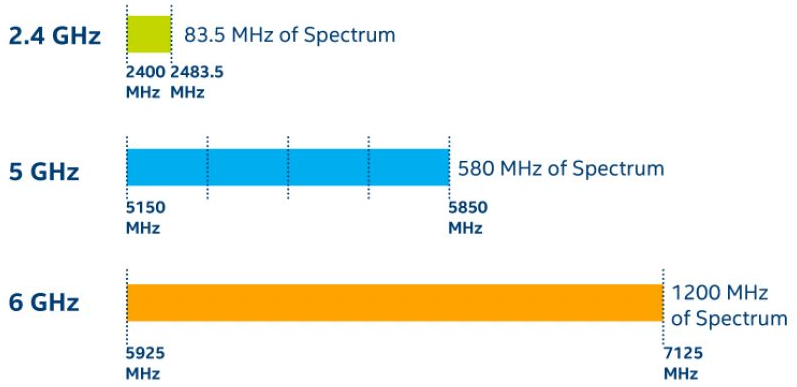
Introducing: Wi-Fi 6E

6 GHz benefits are not for all Wi-Fi 6 devices
(Wi-Fi 6E = Device differentiation & backwards compatibility)



With Wi-Fi 6E, the amount of spectrum used by Wi-Fi is almost 3X more

Comparing Wi-Fi Spectrum



Wi-Fi 6E: new spectrum brings the Wi-Fi 6 promise to reality, with compatibility to legacy Wi-Fi

* Not actual WFA Wi-Fi 6E logo

WiFI 6e- Salient Features

Wi-Fi 6E: Highlights

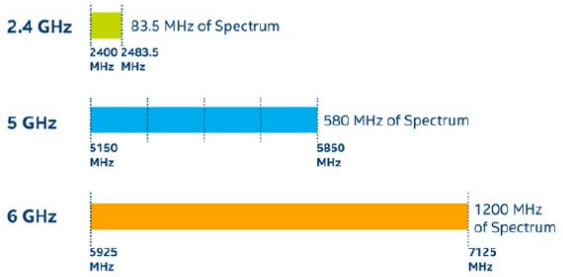
6 GHz Features

Huge contiguous clean spectrum
- 1200 MHz vs. 480 MHz (>2X)

Many more Gigabit Wi-Fi options
- (7) vs. (2) 160 MHz channels

Exclusive to new Wi-Fi 6 products
- No legacy devices (Wi-Fi 4 or 5)

Comparing Wi-Fi Spectrum



6 GHz Benefits

Greater network flexibility
- Ideal for dense environments

Fast downloads/sharing/backups
- Gigabit speed = new normal

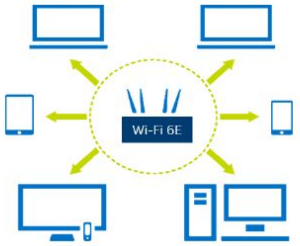
Reduced latency + improved reliability
- No waiting on older/slower devices

Why Is It Important?

1st new Wi-Fi spectrum in 17 years
- New 5 GHz DFS channels in 2003

~70% IP traffic on Wi-Fi by 2022[1]
- Billions of devices already on 5 GHz

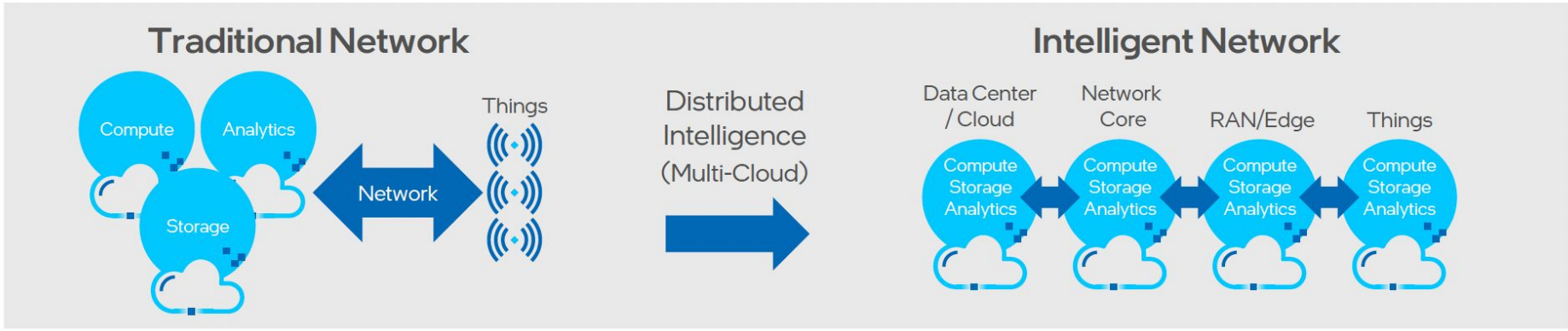
Delivers the max benefits of Wi-Fi 6
- Homogeneous "new" device networks



1) Cisco VNI Global IP Traffic Forecast 2017-22

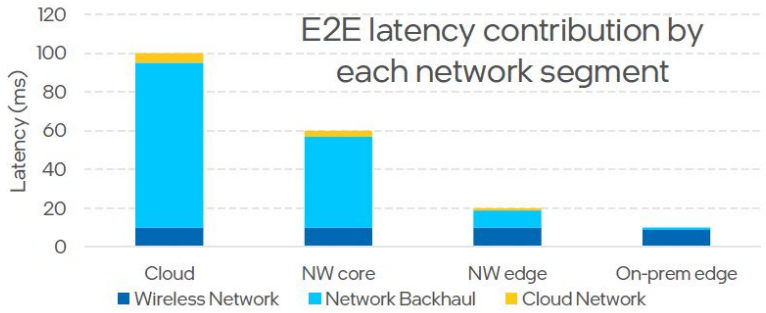
Demand for More

New Experiences Demand Continuous Improvement



New experiences (e.g., industrial IoT, 3D/XR content, real-time collaboration) demand more responsive connectivity

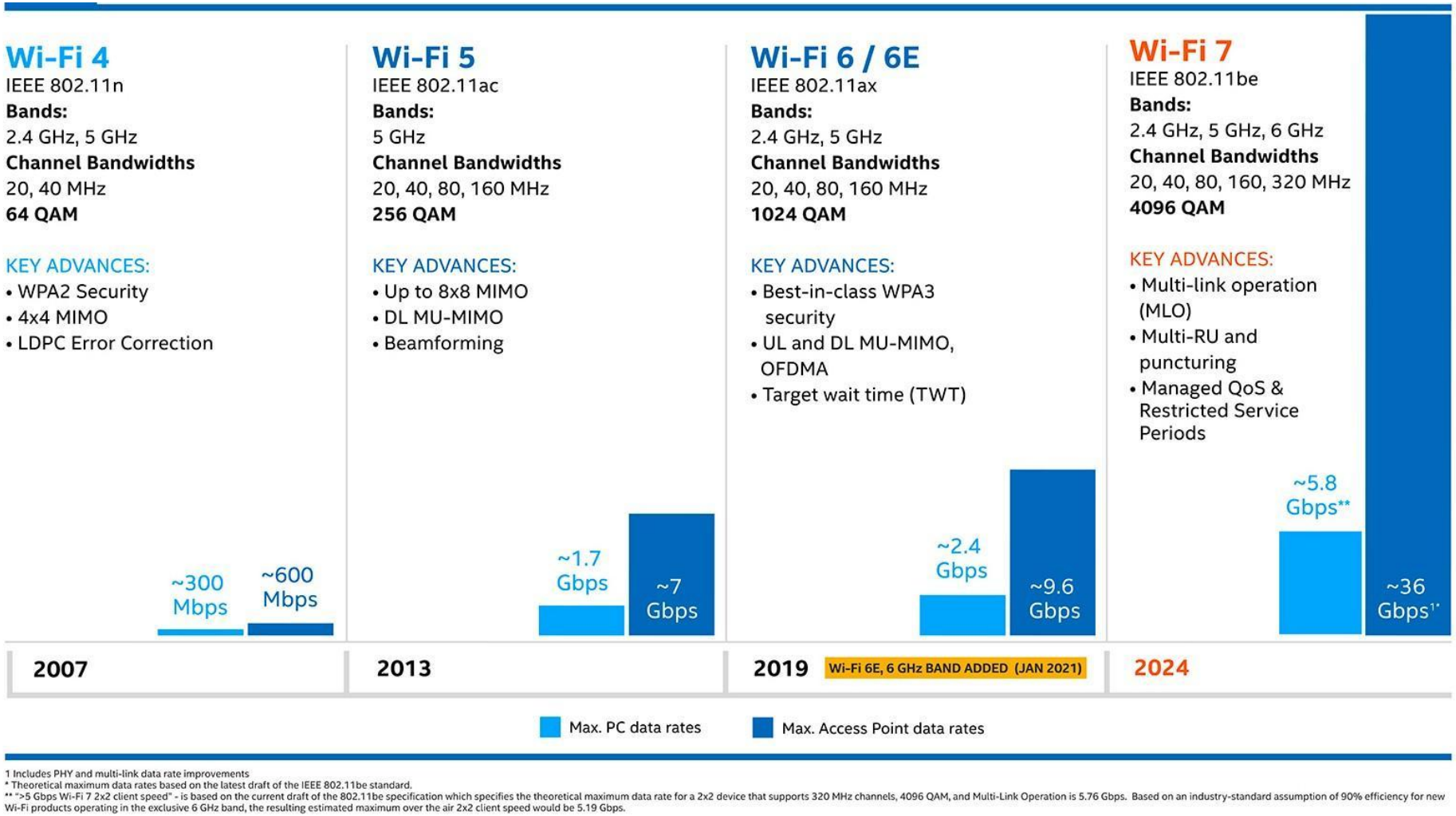
Compute shifting closer to the user, thereby redefining end-to-end (E2E) network performance (e.g., low, single-digit and sub-1ms latency become broadly available)



High performance wireless access is essential to meet growing demand

Latency Chart Source: Intel

Wi-Fi 7 -- NextGen Wi-Fi Technology



1 Includes PHY and multi-link data rate improvements
* Theoretical maximum data rates based on the latest draft of the IEEE 802.11be standard.
** ">5 Gbps Wi-Fi 7 2x2 client speed" - is based on the current draft of the 802.11be specification which specifies the theoretical maximum data rate for a 2x2 device that supports 320 MHz channels, 4096 QAM, and Multi-Link Operation is 5.76 Gbps. Based on an industry-standard assumption of 90% efficiency for new Wi-Fi products operating in the exclusive 6 GHz band, the resulting estimated maximum over the air 2x2 client speed would be 5.19 Gbps.

Beyond 6e- WiFi 7

Up Next: Wi-Fi 7

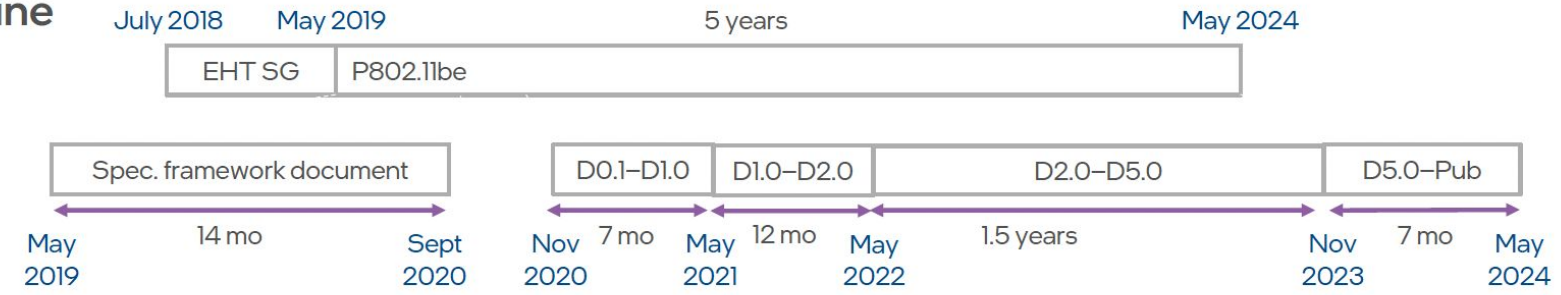
Based on IEEE P802.11be

P802.11be project goals*

- Amendment to 802.11, building on 11ax
- Maximum throughput of at least 30 Gbps
- Frequency range: 2.4, 5, 6 GHz
- Improvements to worst-case latency & jitter

Targeted usages

Target timeline



* http://www.ieee802.org/11/PARs/P802_11be_PAR_Detail.pdf

Breaking Next Frontier- WiFi7 (802.11be)

What's New in Wi-Fi 7?

Wi-Fi 6E was the first Wi-Fi standard to support 6GHz Wi-Fi. **Wi-Fi 7 is the latest** commercially available Wi-Fi standard, which continues to advance Wi-Fi technology with important new features that increase throughput and efficiency.

