SatyaSpeak

IAFI WiFi Day Seminar

19th June.2025@New Delhi, Bharat

Blockchain 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

Professor of Practice- South Asian University

Secretary General- ITU APT Foundation of India

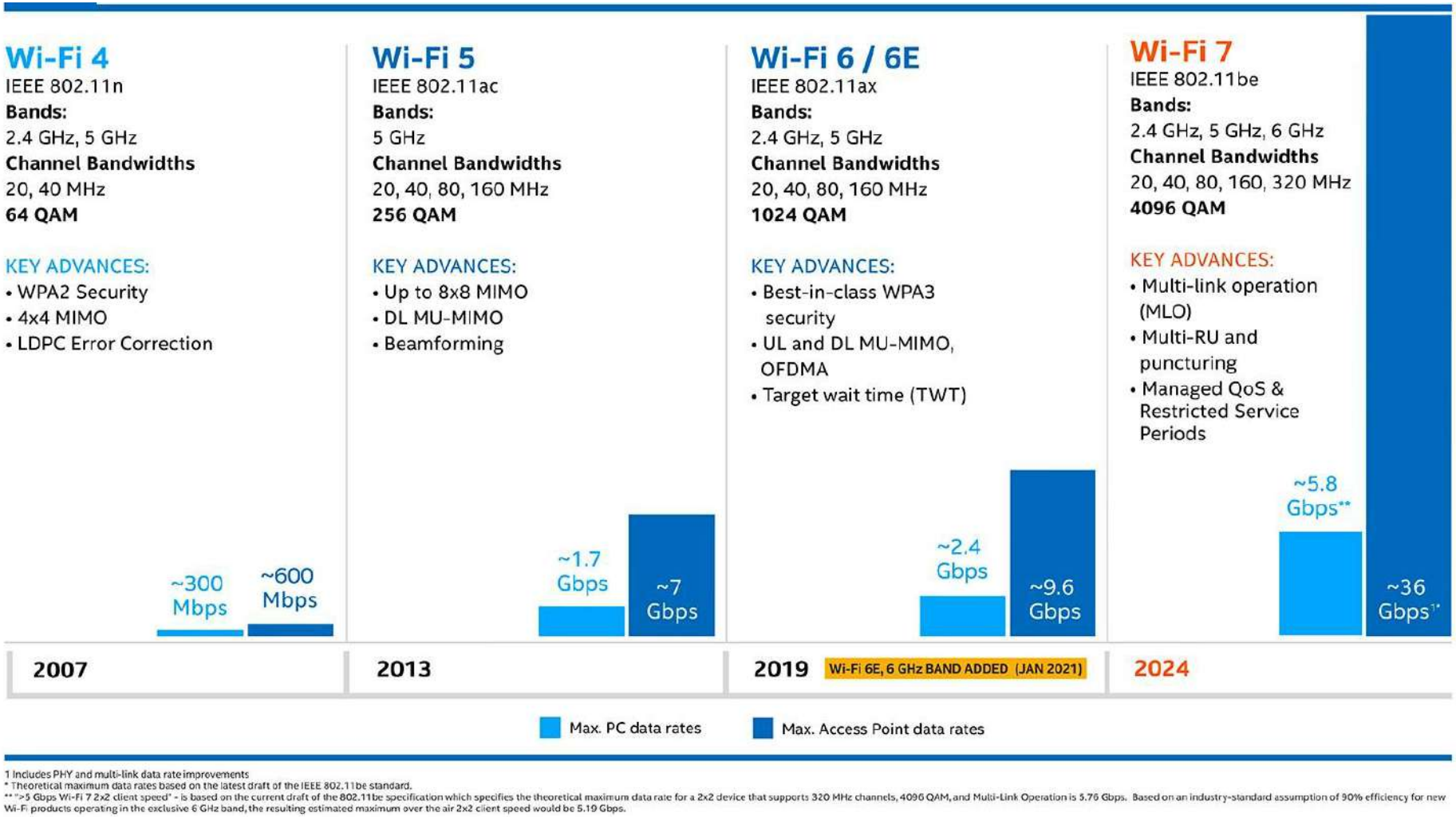
Wi-Fi enabling ubiquitous Last Mile Connectivity(LMC)

1. **Ubiquitous** – Each smart device (including Mobile Phones) is Wi-Fi enabled. 70% of consumer data passes over WiFi.
2. Uses unlicensed spectrum*(ISM Band)* which is free(690 MHz in 2.4GHz and 5GHz Band), 500MHz in 6 GHz and More.
3. All-IP Technology which is very efficient and future-proof, based on open and ever evolving standards of IEEE (802.11x).
4. Plug-n-Play Ecosystem.
5. Low Power consumption and Low Cost – Overall Infra cost about 15% of normal licenced mobile infrastructure.
6. Potential to conserve scarce licensed spectrum through **Mobile Data Offload (MDO), Fixed Mobile Convergence (FMC),Frugal 5G. (These are all Telcos-Surplus)**
7. **NINENP (Non- Interfering, Non-Exclusive, Non-Protected) – Free for All.**
8. Potential to deliver 4G and 5G type services through upgradation(**802.11ac,Wave2,802.11ax,Wi-Fi 6,Wi-Fi 6e,Be)**
9. Ideal futuristic platform for IoT, M2M and E-health, E-farming, E-education, **PM-WANI** and **Job/Entrpreneurs** creation.
10. Wi-Fi has become a part of the **5G and 6G ecosystem** through **Releases 16 & 17 of 3GPP** IMT Standardisation process.

