BDATA provides end-to-end network, application and device level data security to ensure that data stream from the IoT products (drones, autonomous vehicle, pumping stations etc.) to cloud is cryptographically encrypted and immutable.

BDATA gateway device which comes with sim/esim is the best suited to function as the peer in an IoT device private blockchain network, as it has advance security and cryptographic features and fully scalable standardised solution for multiple IoT ecosystem vertices.

**Market Need - High Speed & Secure Connectivity:**

70% of the 4G coverage in North America will be converted to 5G by 2025, which will increase huge amount of use cases in IoT industry e.g. increase in the deployment of remote operation of pumping systems, remote mining operations, remote surgeries etc.

IoT industry was sitting at $250B in 2019, and expected to reach $1.5T by 2027, which heavily rely on the secure connectivity provided by telecom companies.

**Highly Secure and Scalable IoT System Architecture.**

BDIOT (Blockchained Data Internet of Things) provides a patent pending mechanism to ensure network, application and device level security.

BDIOT hardware and software architecture enables IoT devices manufacturer and IoT telecom service providers to leverage the BDATA gateway device with embedded sim as a robust, scalable and standardized hardware peer to protect IoT data communications.

A close up of a map

Description automatically generated

**Network:**

All the communication using eSIM card is authenticated using advance security and cryptographic features of blockchain to ensure end-to-end secure connection.

**Application:**

Application that run on the product (drones, pumping system etc.) is deployed on the blockchain to ensure that no one can tampered the application.

**Device Level Security:**

Most of the IoT use cases required remote operation, which means that device is not being stalked by individuals that increases the risk of the data stolen from the device.

Device operation chaincode is deployed on the device to ensure that all the output ports can be managed and controlled by organization admin to ensure no data is stolen from the device (USB, Bluetooth, HDMI etc.) or no parallel script is running on the device to steal the data.