Wi-Fi 7 Enhancements

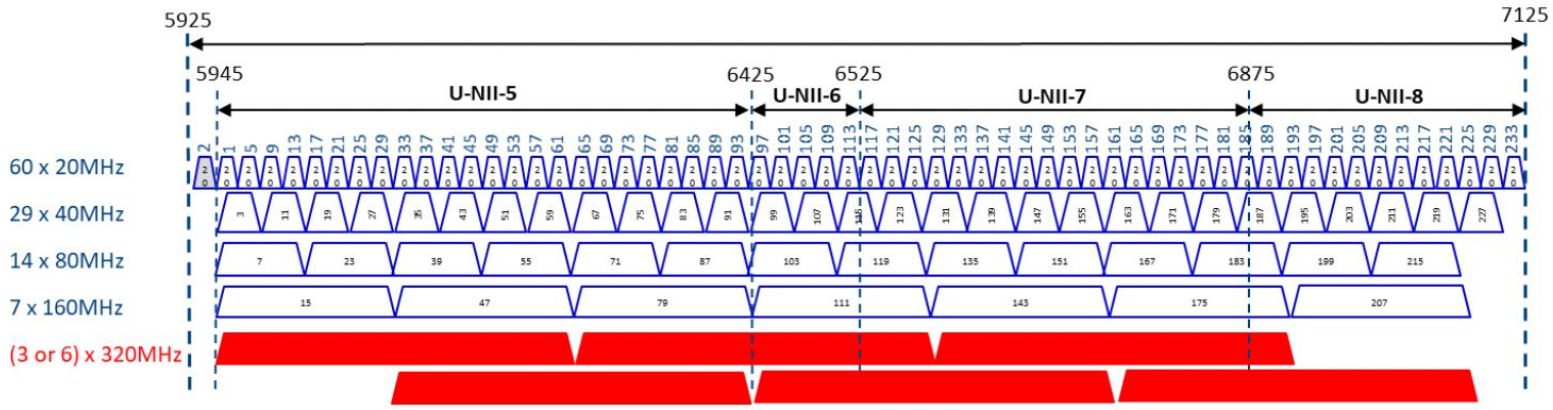
Wi-Fi 7 is built off the 802.11be Extremely High Throughput standard and has a variety of technology feature enhancements, including:

- **Greater efficiency** through a 20% increase in transmission rates with 4K quadrature amplitude modulation (QAM)
- **Superwide 320MHz channels** in the 6GHz band, enabling more data to be transmitted at once
- **Multi-Link Operation (MLO),** a novel Wi-Fi feature that allows Wi-Fi infrastructure to simultaneously use multiple channels across 2.4, 5, and 6GHz bands simultaneously
- **Deterministic latency,** a combination of enhancements to Wi-Fi 7 that enables access points and devices to schedule traffic more efficiently, enabling increased quality of service for supporting high-bandwidth applications, especially in dense environments

Ultra Wide Channel in WiFi7-320MHz

320 MHz Support

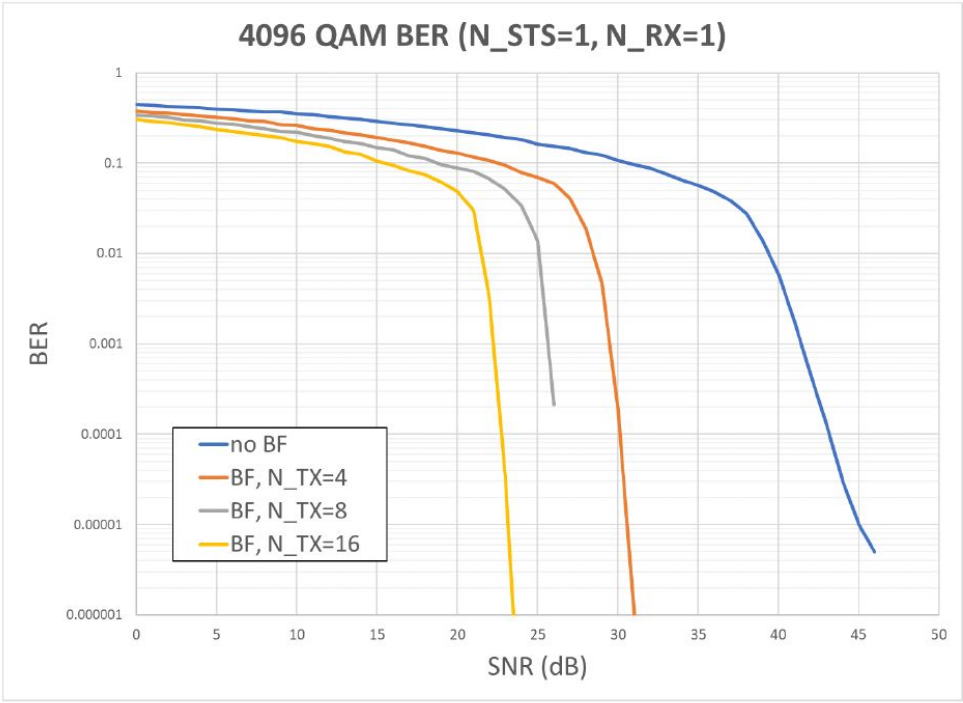
- Wi-Fi 7 supports up to 320 MHz bandwidth, as opposed to 160 MHz in Wi-Fi 6/6E.
  - Both 320 MHz and 160 + 160 MHz modes are supported.
  - Tone plan for 320 MHz uses duplicated 160 MHz tone plan based on Wi-Fi 6.



Technology Breakthrough- 4K QAM in WiFi 7

4096-QAM

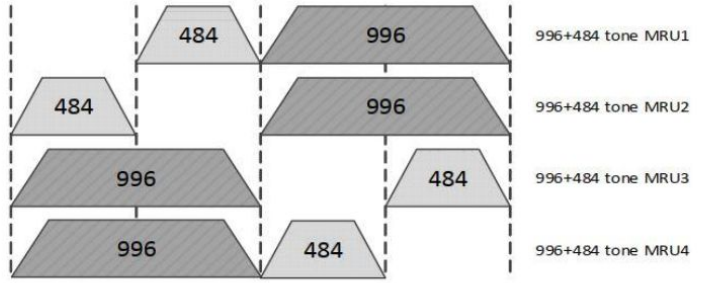
- The highest-order modulation of Wi-Fi 6 is 1024-QAM, whereas Wi-Fi 7 supports 4096-QAM.
  - Beamforming is essential in making the use of 4096 QAM feasible.
  - MCS 12-13: two new MCS index corresponding to 4096-QAM.
  - Tx EVM requirement is -38db to achieve a good balance between Tx power and distortion.



Multi- Resource Units in non-OFDMA mode- WiFi 7

Multi-RU Support

- Resource unit (RU): a group of subcarriers as an allocation for transmission.
- In Wi-Fi 6, each non-AP STA can only be assigned with a single RU.
- While this constraint simplifies the allocation scheme, it brings several limitations.
  - Degrades the spectral efficiency when number of users is small.
  - Wastes bandwidth in preamble puncturing scenarios, where the only primary 20 MHz can be used if radar detected in the secondary 20 MHz.
  - Fails to exploit the frequency diversity.
- Wi-Fi 7 introduces Multi-RU support by allowing the allocation of multiple RUs to a single STA.
  - Allowed Multi-RU combinations for different BWs are defined.



Example: Allowed 996+484-tone MRUs in non-OFDMA 160 MHz EHT PPDU

MLO(Multi- Link Operation) in WiFi 7

Multi-link Operation in Wi-Fi 7

- Existing Wi-Fi devices already support operating in different links.
  - A link is mapped to a specific channel in a specific band.
  - However, currently these links are operating independently without any coordination.
- Wi-Fi 7 introduces a unified framework to manage multiple links in a way that allows an optimized use of resources across multiple links.
  - **Throughput boost:** Aggregating multiple links achieves additive throughput for data flows split over links.
  - **Latency improvement:** Use of multiple links in parallel increases the chance of channel access, thus reducing latency.
  - **Increased reliability:** Duplicating critical data packets over multiple links significantly increases reliability.
  - **Traffic separation/differentiation:** Assigning data flows to different links based on the application needs achieves traffic separation and/or differentiation.

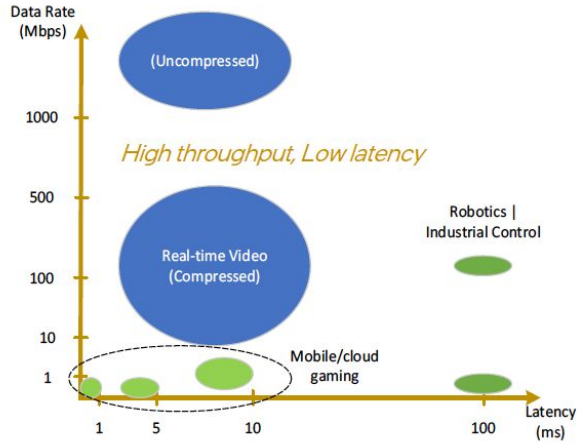
QOS Enhancement in WiFi 7

Enhanced QoS Management

- **Wi-Fi 6 can achieve single-digit millisecond** latency, but the worst-case latency can be high in congested environments.
- With the introduction of features like multi-link operation and 320 MHz channels in Wi-Fi 7, latency will be reduced even further.
- However, to provide enhanced QoS management, for example, deterministic low latency required by some usages (e.g., industrial IoT, AR/VR), new schemes need to be defined.

Wi-Fi 7 features for QoS enhancement

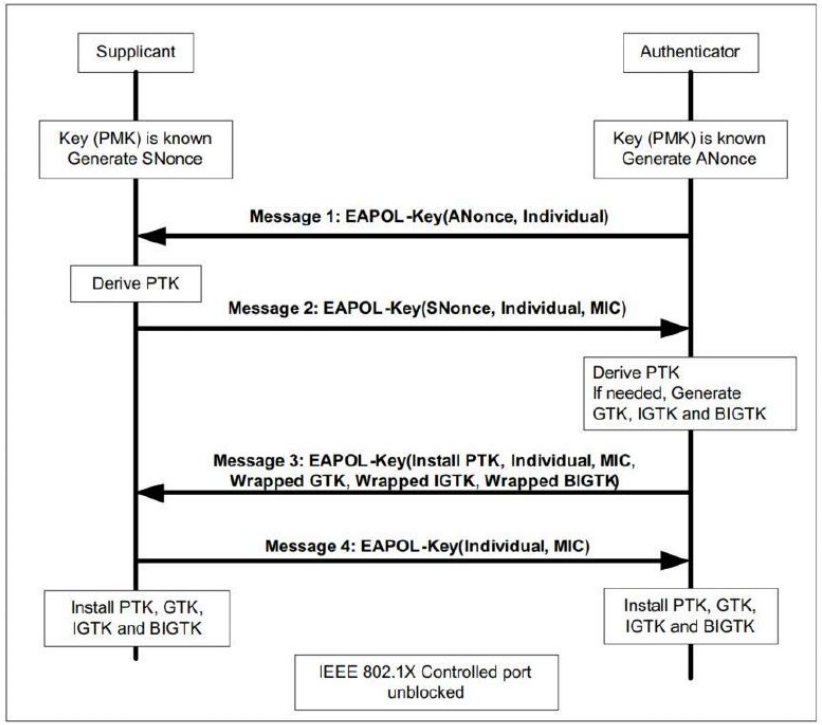
- Define QoS provisioning model with dedicated, deterministic, low-latency (LL) and reliable access category
- Enhanced channel access
  - Restricted service periods
  - National security and emergency preparedness (NSEP) priority service
  - Triggered peer-to-peer transmission



Enhanced Security in WiFi 7

Multi-link Security

- The 4-way handshake to establish pairwise and group keys is extended to cover Multi-link setup.
  - A pairwise master key (PMK) is established, and a pairwise transient key (PTK) is derived through a 4-way handshake between the non-AP MLD and the AP MLD.
  - The PMK, PTK, and the same packet number (PN) space are used for all the setup links for the pairwise transient key security association (PTKSA).
  - In contrast, different links use different group master key (GTK), integrity group temporal key (IGTK), and beacon integrity group temporal key (BIGTK) and each link has its own PN space.



Establishing pairwise and group keys

WiFi in 6GHz driving Outdoor- Frugal 5G (LMLC)