Evolution of Wi-Fi Standard (IEEE802.11) - 1997-2024

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

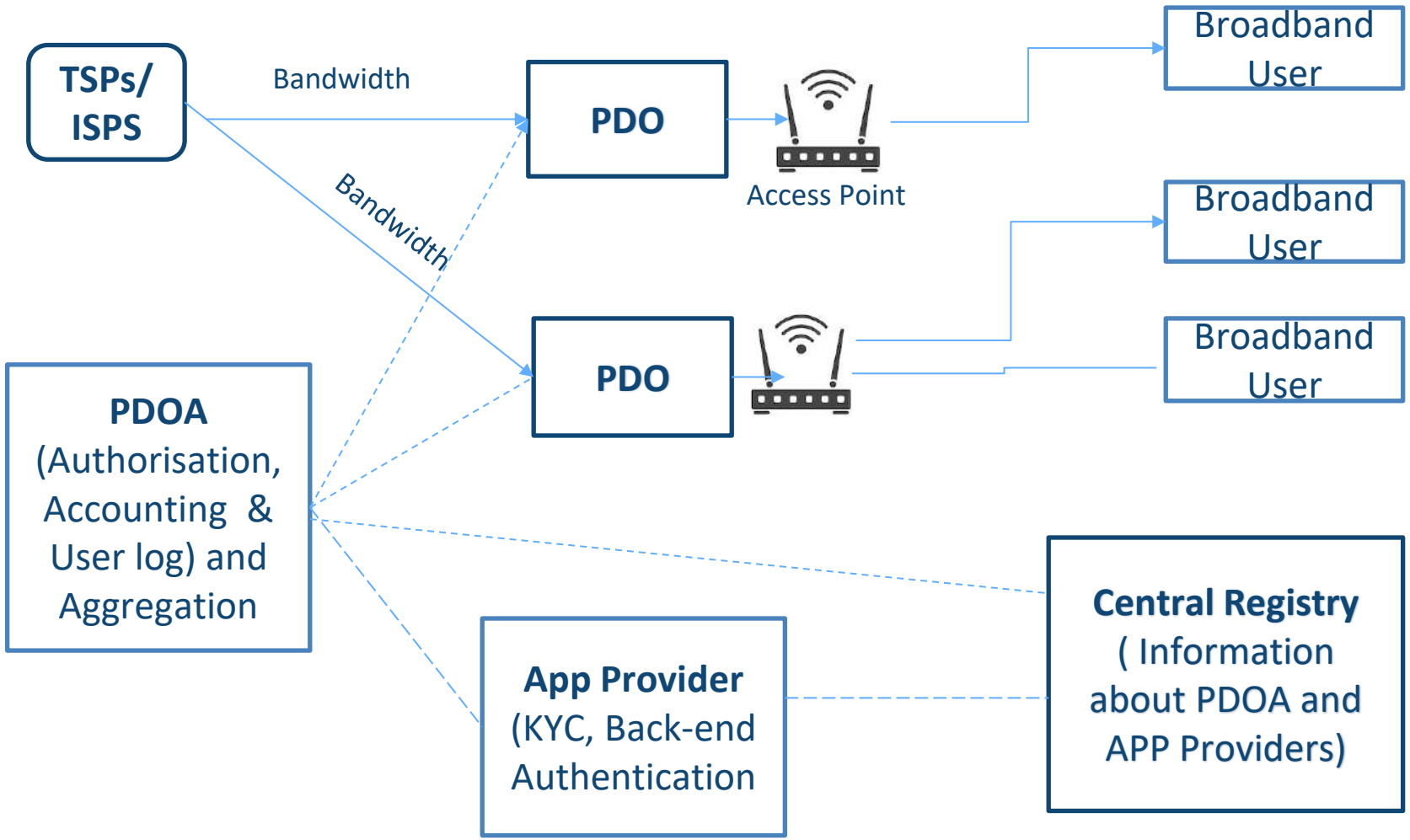
Wi-Fi 7 -- NextGen Wi-Fi Technology



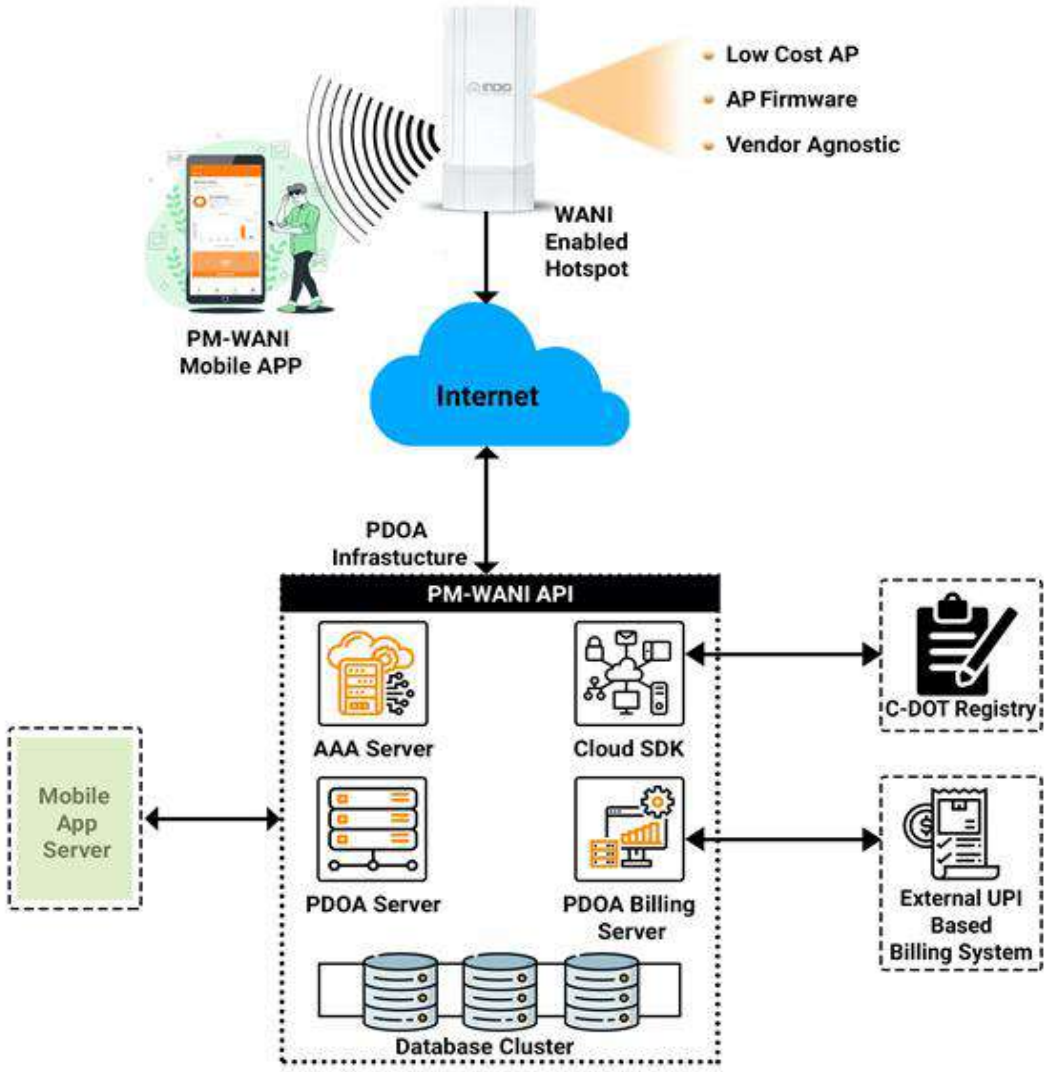
1 Includes PHY and multi-link data rate improvements
* Theoretical maximum data rates based on the latest draft of the IEEE 802.11be standard.
** ">5 Gbps Wi-Fi 7 2x2 client speed" - is based on the current draft of the 802.11be specification which specifies the theoretical maximum data rate for a 2x2 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.

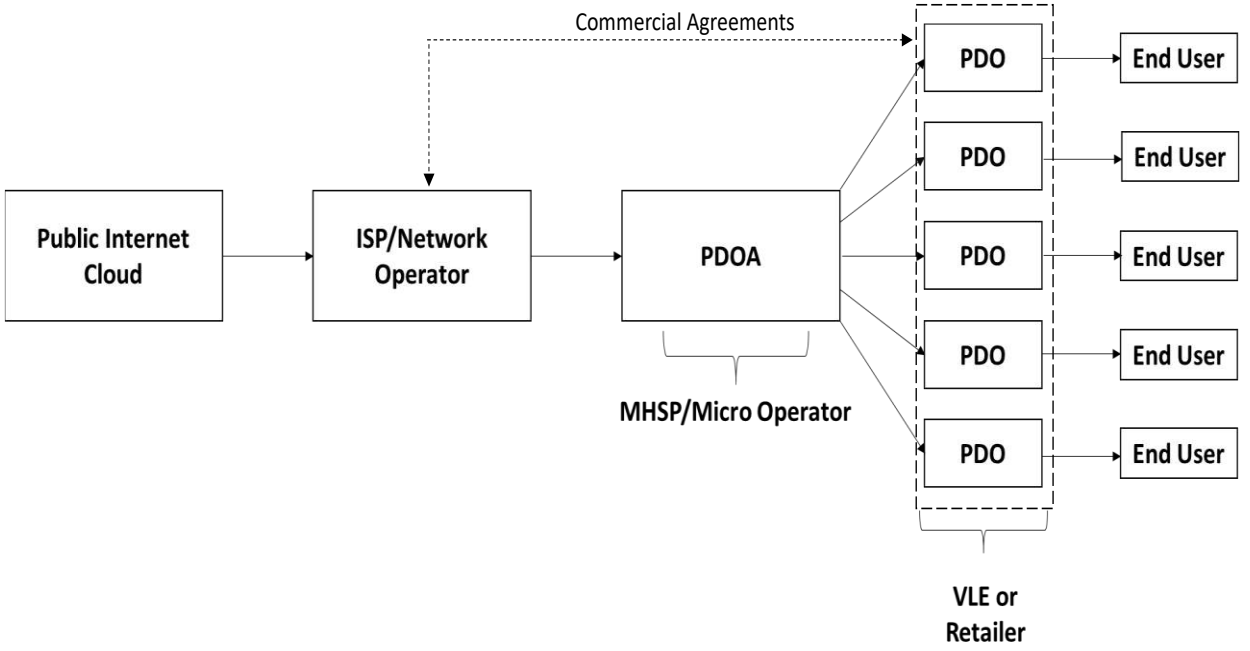
PM-WANI:PRIME MINISTER-WIFI ACCESS NETWORK INTERFACE-
A Liberalised Framework for Last Mile Connectivity(LMC) in Bharat

