

Security in the 6G era

Blockchain in improving **trust and transparency**
in 6G networks - Plenome perspective



July 2025

Presented by Prof. Prabhu Rajagopal with inputs from Anirudh Varna, CTO
Plenome Technologies Pvt Ltd

Content

1 6G vision



2 Threats and vulnerabilities



3 Solutions – Blockchain & AI



4 Implementations & Case studies



5 Possibilities



6 Action points



6G brings exciting new possibilities ...

6G isn't just faster internet – it's
the central nervous system of
human progress

THz communication

1 Tbps internet speeds

Volumetric videos and
immersive education



Large scale IoT networks

Million-device IoT networks

Autonomous swarm
intelligence



AI-native federated networks

AI-dedicated network

Federated learning cross
global sources



... and a lot of new attack vectors.

Beam-steering eavesdropping

High directionality of 6G beams makes it vulnerable to beam attacks via side-lobe leaking or

Atmospheric absorption (THz) forces ultra-precise targeting, creating "sniper-like" attack vectors

Federated learning poisoning

AI-native networks with millions of devices can easily be poisoned by malicious devices with bad data

Trillion-device scale makes manual verification impossible

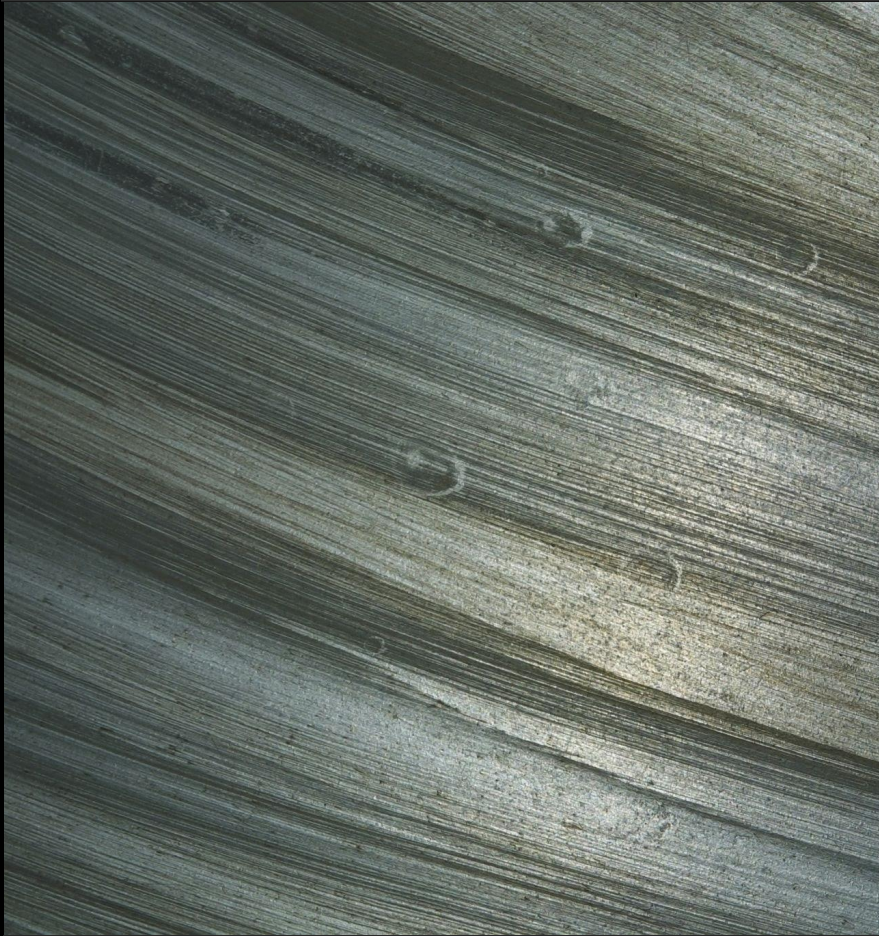
SAGIN satellite signal spoofing

Fake GNSS signals or compromised satellites can deceive IoT network members

Unified SAGIN architecture means one compromised node breaches air/space/ground networks

Major differences

Aspect	5G	6G	Security implication
Latency	1 ms	0.1 ms	Attack windows are 10x shorter
Device density	1 million / km ²	100 million / km ²	Botnet recruitment will scale rapidly
AI integration	Optional	Native	Entire networks can be poisoned



Proposition

Blockchain and AI can synergize to bring potential solutions – secure 6G

Identity, traceability and threat data from a decentralized network
Optimization, resource allocation, prediction with AI.

We have the chance to start 6G securely, instead of patching security as has been the practice.



Blockchain can improve **identity and tracing** across large networks



Identity – Zero-trust device authentication

Decentralized IDs with verification

Consortium systems can be used to have access control



Traceability – permanent record

Immutable logs of all device/user activity

Permanent record available to all regulators for audits



Threat intelligence

Attack pattern data collected across nodes

Trustable behavioral data can be used by AI for threat modeling



AI can help in anything **predictive** – threats, network traffic, behavioral analysis.



Security – threat modelling & prediction

Activity data can be used to identify adversaries and predict



Resource allocation

Device clusters' behavior can be studied for allocating resources across networks



Threat intelligence

Attack pattern data collected across nodes

Predictive security for million-device networks only possible through AI

Blockchain and AI are already used in telecom

Blockchain

DLT Identity Registry
by TRAI

500M+ telemarketers
verified on blockchain

94% spam reduction (TRAI
2023)

6G Application:

Trillion-device identities to
be registered on-chain

AI interventions

NLP firewalls for
spam by Airtel, Jio

12B+ messages analyzed
daily

99.8% deepfake detection
accuracy

6G Evolution:

Semantic attack
prevention with predictive
threat modeling

Large scale global applications can be achieved with secure 6G

Precision agriculture

AI + 6G drones optimizing individual plant nutrition

Edge intelligence for on-field machines to enhance yield

Federated learning

PII-preserving learning for AI without data silos

Truthful AI with immutable proof of every data point leads to explainable AI

Holographic clinical response

Large volumetric data can be streamed across global counterparts

Remote surgeries, AI training without PII invasion

Our work

Plenome is working on making federated learning a reality.

We are working towards building a decentralized learning protocol for federated learning in domains with sensitive PII-infused data.

6G plays a major role in making federated learning commercially viable



Problems to be solved

Scalability trilemma



10M TPS to be achieved on blockchain to enable trillion-device networks (comparing to the 1 Tbps throughput of 6G)

Explainable AI audits



Regulatory-compliant decision trails which can automate audits

Differential privacy in FL



Finding a balance in federated learning – noising local weights to stop prompt injection attacks, while tracking honest data contributors

THz beam security – DoS



Bringing in AI-driven and physical systems against eavesdropping, spoofing and DoS

Thank you

Prof. Prabhu Rajagopal

prajagopal@iitm.ac.in

Anirudh Varna

anirudh@plenome.com

References

THz Security: Kumar, A. et al. "Physical-Layer Security for 6G" IEEE Comm. Surv. (2024)

AI-Blockchain: MIT 6G Lab "Autonomous Network Defense" (2025)

Quantum Ledgers: NIST IR 8413 "PQC for Distributed Ledgers"

India DLT: TRAI "Regulatory Impact Study" (2023)

Healthcare AI: Chen, L. "MedBlockFL" Nat. Dig. Med. (2024)

Threat Models: 3GPP TR 38.845 v18

6G Economics: McKinsey "The 6G Security Market" (2025)