Power Levels for WiFI in 6GHz

Equipment Classes for Unlicensed 6 GHz

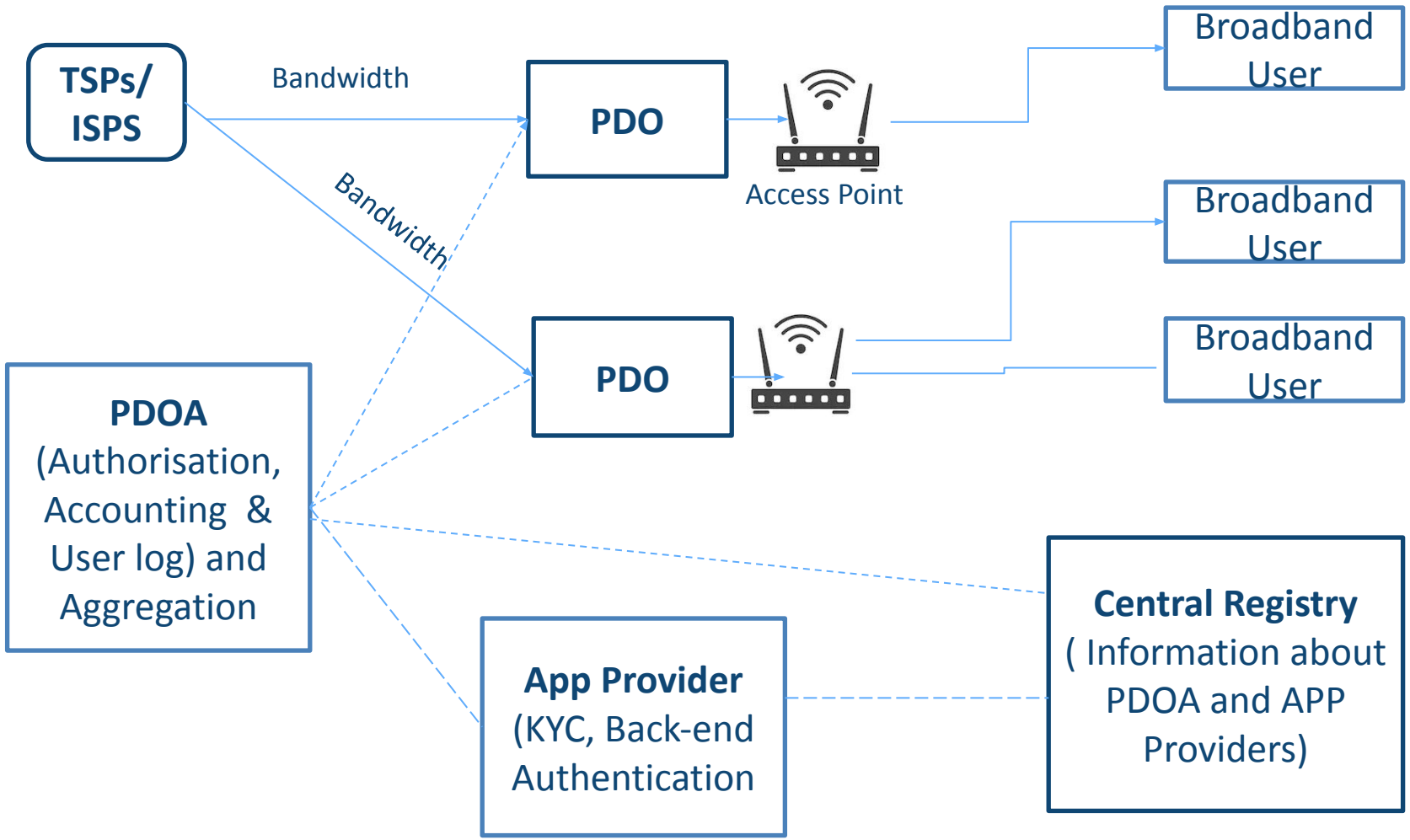
Class	Power	Access Requirements
Indoor Low Power AP**	5 dBm/MHz	Indoor Use Only
Standard Power AP	36 dBm	AFC
Portable Client Device	6 dB below AP (= -1 dBm/MHz)	Under Control of Access Point
Client to Client Communications	-1 dBm/MHz*	Indoor Use Only; in Range of AP*
Very Low Power Portable AP*	14 dBm EIRP*	Very Low Power*

Class	Power	Access Requirements
Indoor Low Power AP	23 dBm	Indoor Use Only
Outdoor Standard Power AP	TBD	Registration/Light License on National Basis
Portable Client Device	23 dBm	Under Control of Access Point
Very Low Power Portable AP	14 dBm	Very Low Power

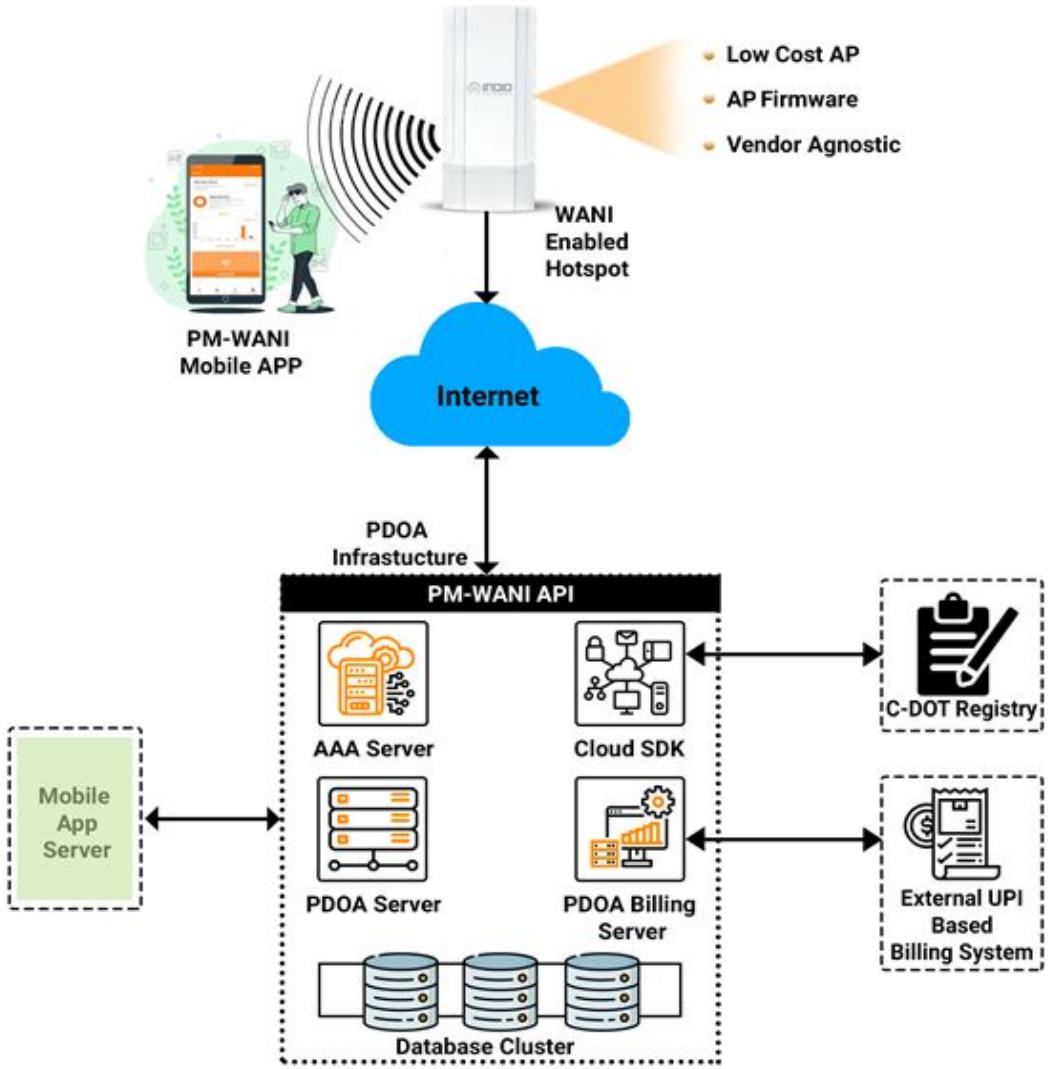
* Seeking authorization under Further Notice of Proposed Rulemaking (FNPRM)
** US LPI Rules based on 5 dBm/MHz PSD so that the larger the bandwidth, the greater the total power. FCC is now evaluating whether to increase LPI PSD to 8 dBm/MHz and 33 dBm total power for 320 MHz channel.

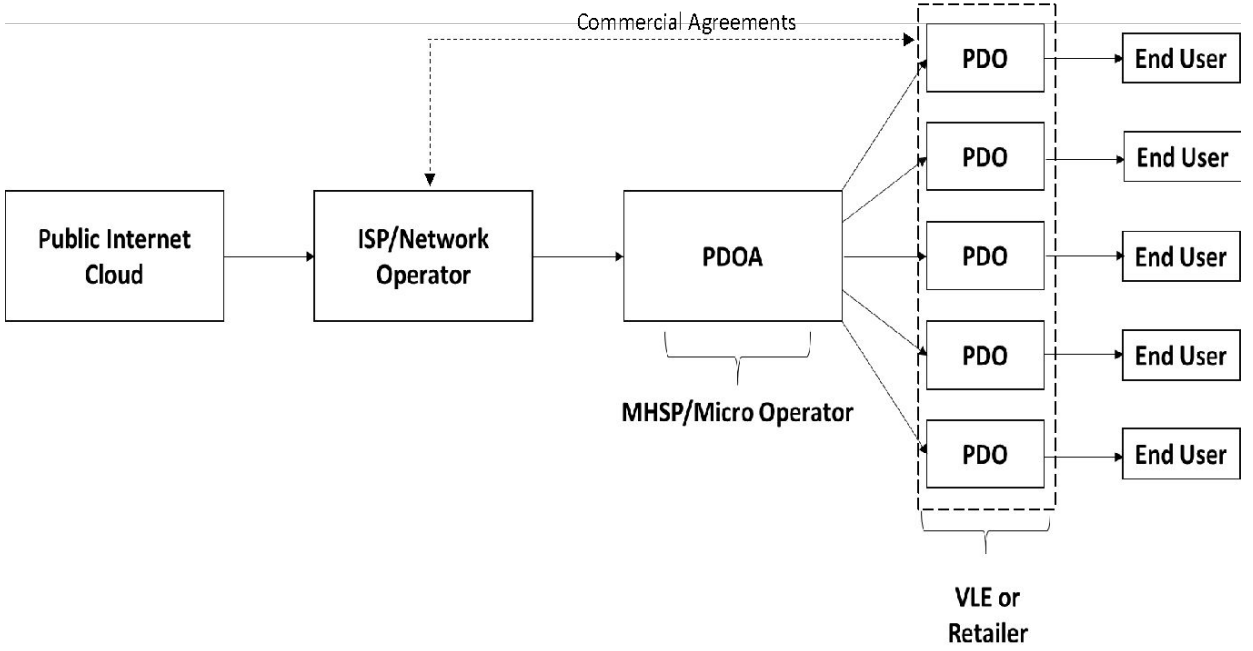
PM-WANI:PRIME MINISTER-WIFI ACCESS NETWORK INTERFACE- A Liberalised Framework for Last Mile Connectivity(LMC) in Bharat

WANI - Unbundled and Distributed Architecture



PM-WANI System Architecture

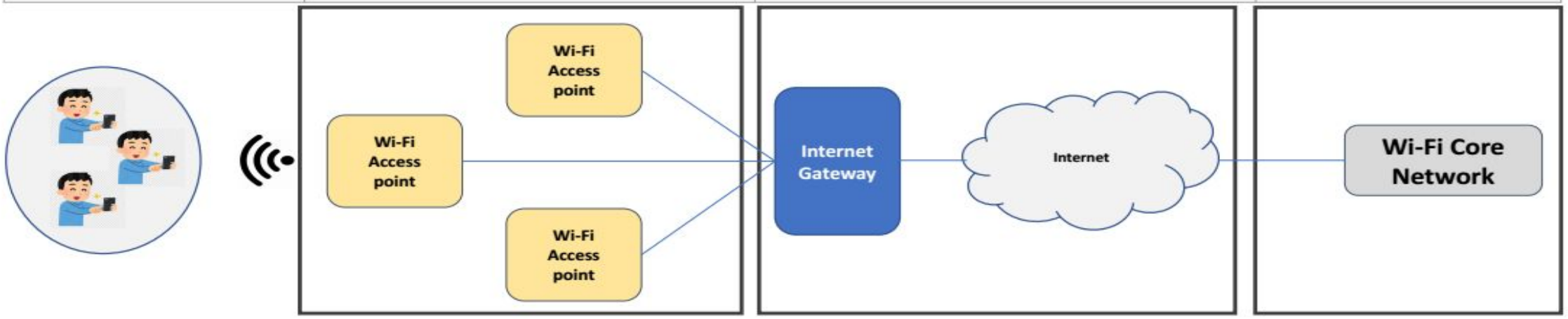




PM-WANI-- Multi-partner play for end-to-end service delivery

Deployment in India as PMWANI Program

Service Provider	Wi-Fi Access Network Infrastructure	Internet Infrastructure	Wi-Fi Core Network Infrastructure
Wi-Fi VNO	**Wi-Fi VNO**	**ISP**	**MNO**
Prepaid/Postpaid Data plans	Installation of Access point, Power, O&M	Wi-Fi VNO arranges Internet backhaul from local ISPs	providing AAA, OSS, BSS functions for Wi-Fi
VLE (Village Level Entrepreneurs) or PDO (Public Data Office)	**VLE or PDO (Public Data Office)**	**Local ISP**	**Wi-Fi Aggregator or PDO Aggregator**



In this deployment scenario, New entity (Wi-Fi VNO) offers services by using its own Wi-Fi Access network infrastructure. Wi-FI VNO also arranges internet backhaul from local ISPs and takes service from MNO for Wi-Fi core functions.