WANI - Unbundled and Distributed Architecture



PM-WANI System Architecture

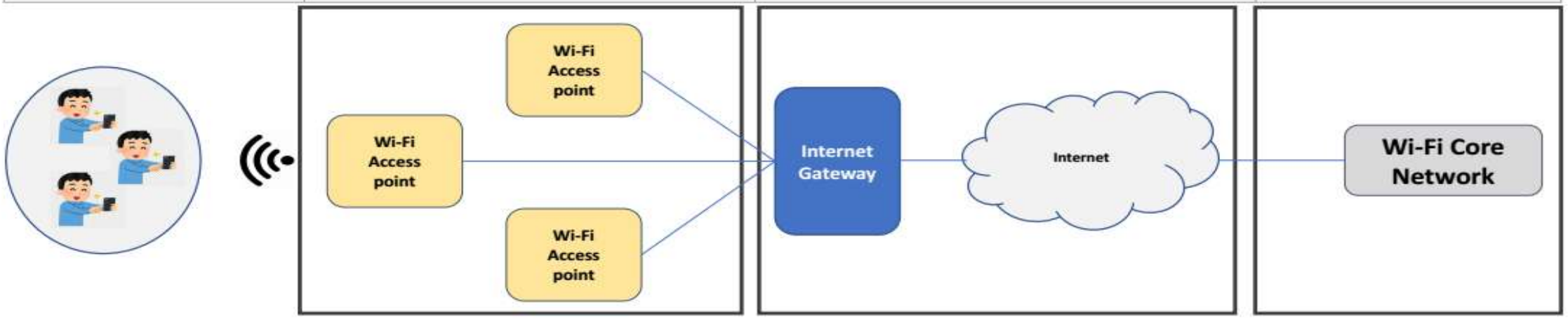




PM-WANI-- Multi-partner play for end-to-end service delivery

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

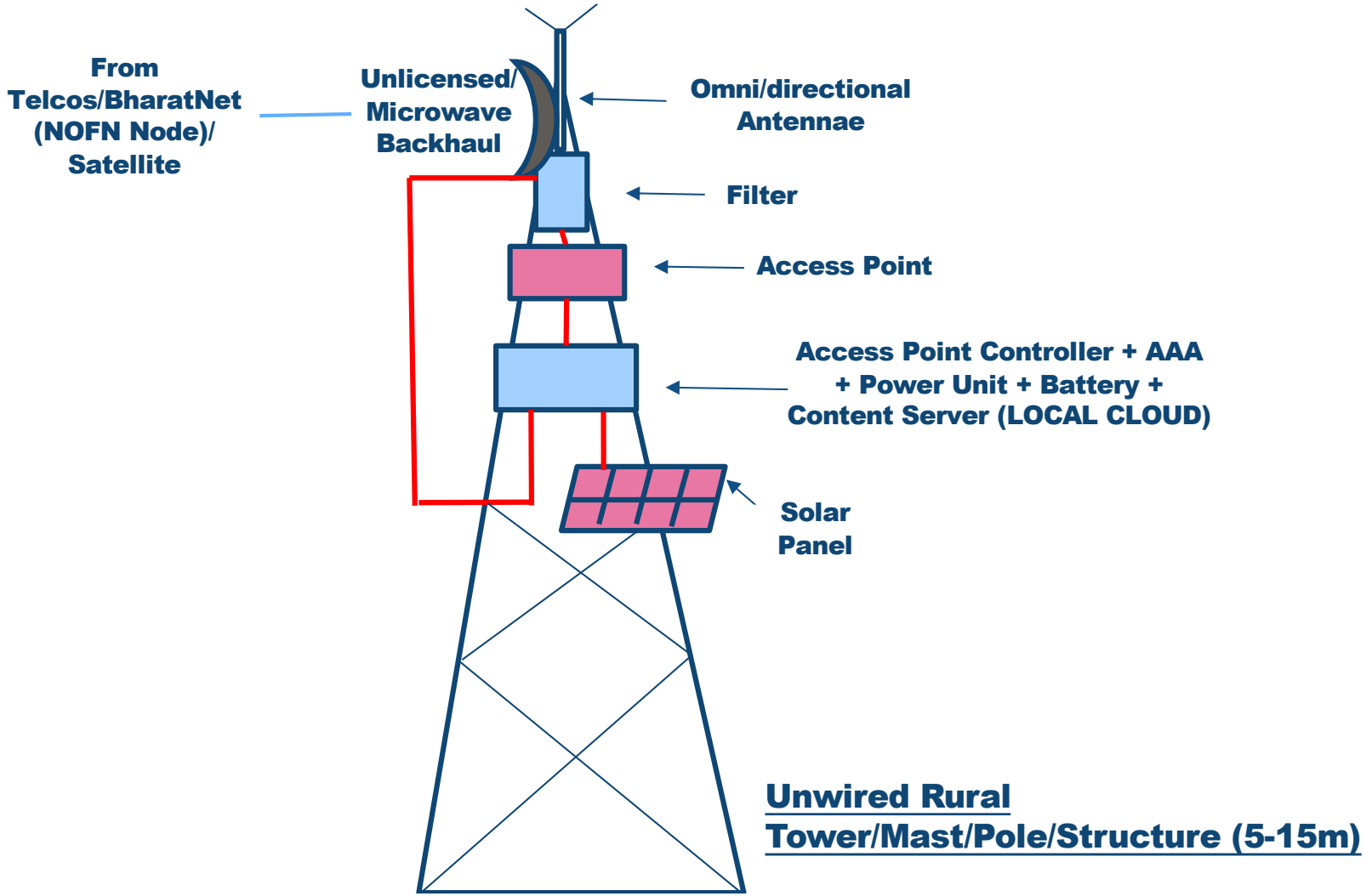
"Look at the world around you. With the slightest push, at just the right place, it can be tipped''

"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 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 rules for auto-execution.

PDOA

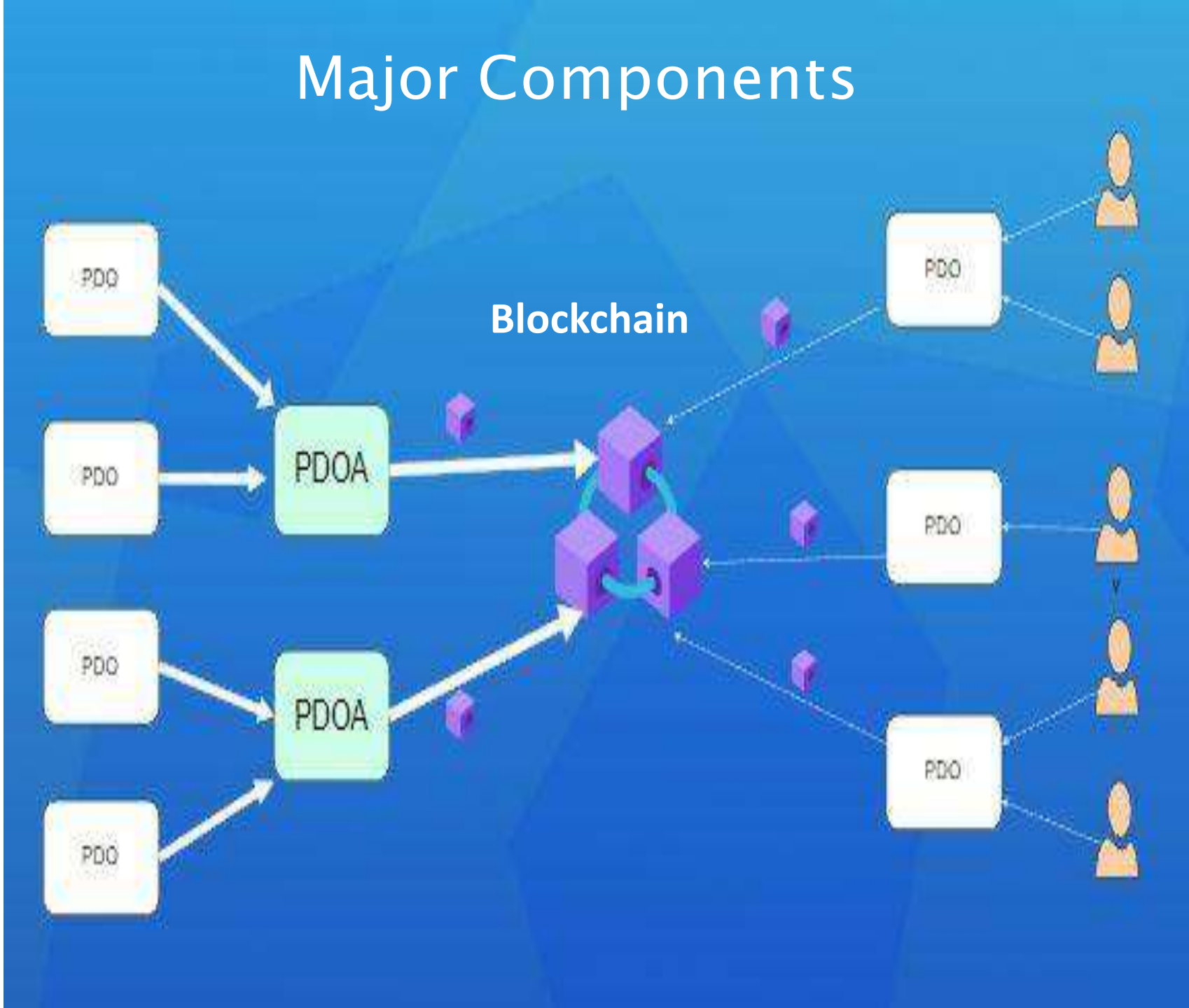
- PDOA an be mandated to register as a Node with the Wifi DAO and add all the PDOs functioning under it.

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 payments.

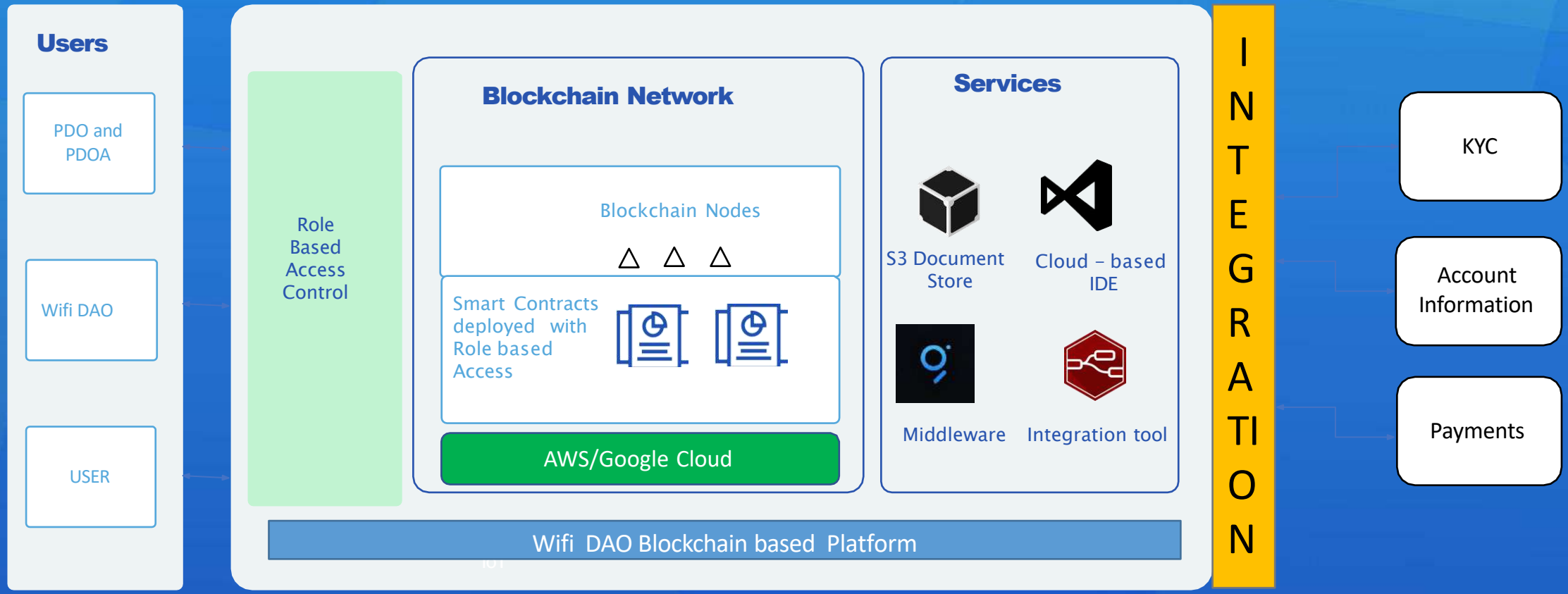
Users

- 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



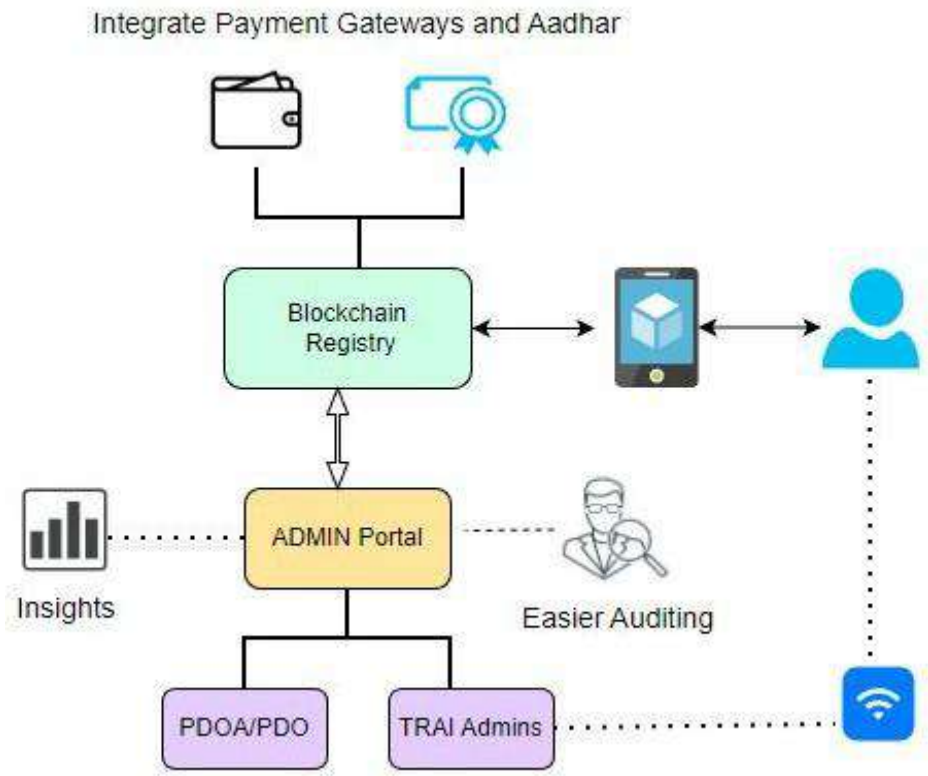
High Level Architecture

- 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

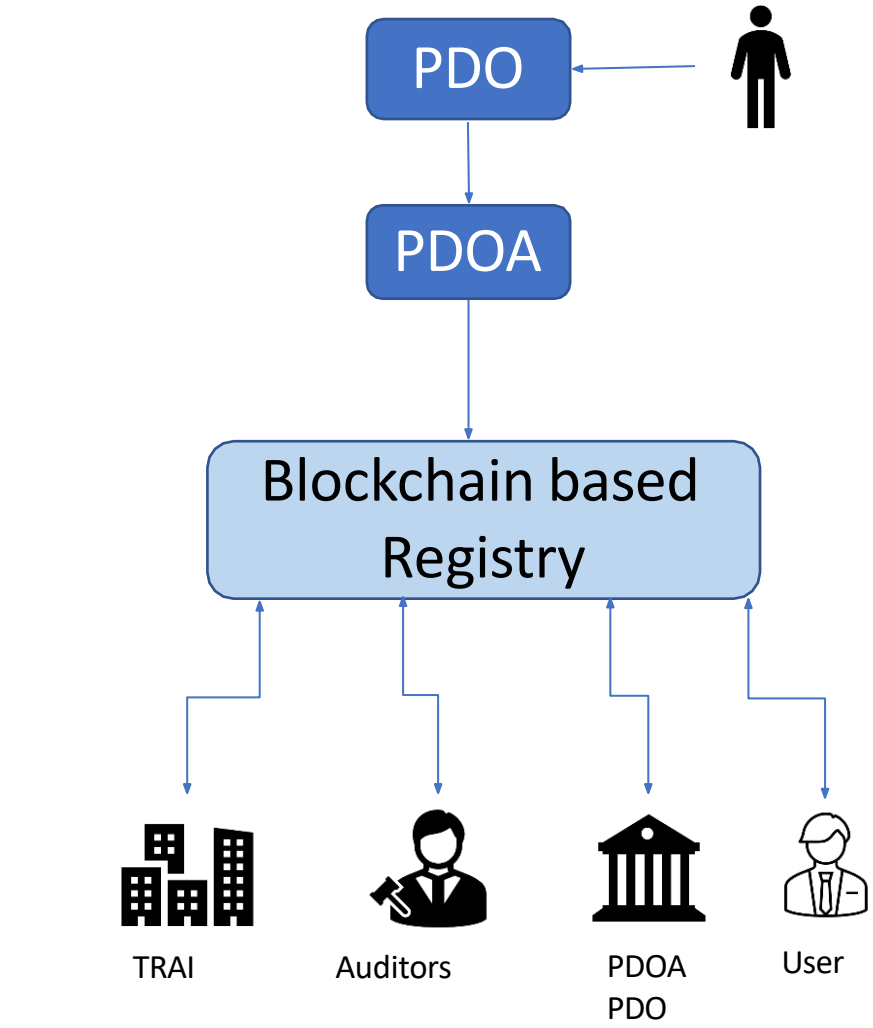
User data for all the Users will be updated by the verified Wi-fi access points.
Users can verify the MAC-ID with the nearest SSID.

Monitoring

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

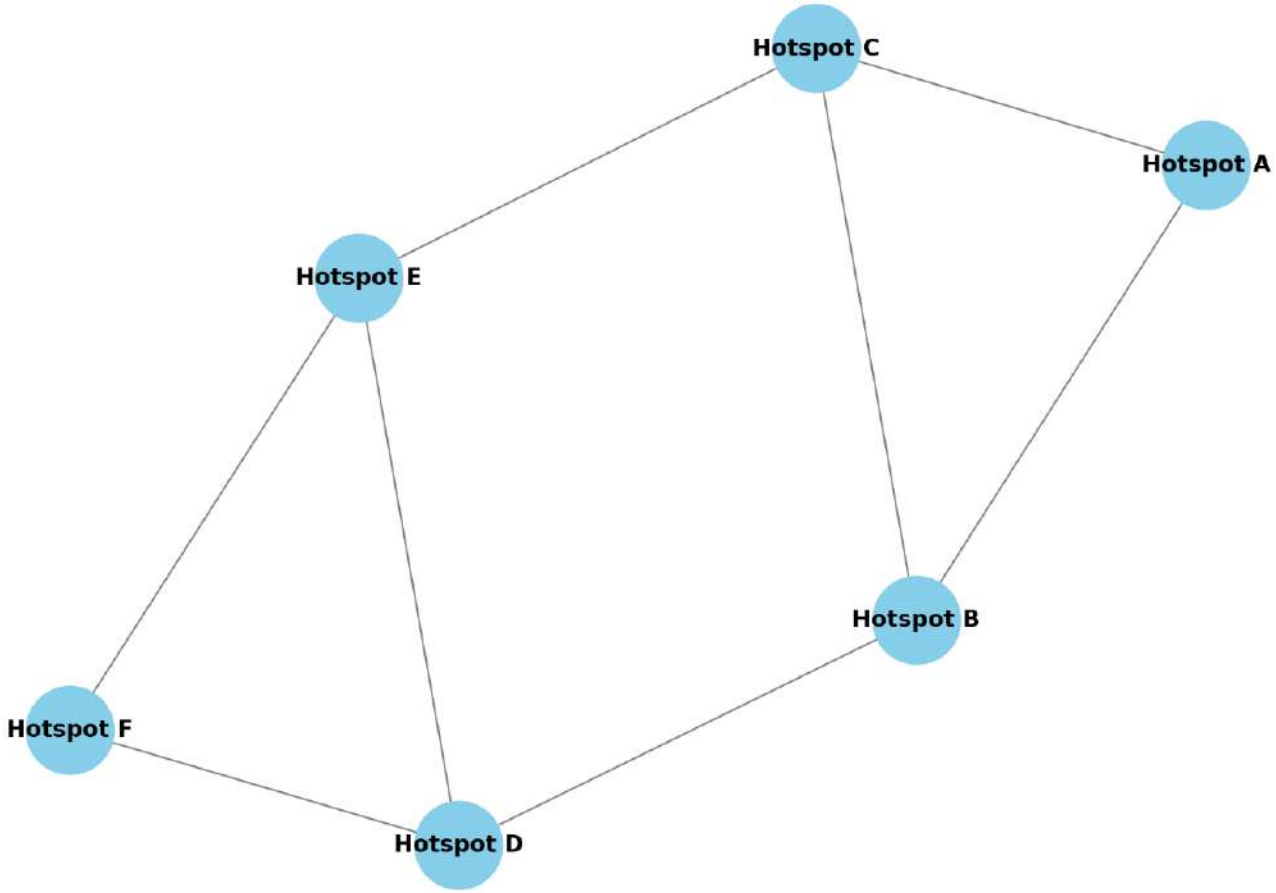
Payment

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

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 and Resilience.