Social Impact-Using multiplier effect of an idea whose time has come.- Archimedes' Principle

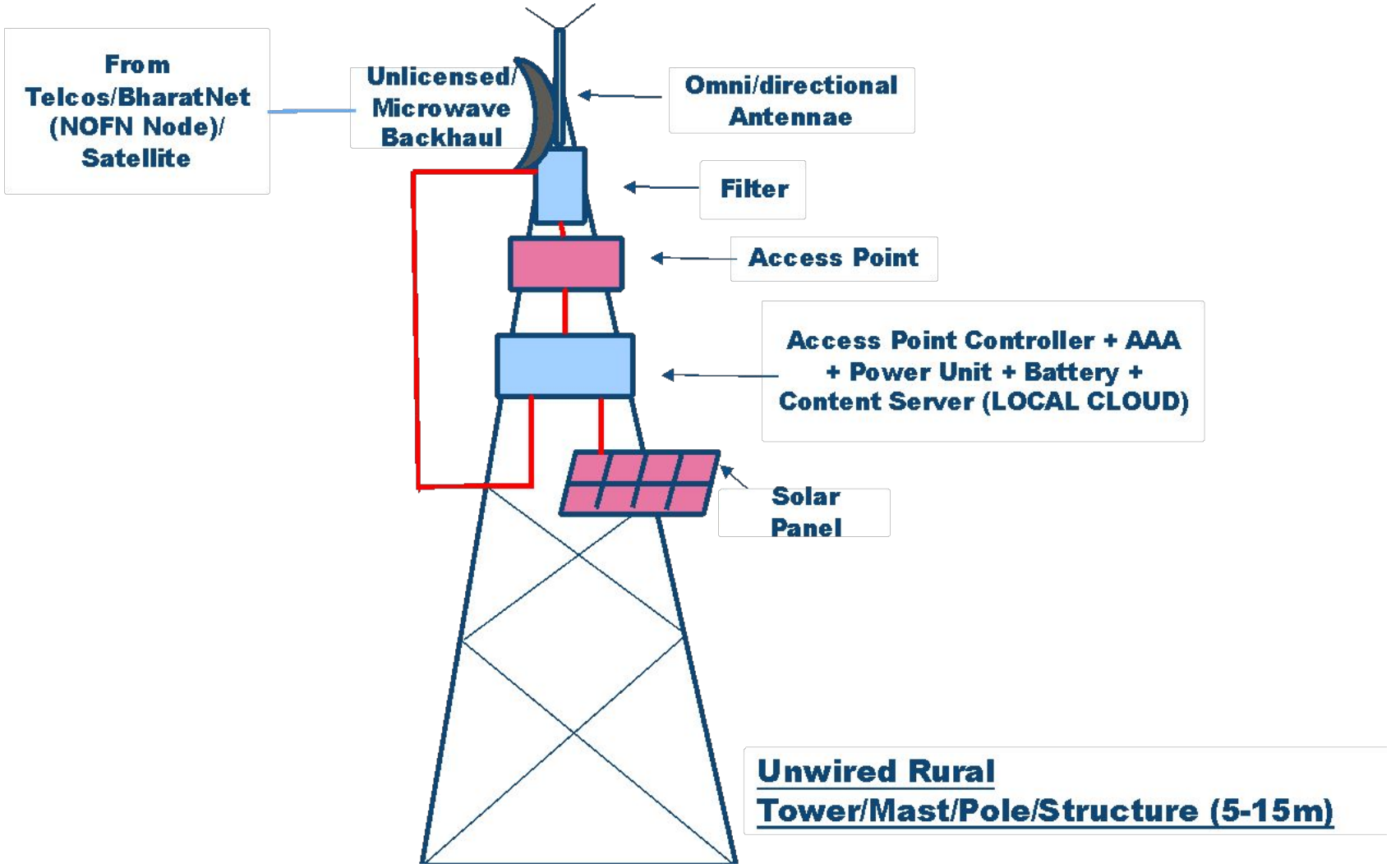
"Look at the world around you. With the slightest push, at just the right place, it can be tipped"

"Give me a rod (mast) long enough strong enough- and we can change the life-style of the rural folks"

Managed Hotspot Service Provider (MHSP) as WANI PDOA

Value Innovation to achieve Affordability - Everything on Tower

(5Ls- Low Cost, Low Power, Low Maintenance, Local Control, Local Cloud)



Blockchain based Decentralized PM-WANI

Innovation;

Blockchain provides a compelling Use case to adopt Blockchain technology for PDO and User registration for benefits of Decentralization, Transparency, Efficiency and Ubiquity.

This can help to create a network of PDOs(Public Data Offices) and PDOAs(Public Data Office Aggregators) which will enable users to find and access the public Wi-fi in a cost-effective manner.

User Information like KYC, Identity and Package details will be stored in a Distributed Ledger Platform and can be verified by Smart Contracts thus making it easy for the Users to connect to any PDO.

Major Components

DAO

- A community based Wifi-Cooperative as Decentralised Autonomous Organisation can be established to create a Blockchain based platform and lay down the governing [illegible]uto-execution.

PDOA

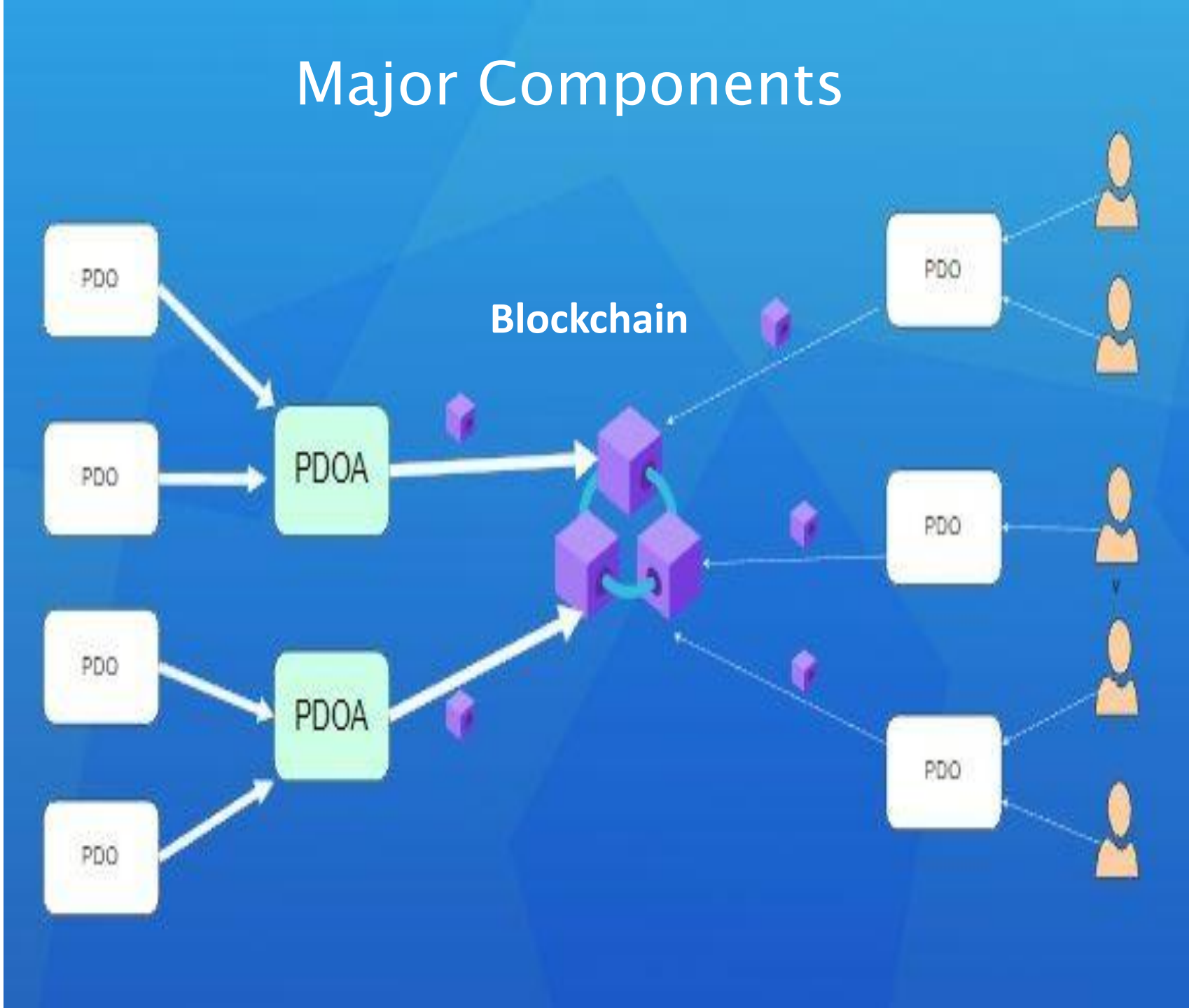
- PDOA an be mandated to register as a Node with the Wifi DAO and add all the PDOs functioning under it.

PDO

- Local entrepreneurs will provide the Wi-fi access to the Users.
- PDOs will be adding users to the Platform and implement the eKYC and

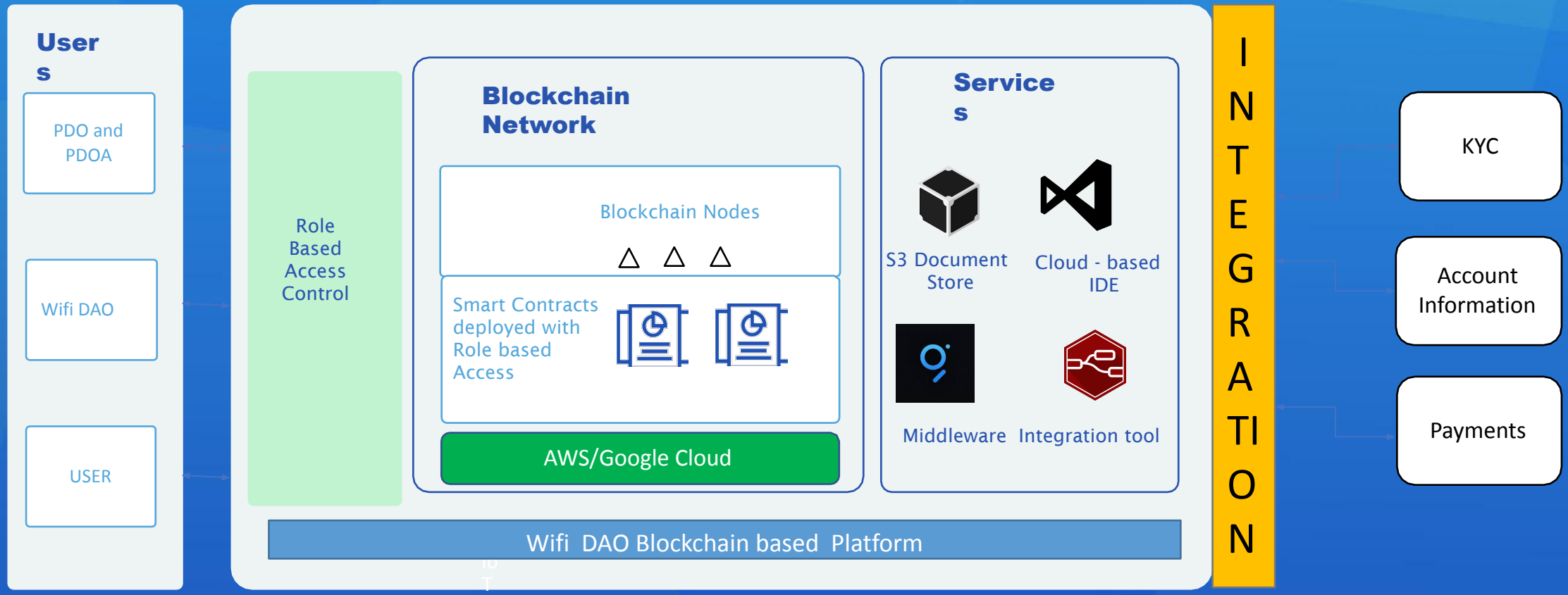
Users

- Users can subscribe to the network and buy the suitable packages.
- The mobile application can be used to find Wi-fi zones and connect to Wi-fi



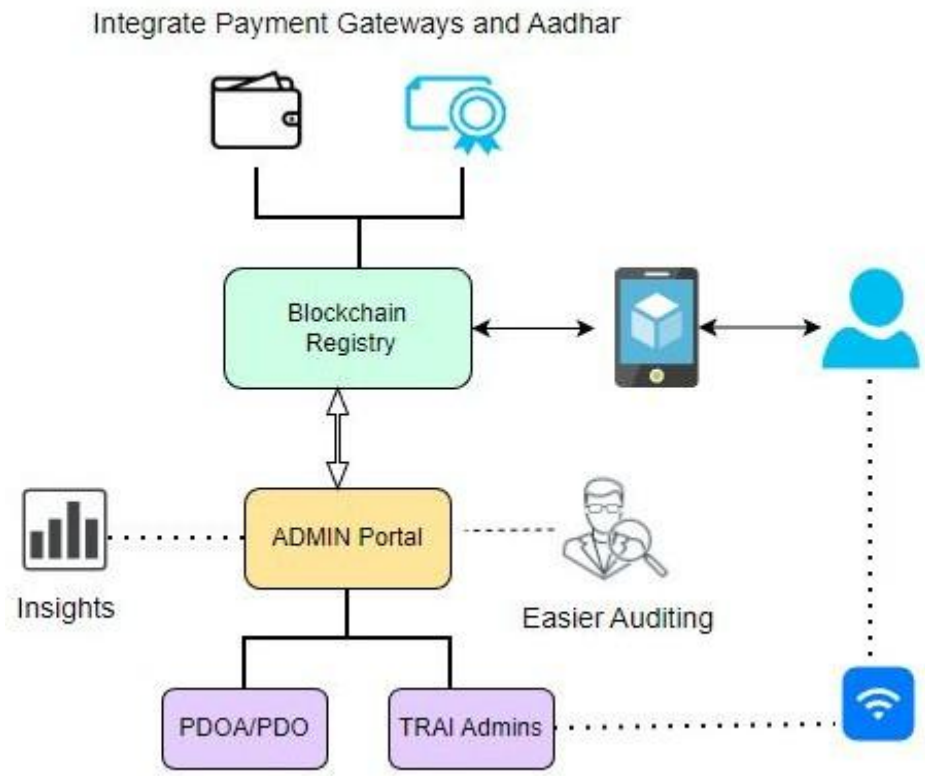
High Level Architecture

- Wifi DAO would form the Blockchain Platform and policies/roles for the network to operate
- The stakeholders would be given secure access over the Blockchain Platform
- Information will be shared securely between the participants on p2p basis



Solution Approach

- It is proposed to create a blockchain based distributed data ledger platform which allows sharing of necessary information among all the major players and users. The system shall be future proof and scalable
- All the interactions will be noted on smart contracts, with the required approvals. The Admin portal shall have role-based authentication which shall provide valuable insights.
- Auditors or other approved officials can be given permission to view data by the DAO in automated way.
- The portal will provide real-time information of an active User to any PDO, thus eliminating re-registering process and providing a superior User experience.
- The portal will hook with Sovereign Identity Aadhar and Payments Gateway to enable KYC and fiat payments to the PDOAs and PDOs.



Flow

Registration

PDOA registers to the Blockchain registry and add PDOs.
Users registers through PDO.