DeWi Innovation:

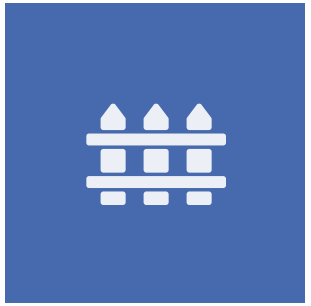
Blockchain / Mesh Networking / dApps

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.

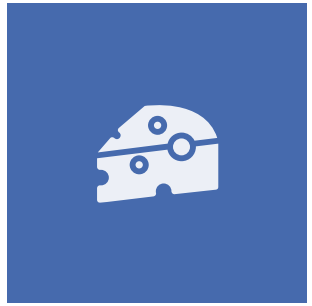
Mesh Networking

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.

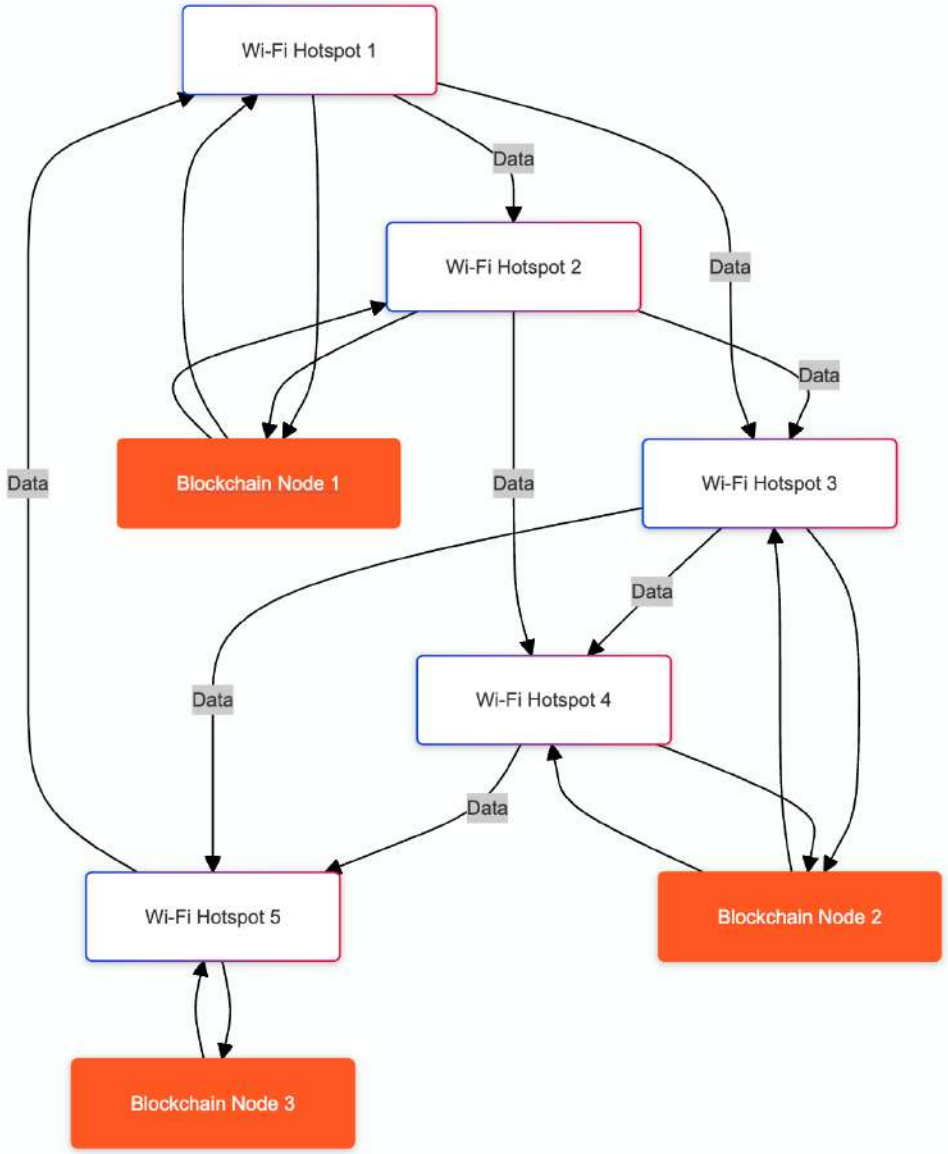
- **Proof-of-Stake (PoS)**

  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

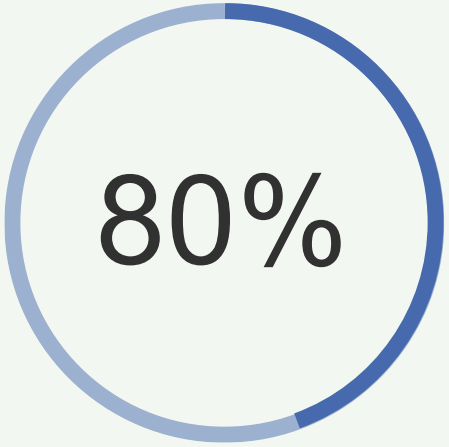
The mesh network architecture of DeWi provides inherent resilience against single points of failure and enables secure data routing through multiple redundant paths, improving overall network security.

Smart Contract-based Security

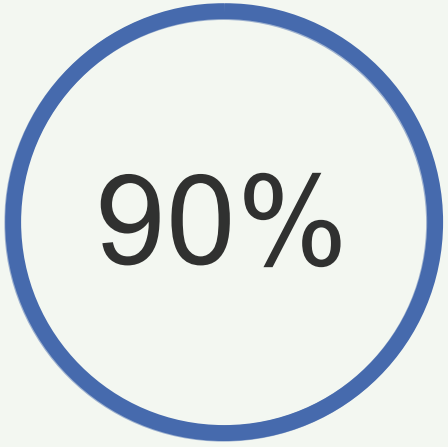
DeWi leverages smart contracts to enforce security policies, manage access control, and automate security-critical operations, reducing the risk of human error and improving the overall security posture.

Protecting against Network Attacks

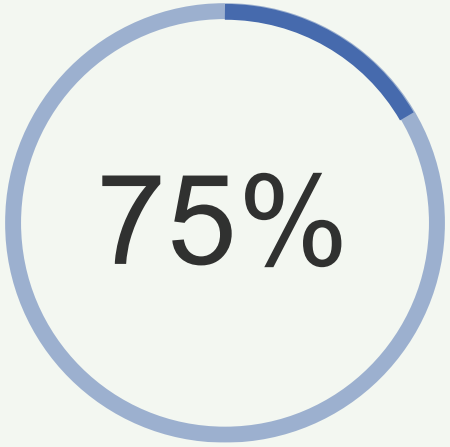
Comparison of effectiveness of security measures against common DeWi network attacks (0-100%)