Authentication

Role Based Authentication for Admin Portal will be implemented
User registration will be validated through Aadhar integration

Usage

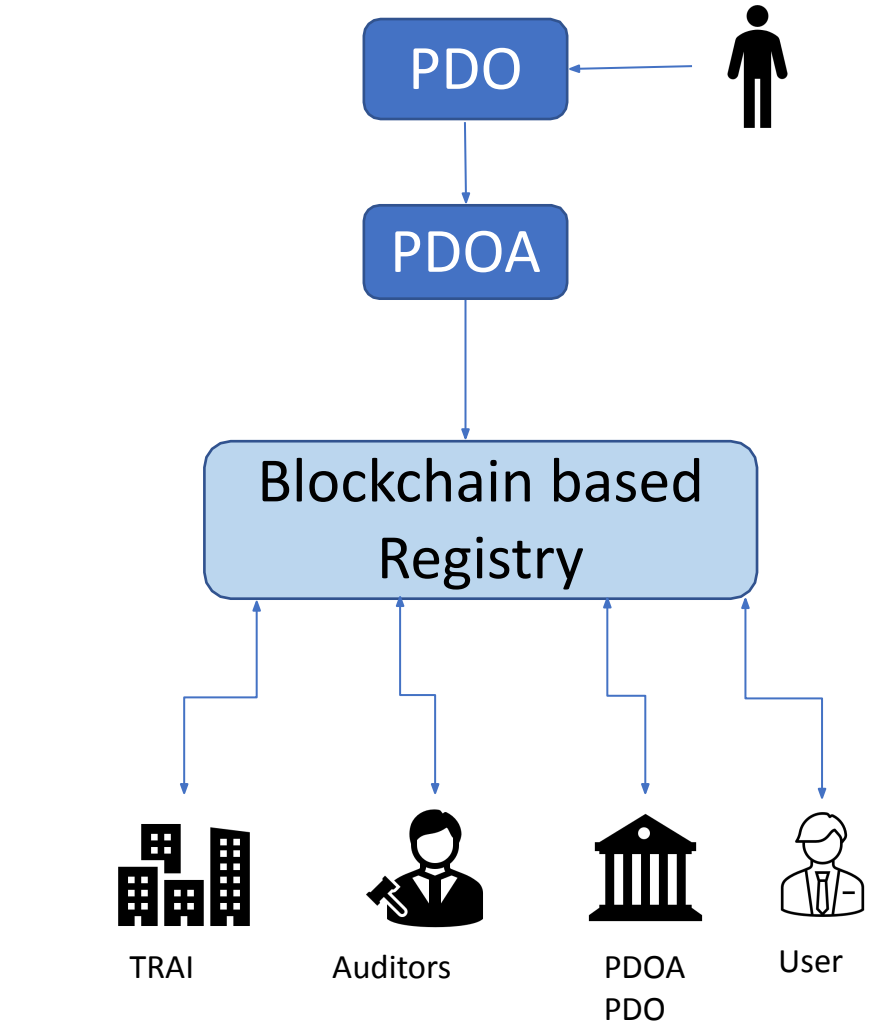
User data for all the Users will be updated by the verified Wi-fi access points.
Users can verify the MAC-ID with the nearest SSID.

Monitoring

Auditors will be given access to the Admin portal.
The Admin portal shall have dashboards that will provide key insights.

Payment

Payments for the services provided by PDOs and PDOAs
can be automated by integrating with a payment gateways



Integration of Payment Gateways and Aadhar through external systems

OpenRoaming- Making WiFi Seamless

OpenRoaming: Anywhere & Any Network Connected Wi-Fi Clients

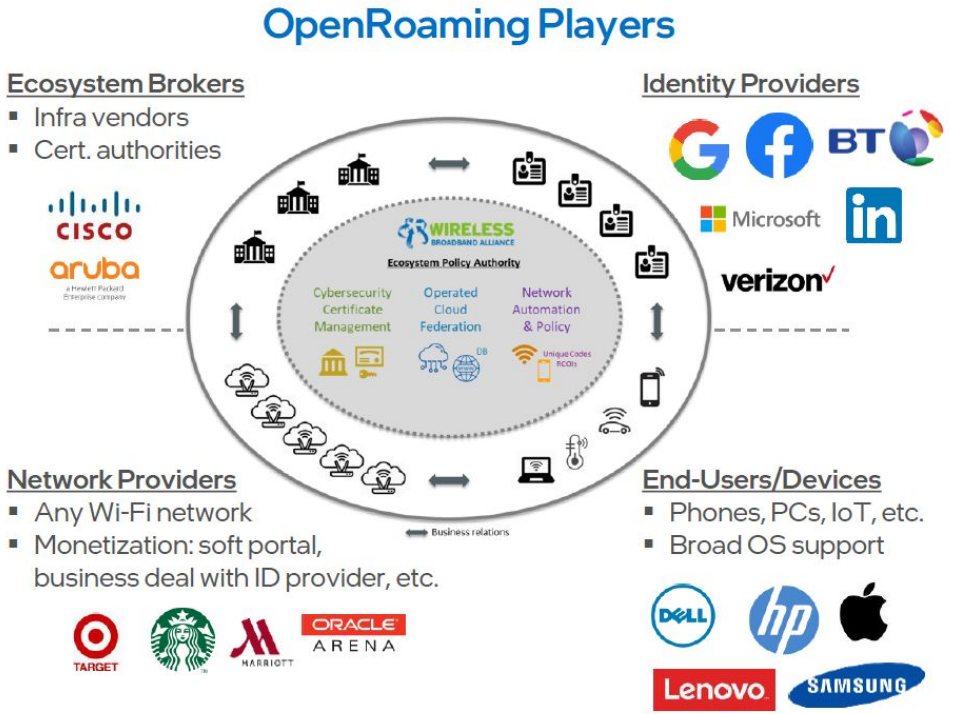
Problem Statement

Wi-Fi hotspots can be found virtually everywhere, but clients connecting to these hotspots are either disallowed (e.g., lack of credentials) or cumbersome (e.g., captive portal).

Solution

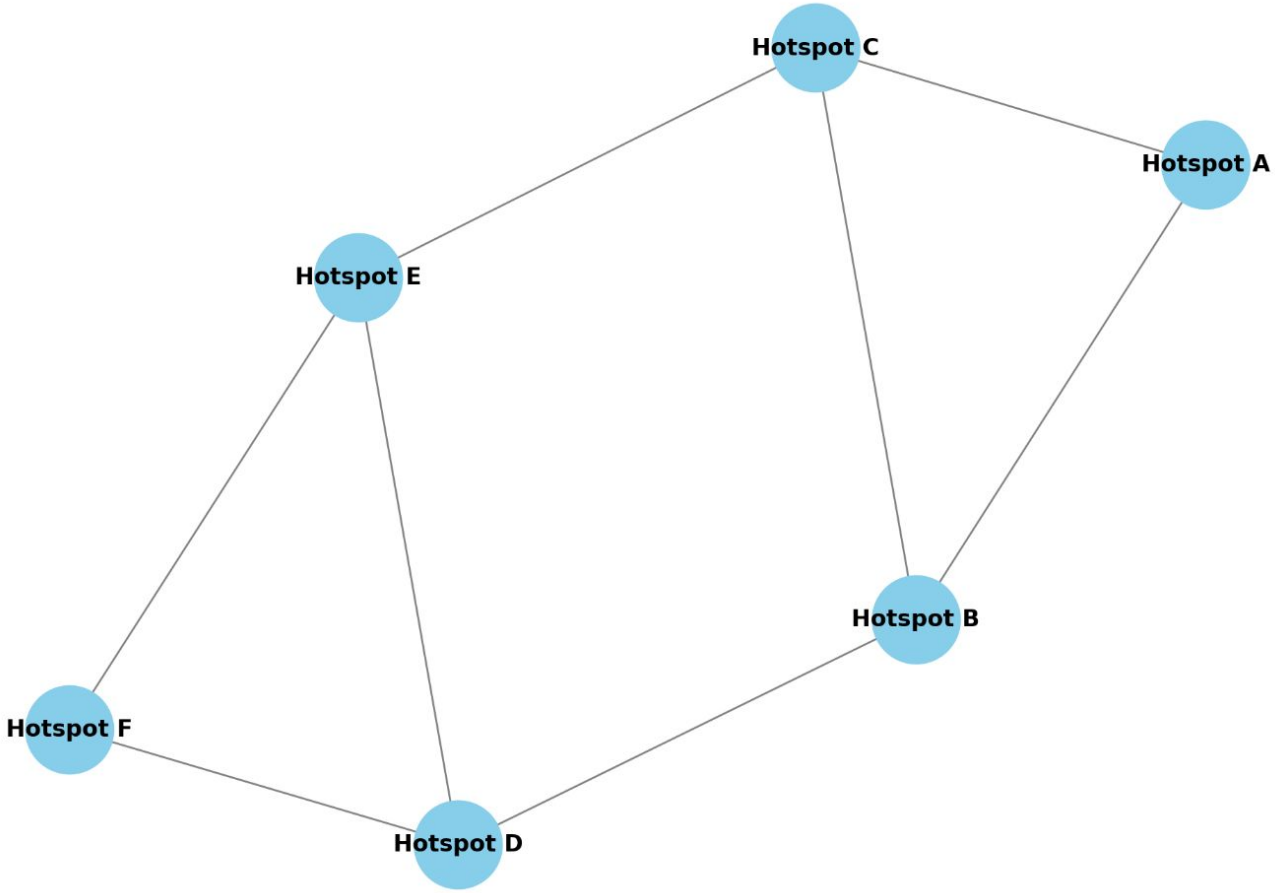
OpenRoaming (OR) is an industry initiative that aims at connecting clients to Wi-Fi networks as seamlessly and pervasively as in cellular.

- Based on Passpoint technology
- Scalable, many-to-many business relationships



OpenRoaming enables seamless connectivity of Wi-Fi clients across networks

Decentralized Wireless (DeWi) Network



Decentralized nature of the network, where multiple Wi-Fi hotspots (nodes) communicate with each other in a P2P Mesh configuration, enabling Redundancy, Availability and Resilience.

DeWi Innovation:

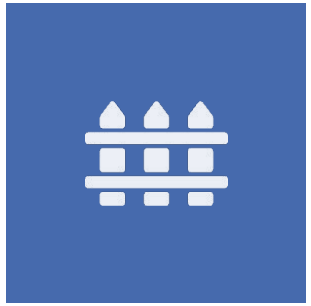
Blockchain / Mesh Networking / dApps

Blockchain Protocols

Decentralization, Smart contracts Consensus mechanisms, such as proof-of-work or proof-of-stake, that enable peer-to-peer transactions and security in a distributed network.

Mesh Networking

Wireless nodes that form a decentralized network, enabling data to be routed through multiple hops without a central authority.



Security Mechanisms

Cryptographic techniques, such as encryption and authentication, that ensure the integrity and confidentiality of data in a decentralized wireless environment.

Decentralized Applications (dApps)

Distributed applications that leverage the capabilities of decentralized wireless networks to provide services and functionality to users.

Decentralized Wireless (DeWi) combines Blockchain, Mesh networking, and Security mechanisms to create a decentralized, resilient, and secure wireless infrastructure, enabling new applications and services.

Blockchain Elements in DeWi

Blockchain's Role in DeWi	Consensus Mechanisms in DeWi	Smart Contracts in DeWi	Decentralized Governance(DAO) in DeWi
Explore how blockchain technology is leveraged in the context of Decentralized Wireless (DeWi) networks, enabling decentralized governance, secure transactions, and trusted data management.	Discuss the various consensus mechanisms, such as Proof-of-Work (PoW), Proof-of-Stake (PoS), or Proof-of-Authority (PoA), that are used to maintain the integrity and security of the blockchain in DeWi networks.	Examine how smart contracts, self-executing agreements stored on the blockchain, can be utilized in DeWi to automate network operations, facilitate transactions, and enforce service-level agreements between participants.	Explore the decentralized governance models enabled by blockchain in DeWi, where network participants collectively make decisions, manage resources, and ensure the overall system's resilience and responsiveness.

Consensus Mechanisms in DeWi-Options

- **Proof-of-Work (PoW)**

  A consensus mechanism where network participants (miners) compete to solve complex mathematical problems to validate transactions and add new blocks to the blockchain. The miner who solves the problem first is rewarded with cryptocurrency.

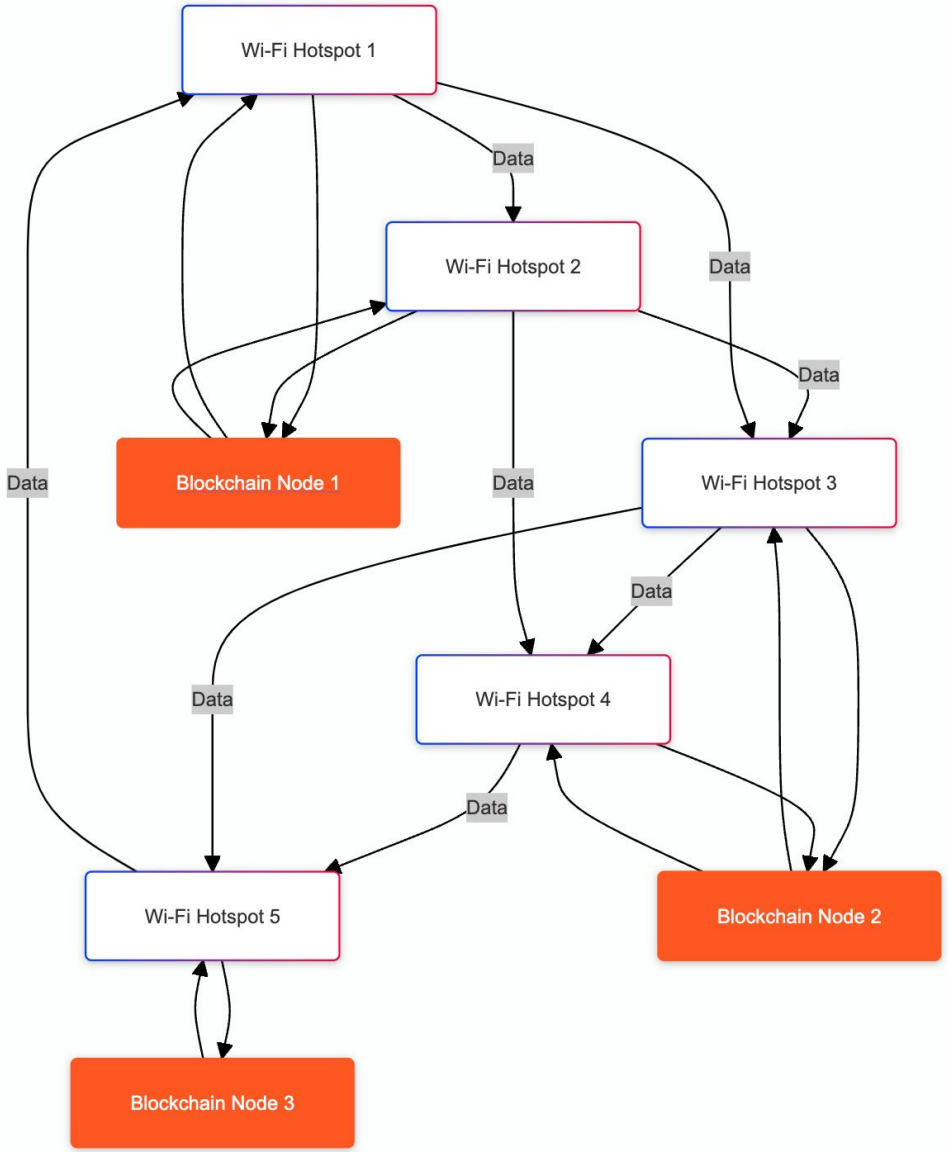
- **Proof-of-Stake (PoS)**

  A consensus mechanism where network participants (validators) stake their cryptocurrency to validate transactions and add new blocks to the blockchain. Validators are selected based on the amount of cryptocurrency they have staked, and they earn rewards for their participation.

- **Proof-of-Authority (PoA)**

  A consensus mechanism where a pre-approved set of network participants (authorities) are responsible for validating transactions and adding new blocks to the blockchain. This approach is often used in private or consortium blockchains and provides faster transaction times but with less decentralization than PoW or PoS.

Decentralization: Rethinking Network Ownership



- ✔ Wi-Fi Hotspots as nodes.
- ✔ Blockchain integration through a Decentralised Ledger.
- ✔ Data flow arrows depicting data movement and transaction validation by Blockchain nodes.

Security Mechanisms in DeWi

Cryptographic Methods

DeWi utilizes advanced cryptographic techniques, such as public-key cryptography and hashing algorithms, to ensure secure communication, data integrity, and authentication.

Decentralized Authentication

DeWi employs decentralized authentication mechanisms, such as blockchain-based identity management and distributed access control, to enable secure access to the network without relying on centralized authorities.

Protection Against Network Attacks

DeWi incorporates security measures to mitigate common network attacks, including distributed denial-of-service (DDoS) attacks, man-in-the-middle attacks, and routing protocol vulnerabilities.

Secure Mesh Networking

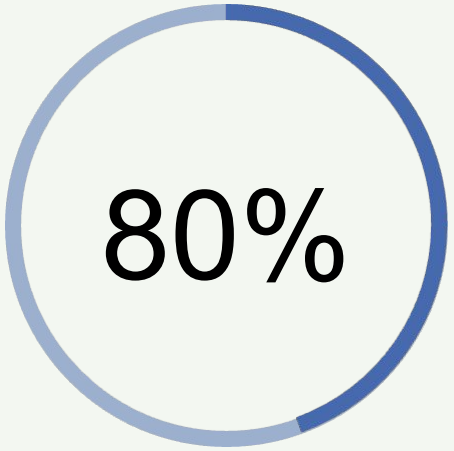
The mesh network architecture of DeWi provides inherent resilience against single points of failure and enables secure data routing through multiple redundant paths, improving overall network security.

Smart Contract-based Security

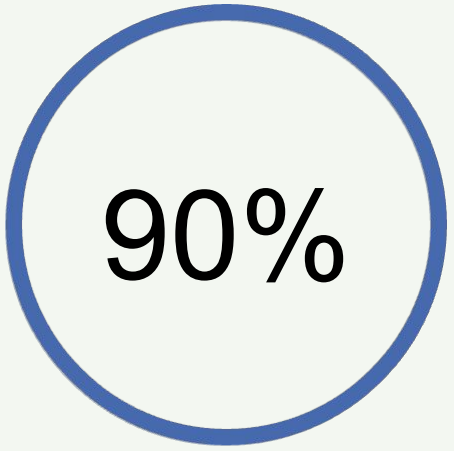
DeWi leverages smart contracts to enforce security policies, manage access control, and automate security-critical operations, reducing the risk of human error and improving the overall security posture.

Protecting against Network Attacks

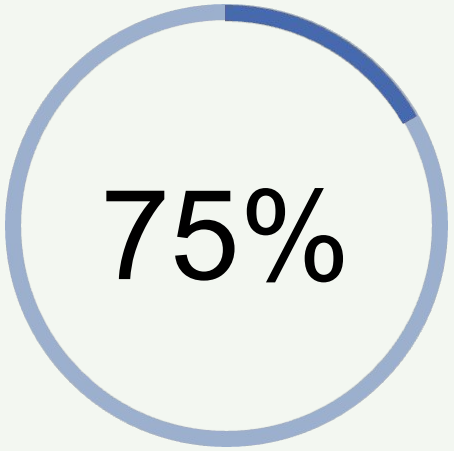
Comparison of effectiveness of security measures against common DeWi network attacks (0-100%)



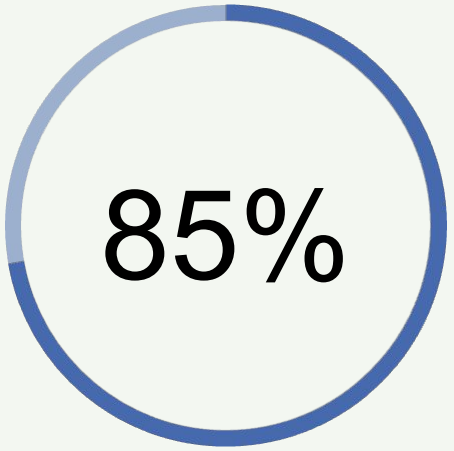
DDoS Attack Protection



Man-in-the-Middle Prevention

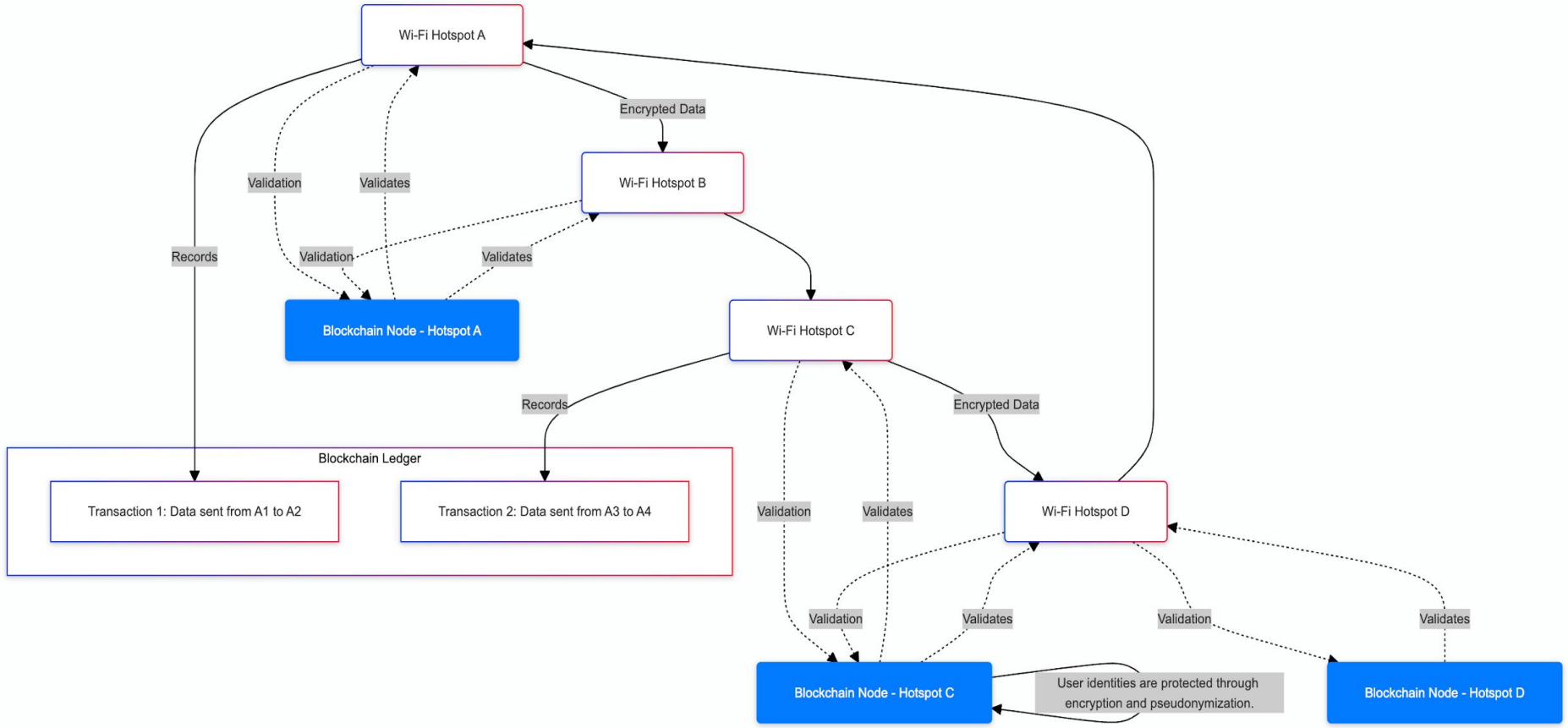


Sybil Attack Mitigation



Encryption & Authentication

Data Flow: Privacy and Security in DeWi

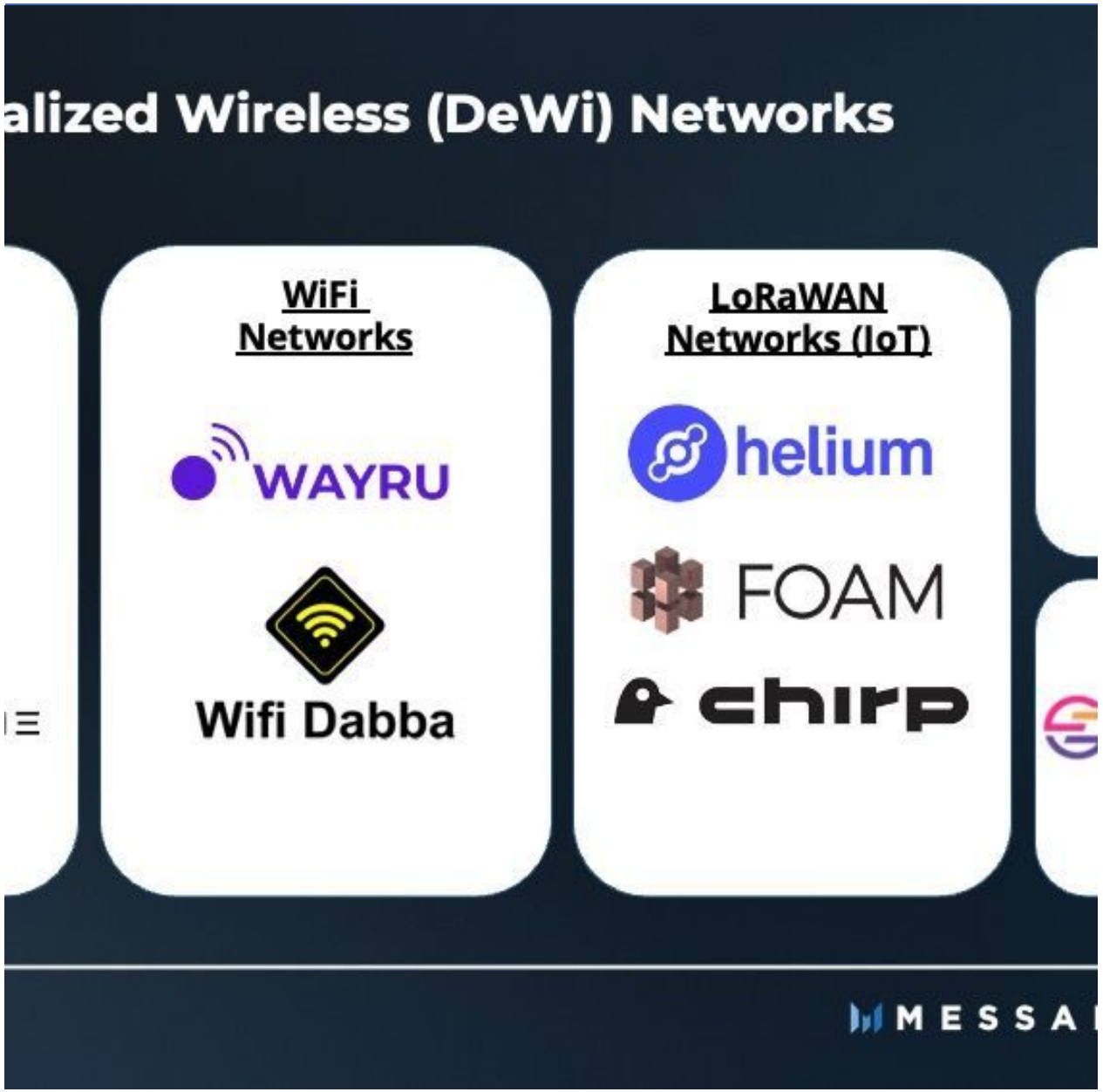


Security and Privacy protections provided by Blockchain in a DeWi network, includes:

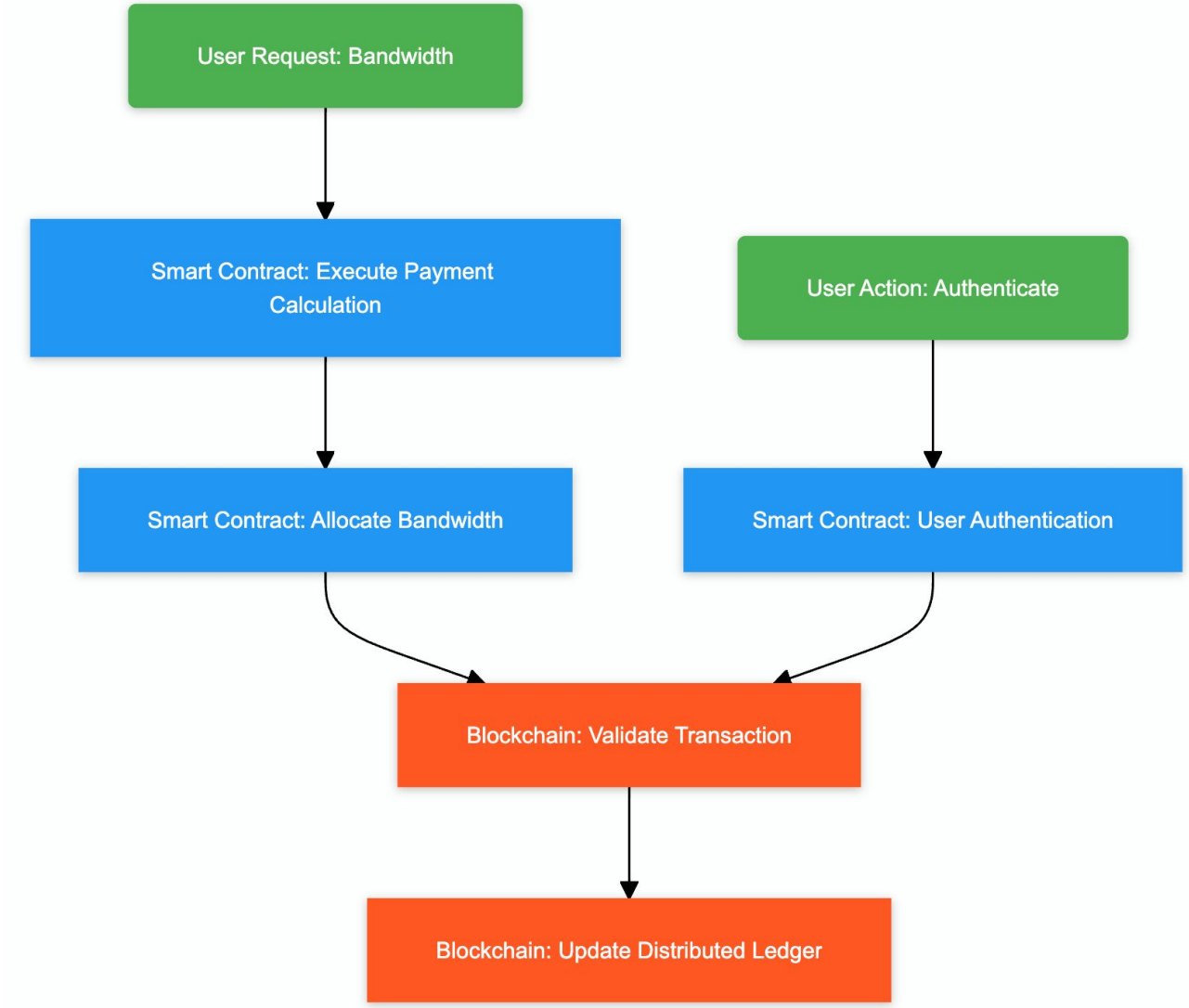
a. **Encrypted Data Transmission:** The diagram shows arrows marked with "Encrypted Data" moving between nodes (hotspots) to indicate secure data transmission.
b. **Blockchain Ledger:** A subgraph titled "Blockchain Ledger" includes transactions, illustrating how each transaction is recorded and validated by the blockchain nodes.
c. **User Privacy:** A note explains that user identities are protected through encryption and pseudonymization, ensuring privacy.

Smart Contracts in DeWi

Smart contracts play a crucial role in enabling decentralized governance and automation within the Decentralized Wireless (DeWi) ecosystem. These self-executing digital agreements allow for the transparent and autonomous management of various aspects of the DeWi network, including resource allocation, service provisioning, and conflict resolution.



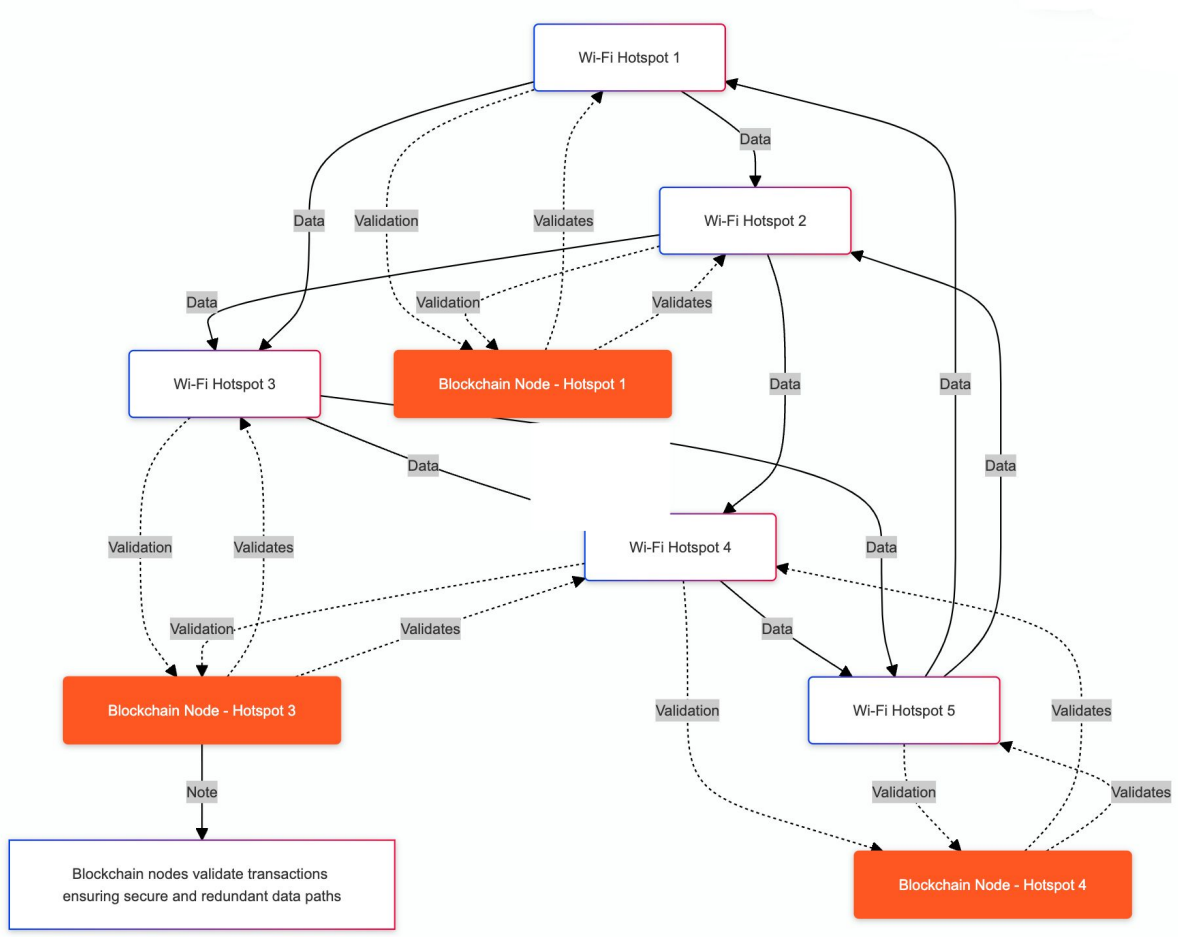
DeWi: Smart Contract Operation Flow



Mesh Networking:

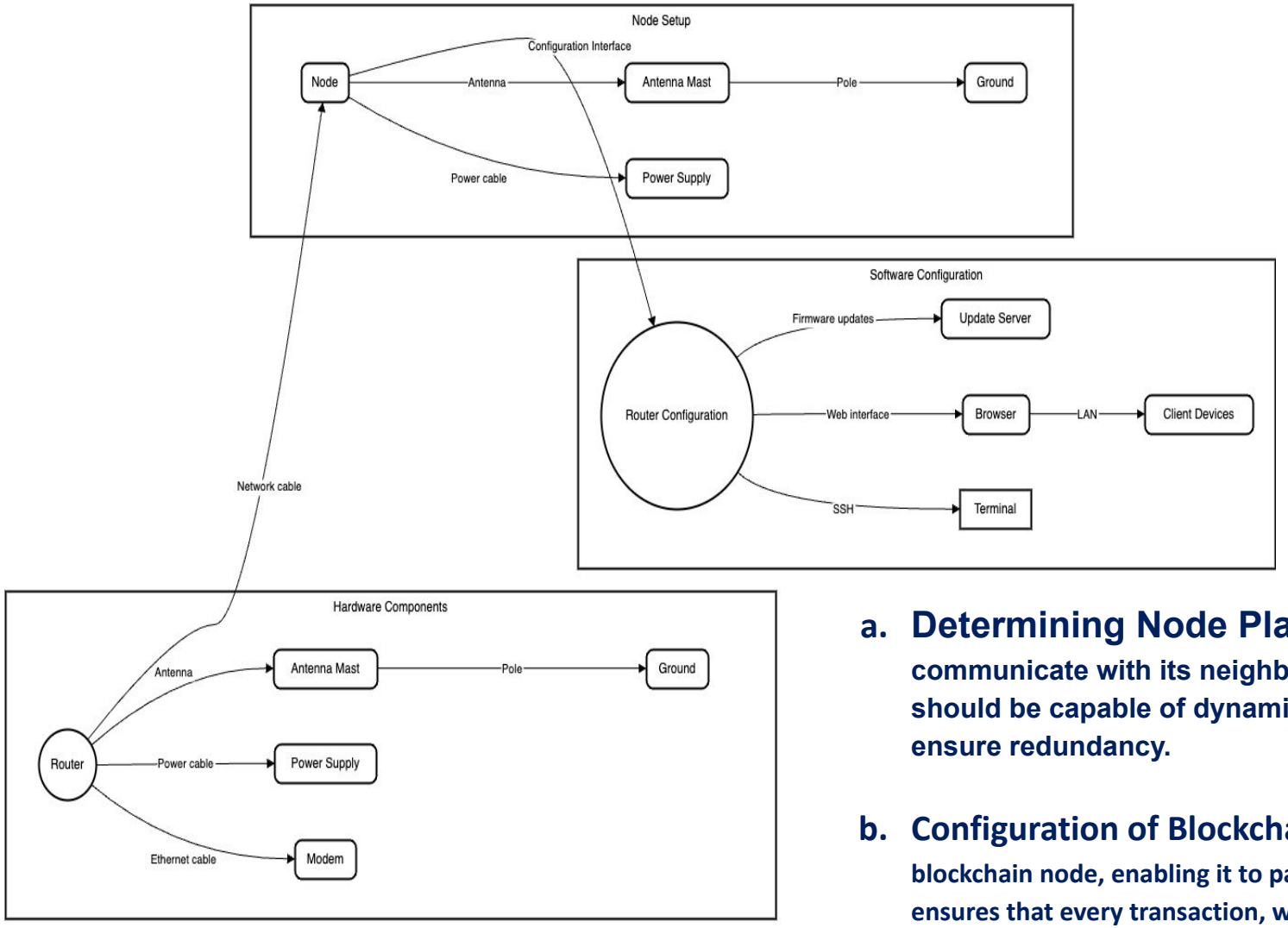
Building Resilience and Scalability through Blockchain-enabled Infrastructure

- The mesh network architecture is inherently scalable.
- As more hotspots join the network, the coverage area expands, and the network's capacity increases.
- This scalability is particularly advantageous in urban environments where dense populations can place significant demands on network resources.
- In rural areas, mesh networking extends the reach of the network, providing connectivity to regions that are otherwise difficult to serve.
- Blockchain's role in mesh networking is critical.
- It ensures that each node operates securely within the network, with transactions being recorded on the blockchain to prevent fraud, misuse, or unauthorized access.
- Blockchain-enabled infrastructure allows DeWi networks to be highly resilient, scalable, and self-healing, as each node can independently validate and route data, adapting to changes in the network environment.



- Nodes in a Mesh Network: Multiple interconnected Wi-Fi hotspots.
- Blockchain Nodes: Highlighted nodes also serve as blockchain nodes.
- Data Paths: Illustrating redundant and secure paths for data.