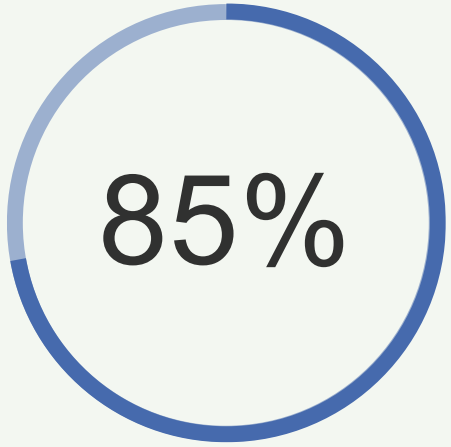
DDoS Attack Protection



Man-in-the-Middle Prevention

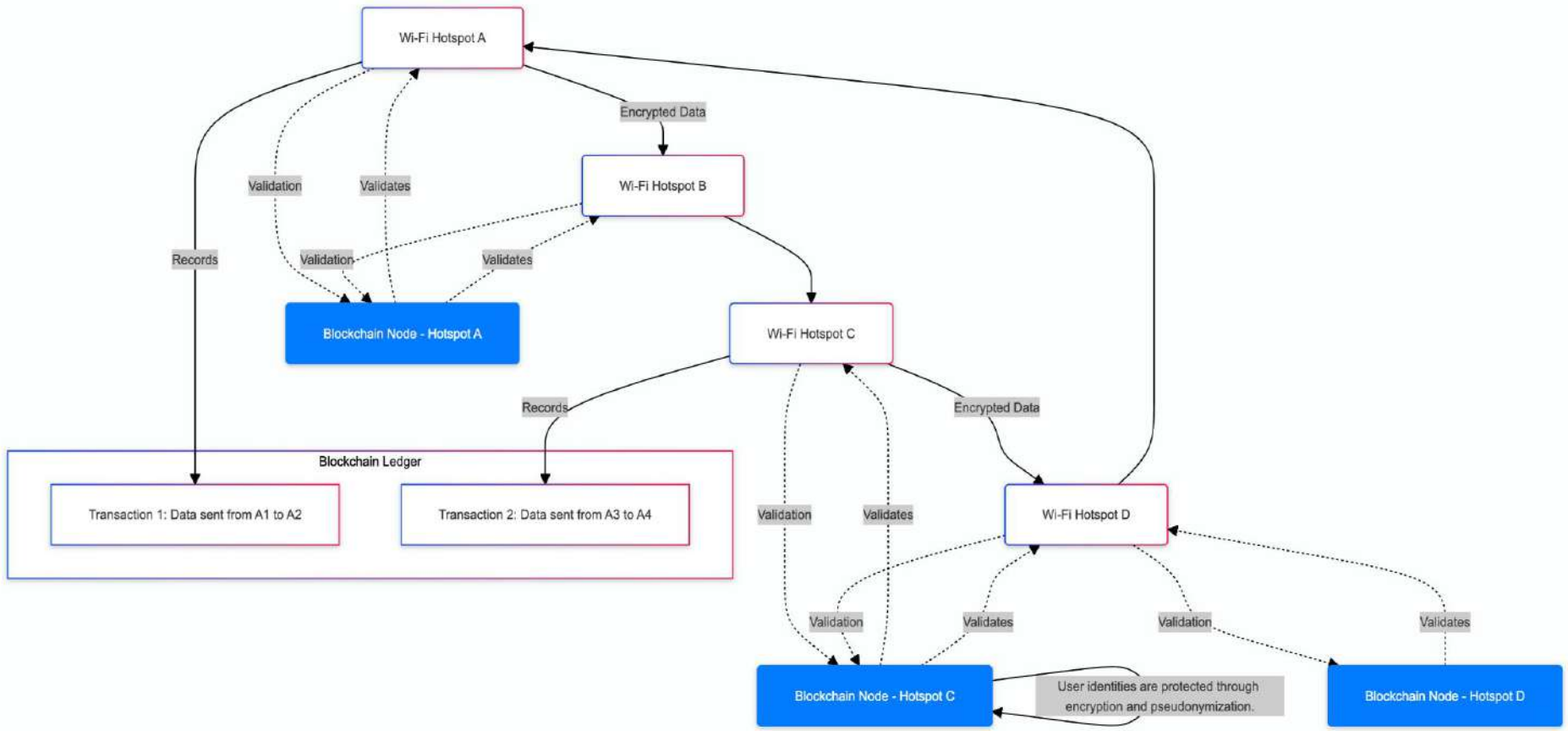


Sybil Attack Mitigation



Encryption & Authentication

Data Flow: Privacy and Security in DeWi

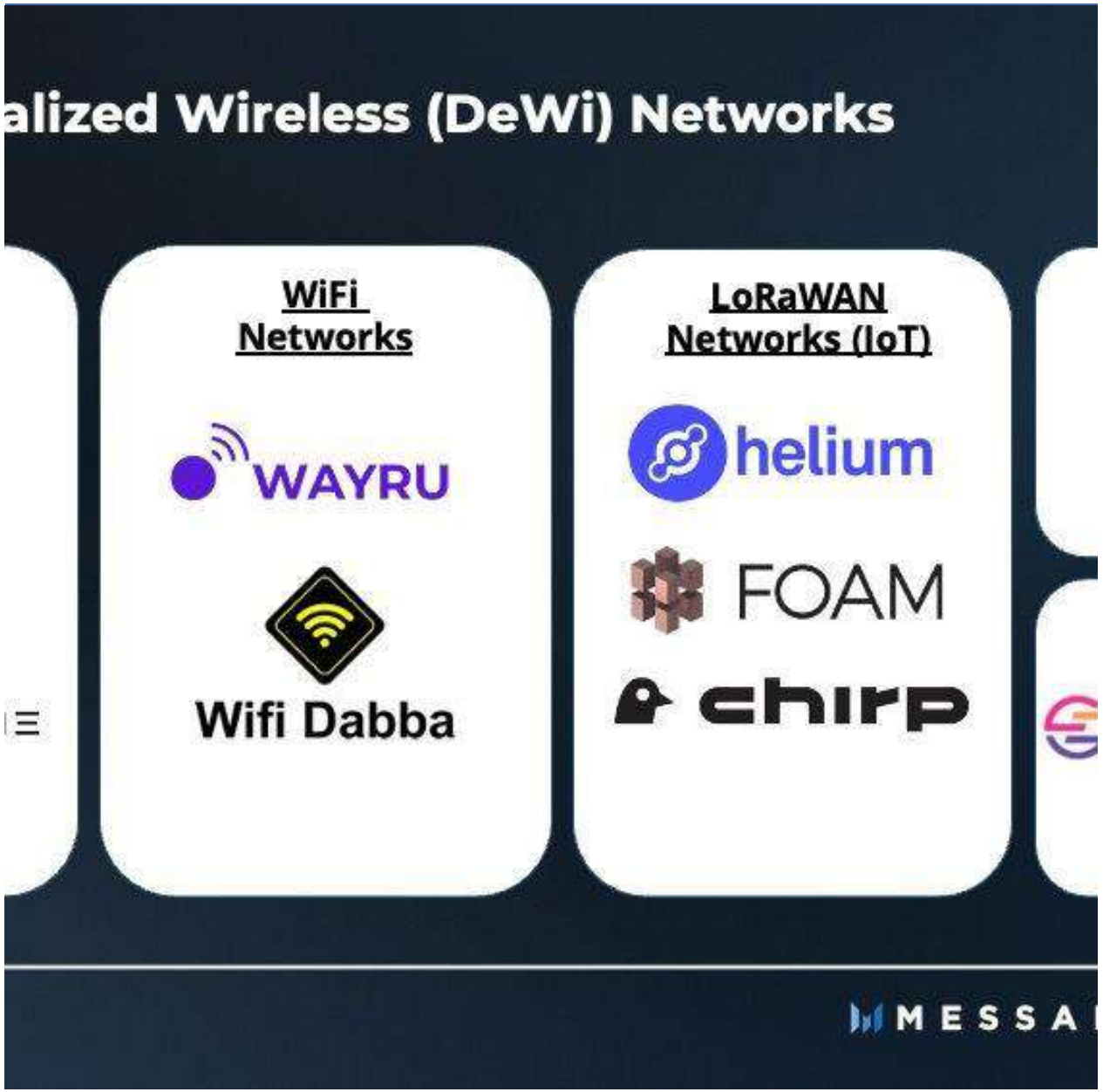


Security and Privacy protections provided by Blockchain in a DeWi network, includes:

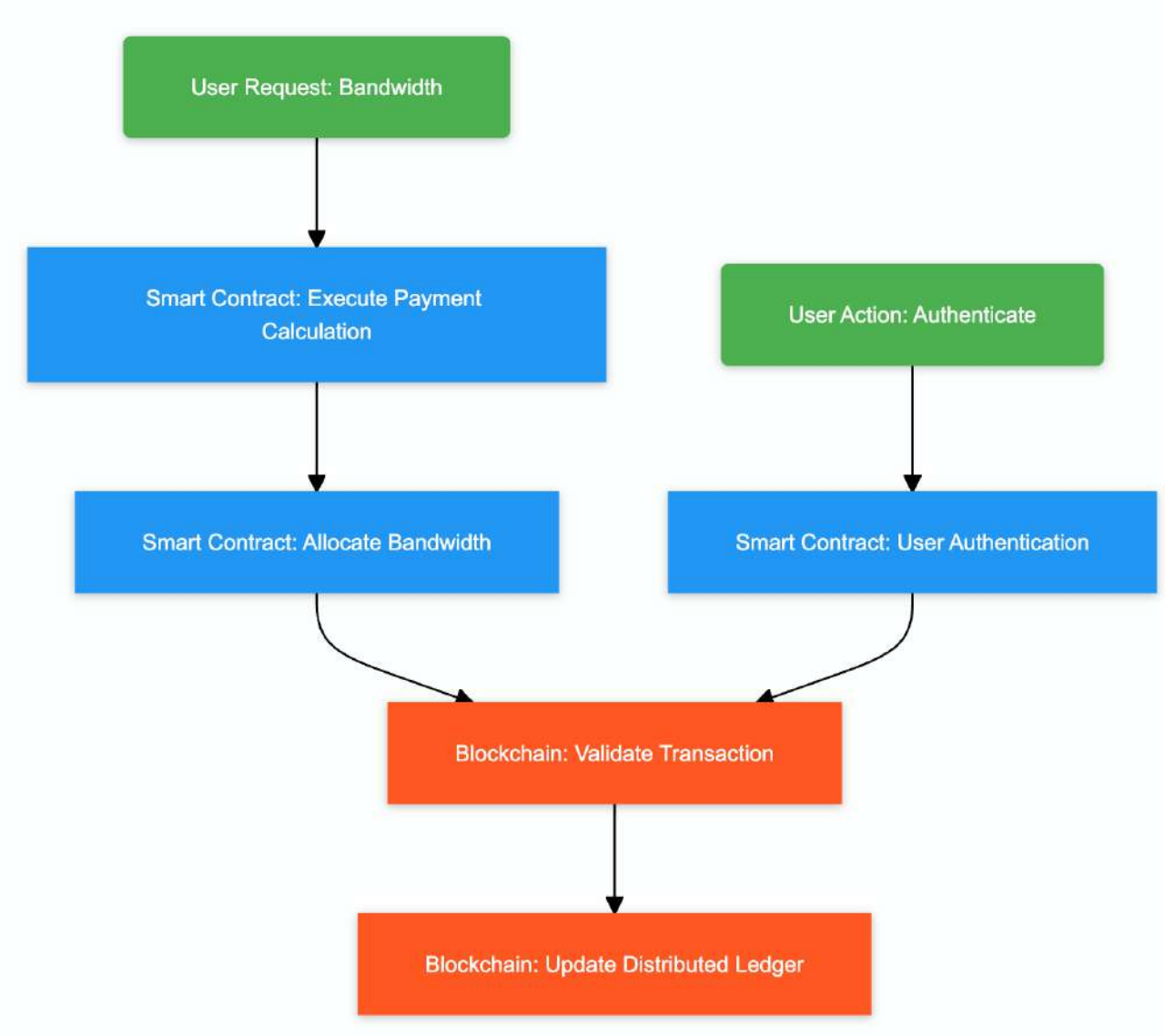
a. **Encrypted Data Transmission:** The diagram shows arrows marked with "Encrypted Data" moving between nodes (hotspots) to indicate secure data transmission.
b. **Blockchain Ledger:** A subgraph titled "Blockchain Ledger" includes transactions, illustrating how each transaction is recorded and validated 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.