Node Placement & Strategic Design



a. **Determining Node Placement**: Each node must be configured to communicate with its neighboring nodes, forming a mesh network. The network should be capable of dynamically routing data to optimize performance and ensure redundancy.

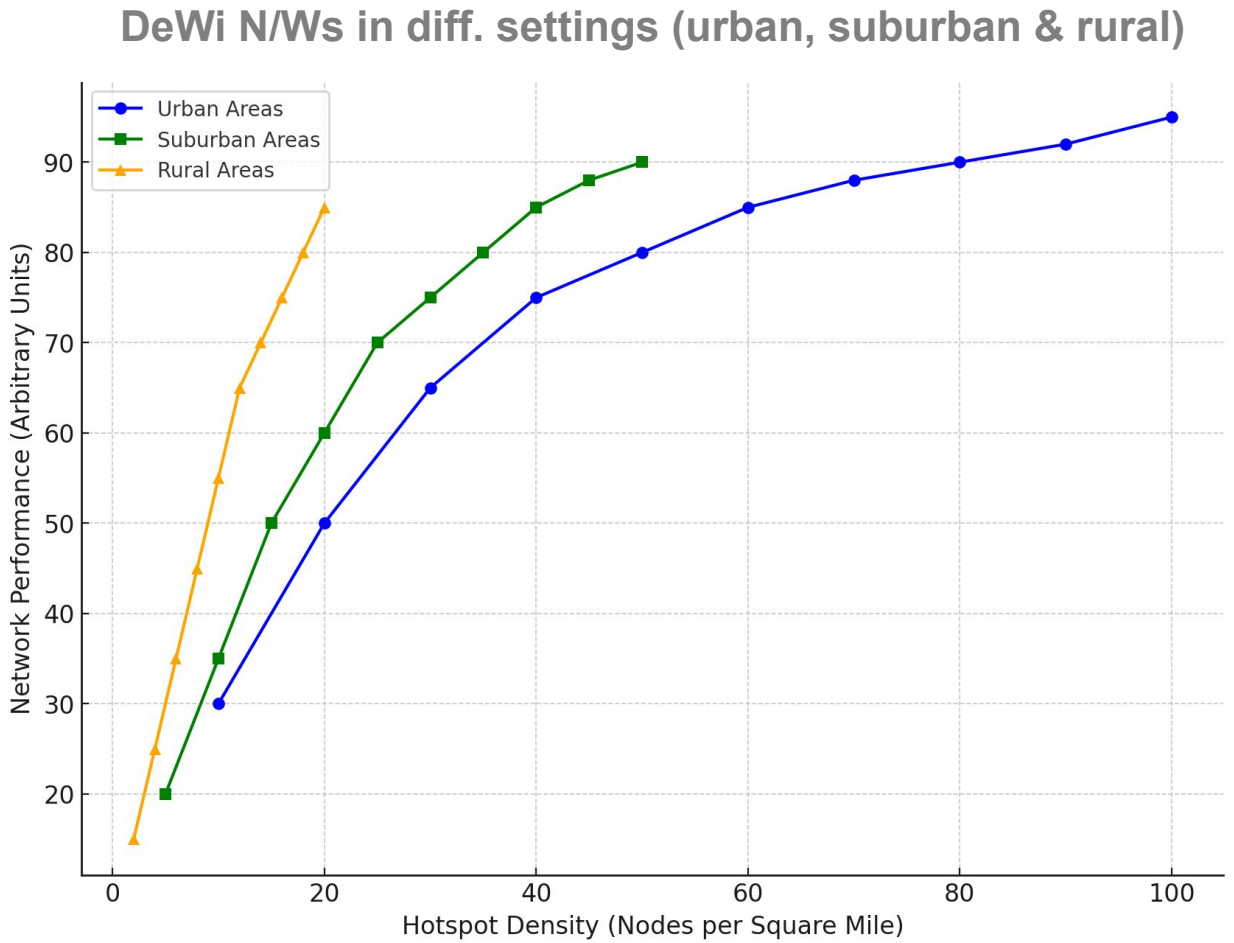
b. **Configuration of Blockchain Nodes**: Each Wi-Fi hotspot must be equipped with a blockchain node, enabling it to participate in the network's distributed ledger. This setup ensures that every transaction, whether it’s bandwidth sharing, data transmission, or user authentication, is securely processed and recorded on the Blockchain.

Decentralized Authentication in DeWi

Decentralized Authentication Mechanism	How it Secures DeWi Networks
Public Key Infrastructure (PKI)	PKI enables secure communication and identity verification in DeWi networks. Digital certificates issued by a trusted Certificate Authority (CA) bind public keys to user/device identities, allowing for authentication, encryption, and integrity protection
Decentralised Identity(DID) Systems	Decentralized identity systems, such as self-sovereign identity (SSI) and decentralized identifiers (DIDs), enable users and devices to manage their own digital identities without relying on a central authority. This enhances privacy and security in DeWi networks by giving individuals control over their personal data

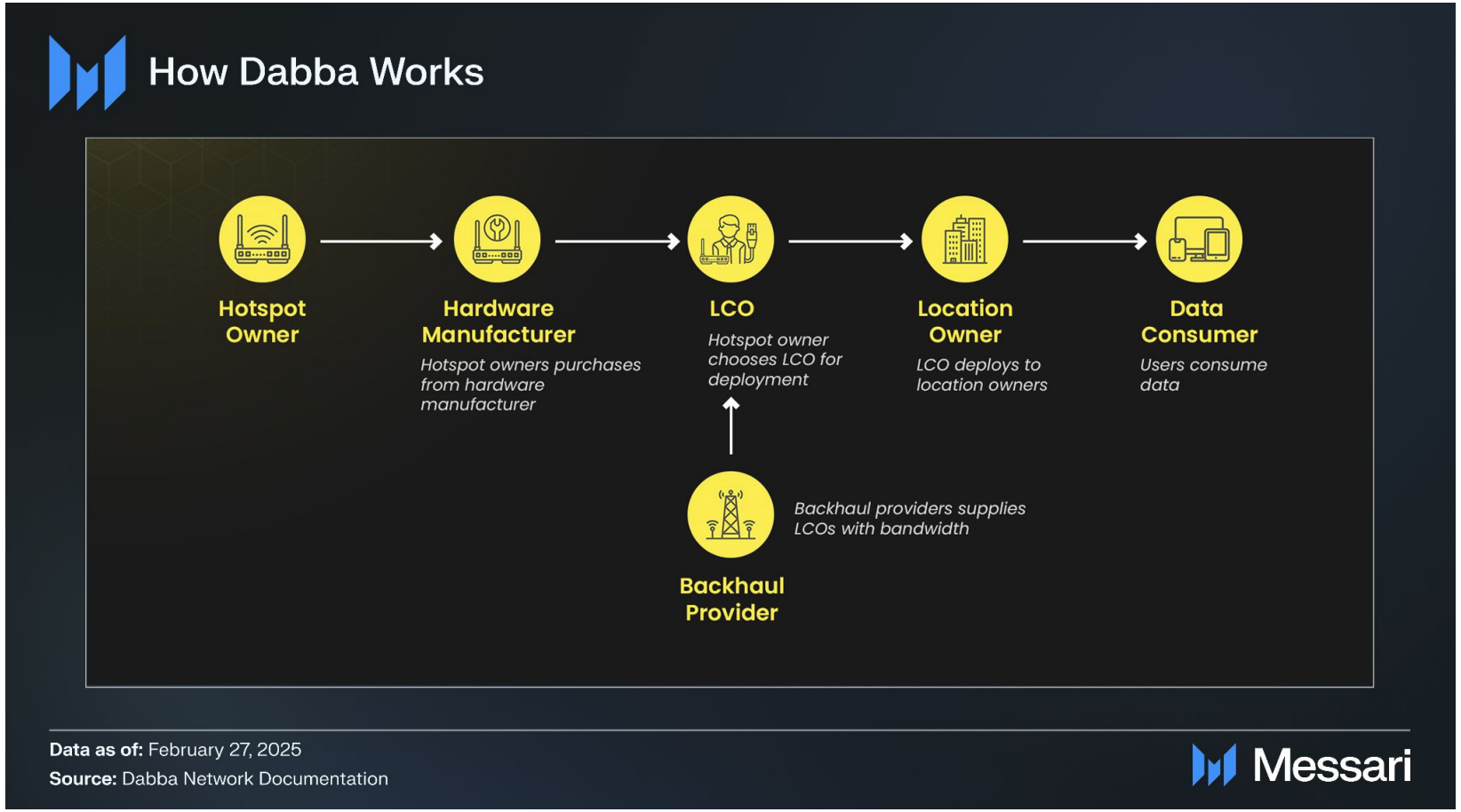
***The information in this table is derived from various academic and industry sources on decentralized authentication and security in decentralized wireless (DeWi) networks**.

Scalability of DeWi Networks in Different Settings

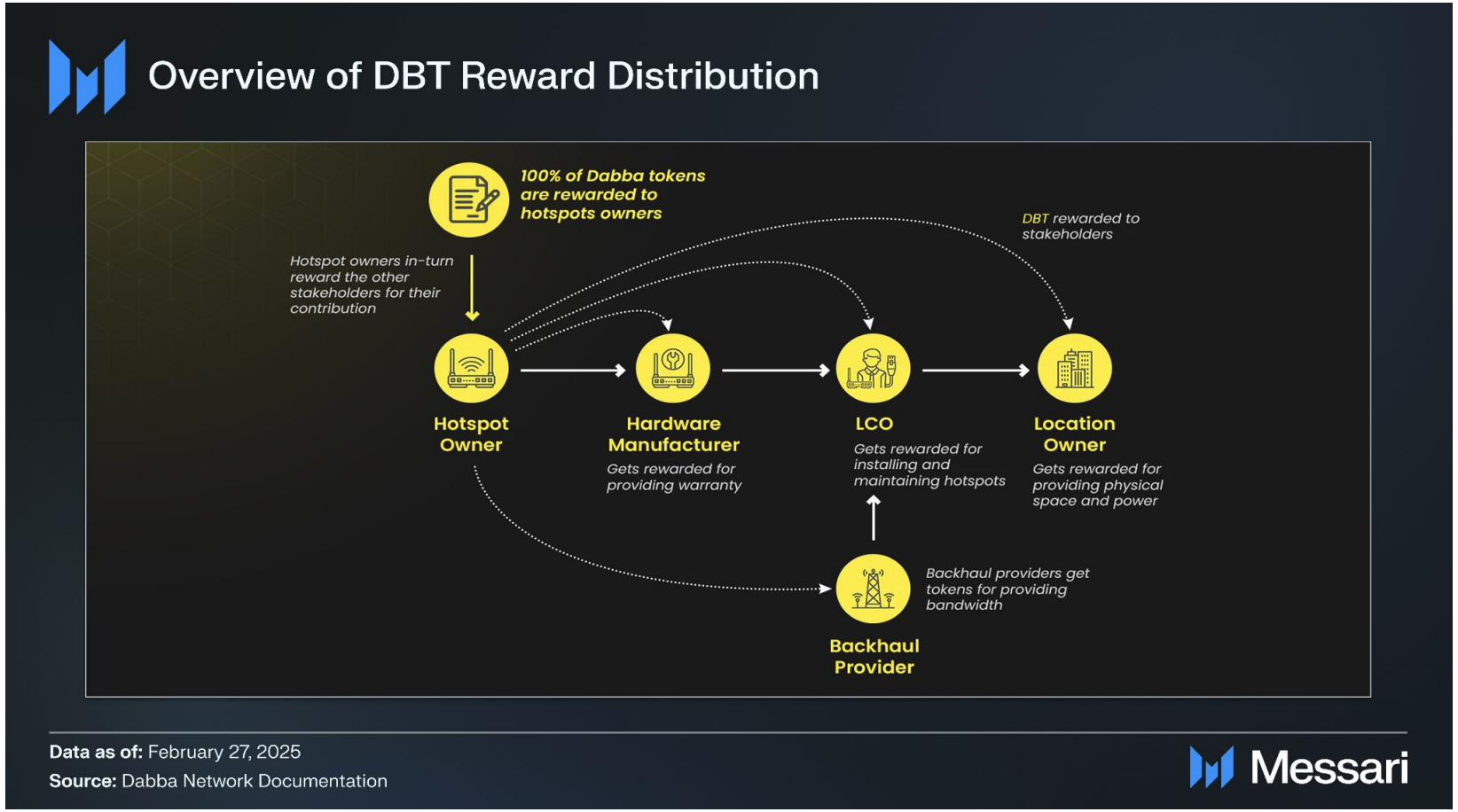


Network performance improves as the density of Wi-Fi hotspots increases, with urban areas showing the highest potential performance due to higher node density.

A DeWi Use Case in India- WiFi Dabba



A DeWi Use Case in India- WiFi Dabba Contd.----



Next step-Timeline for a POC to make Users also Owners- Towards Phygital Public Good

1

Discovery & analysis

analyse the use case and assess the potential fit for blockchain.

1 WEEKS

2

Network deployment

Deployment of the Blockchain network

3

Initial development

Development of the backend application, admin platform, and smart contracts for the solution.

6-7 WEEKS

4

Iterative Testing

Test the initial smart contract, admin platform build and improve according to business needs iteratively.

1-2 WEEKS

5

User Acceptance Testing

Aggregate data from testing various scenarios to find insights on how to proceed with the Go Live.

1 WEEKS

6

MVP Live!

Based on your testing and evaluation, move forward with the production launch.

Go Live!

Total -Approx. 3 Months

Thank You

Dr. Satya N. Gupta
sg.ngnguru@gmail.com

(Download complete PM-WANI Framework and various Business Models in the book by author from www.digigaonfoundation.com)