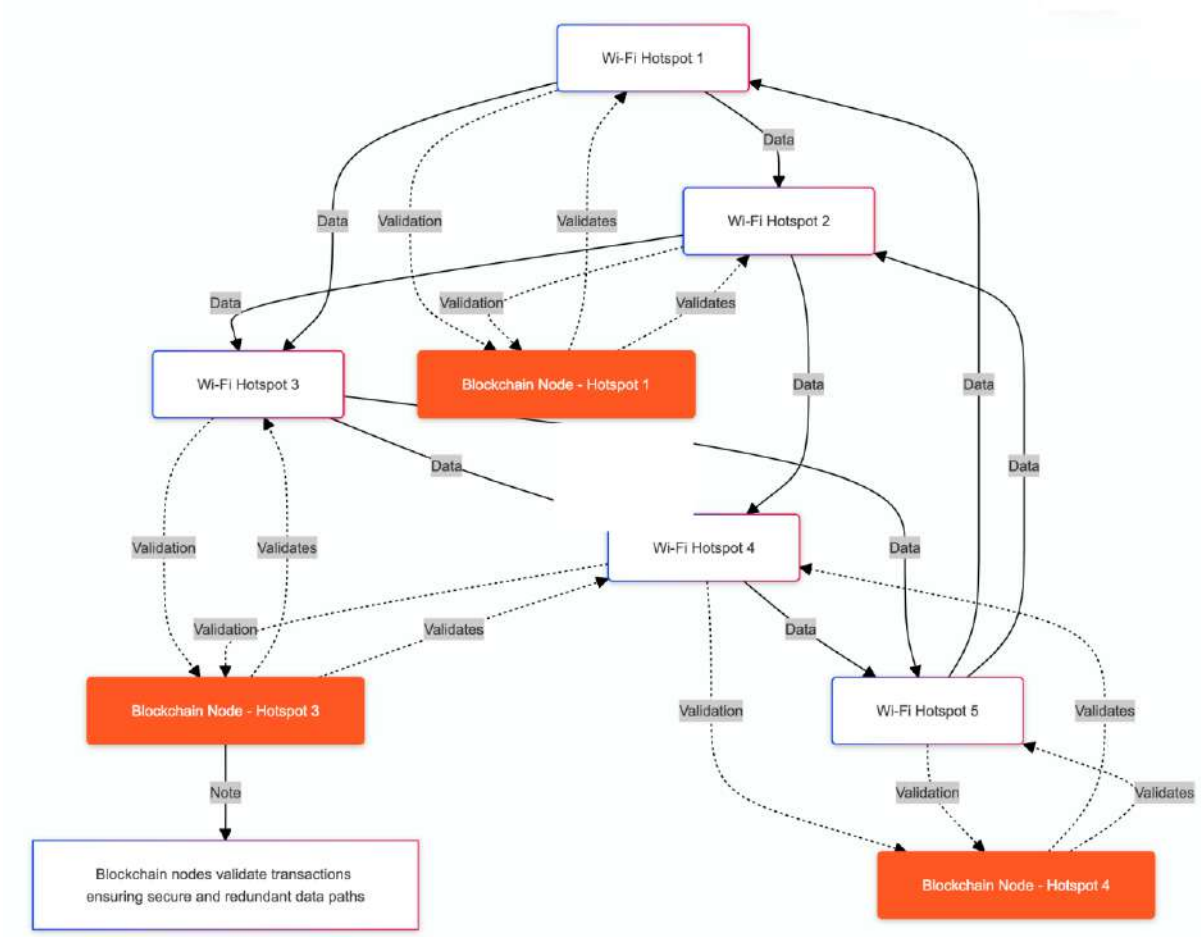
DeWi: Smart Contract Operation Flow



Mesh Networking:

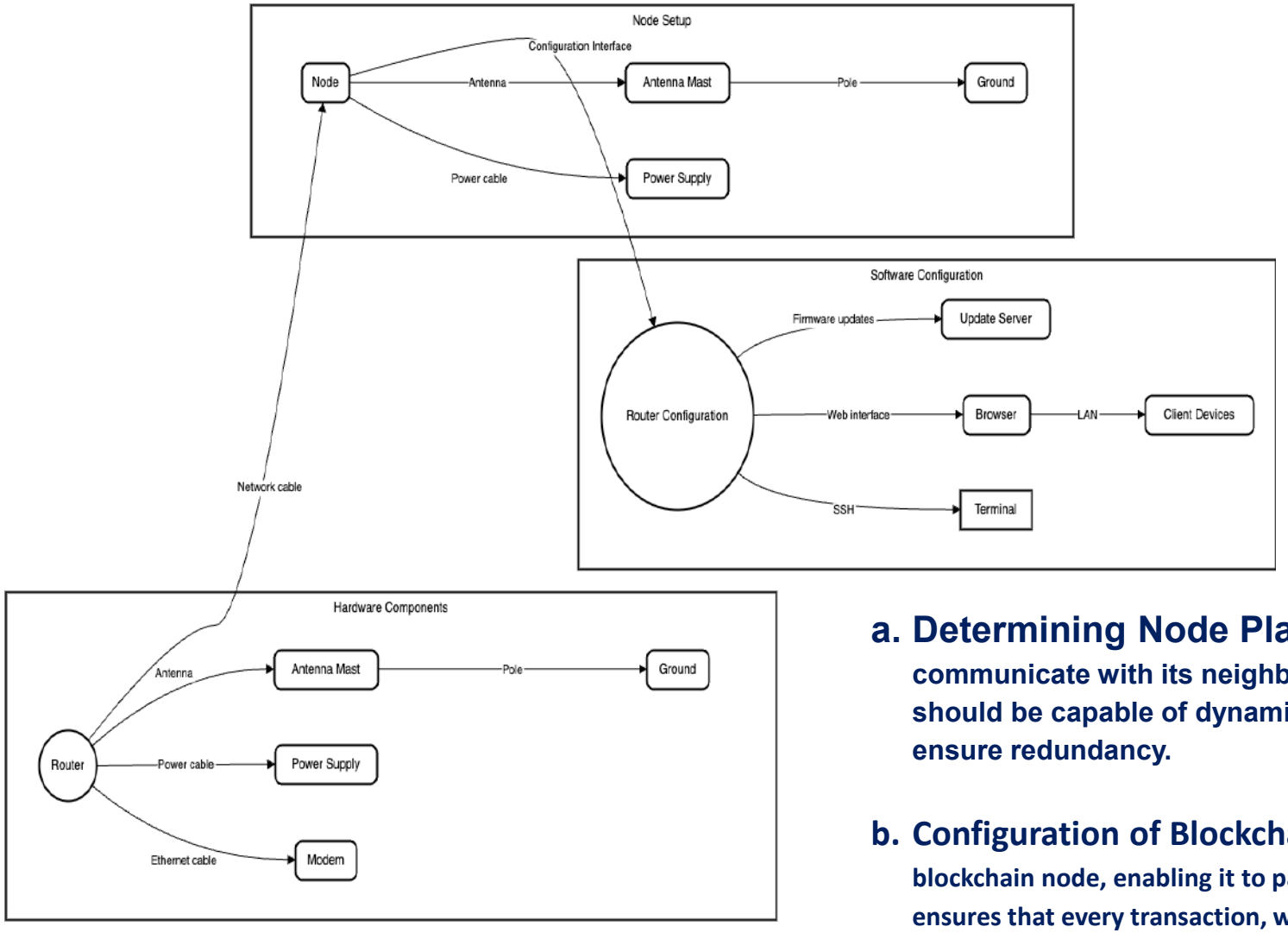
Building Resilience and Scalability through Blockchain-enabled Infrastructure

- 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.

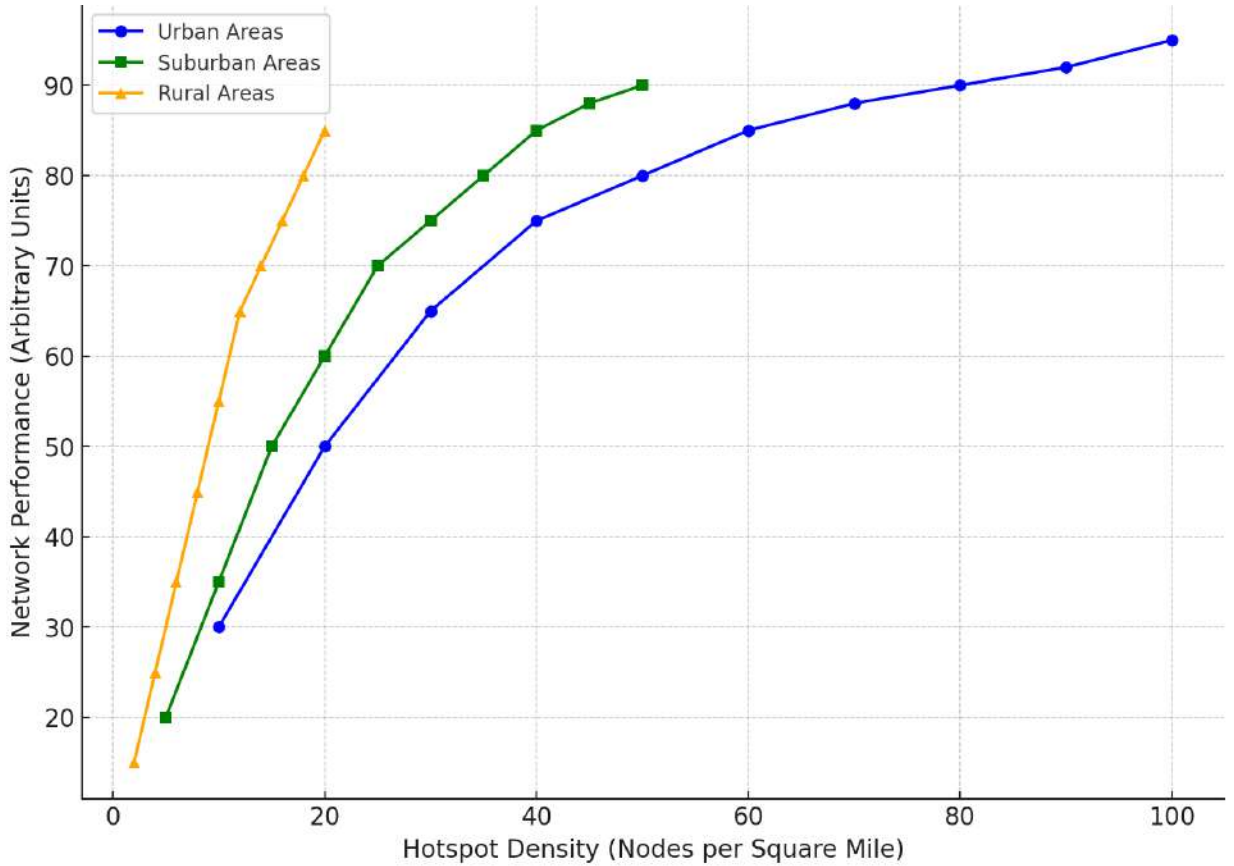
Decentralized Authentication in DeWi

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.

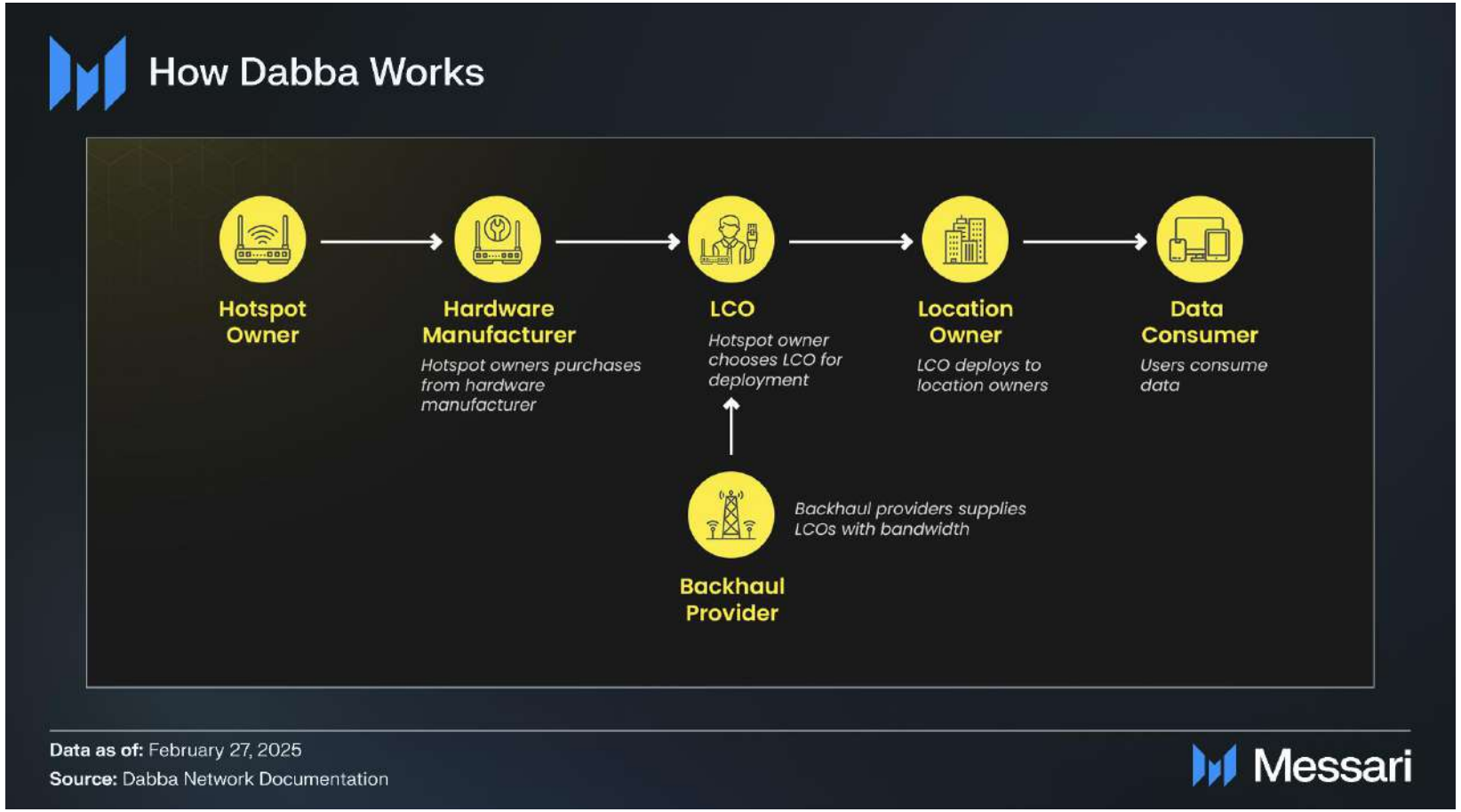
Scalability of DeWi Networks in Different Settings

DeWi N/Ws in diff. settings (urban, suburban & rural)

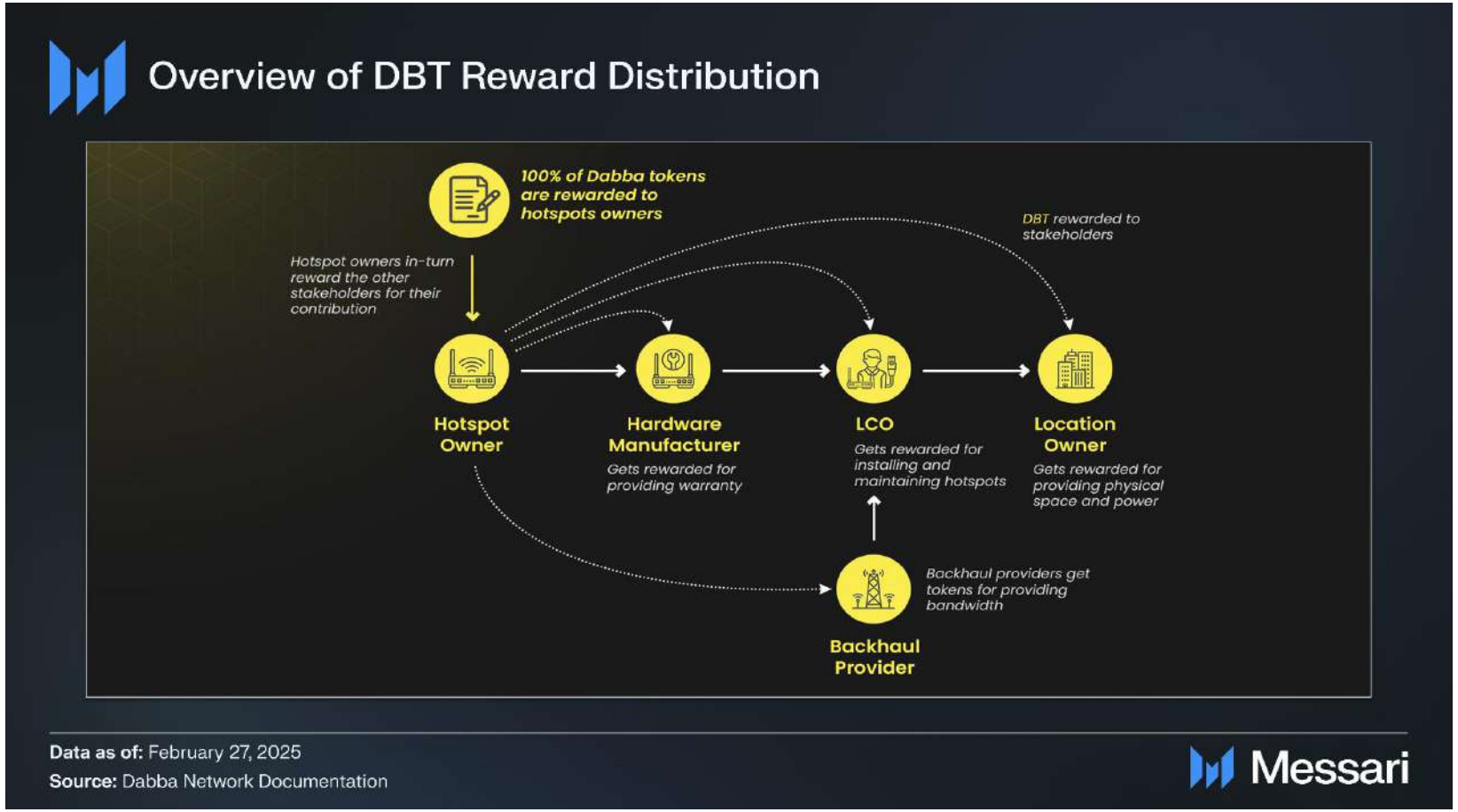


Network performance improves as the density of Wi-Fi hotspots increases, with urban areas showing the highest potential performance due to higher node density.

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

1

Discovery & analysis

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

1WEEKS

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.

1WEEKS

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)