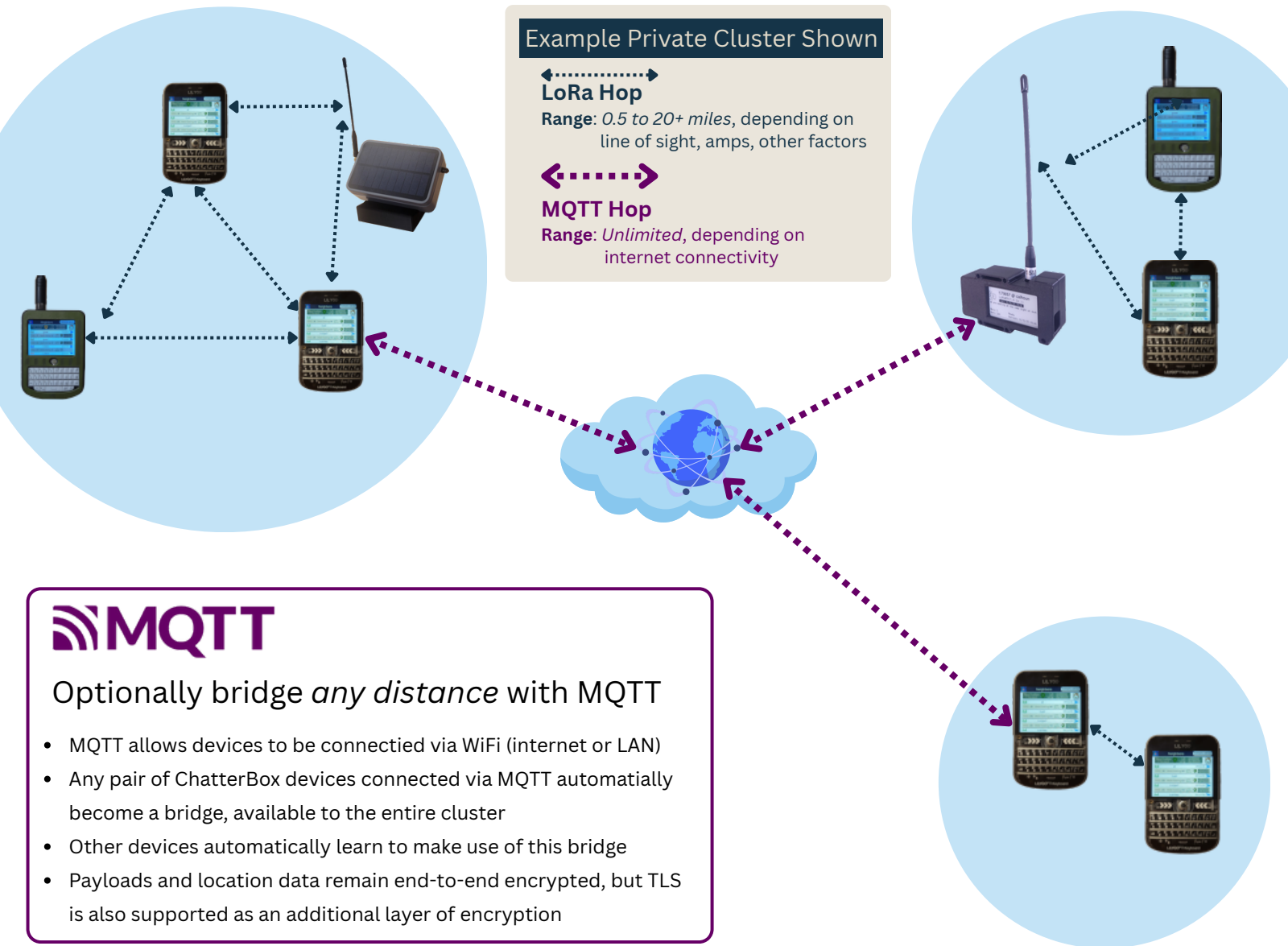
ChatterBox protocol uses LoRa, asymmetric encryption, meshing, and digital signatures to securely keep devices in contact.

- **Meshing**: Messages & location automatically route through best path
- **Delivery Confirmation**: *Signed* confirmation is relayed back to sender
- **Decentralized**: Trusted devices work together to securely deliver
- **Secure**: Each device along the way validates signature & plans next hop
- **Anti-jamming**: cluster automatically / unpredictably hops frequencies

LoRa



MQTT

Optionally bridge *any distance* with MQTT

- MQTT allows devices to be connectied via WiFi (internet or LAN)
- Any pair of ChatterBox devices connected via MQTT automatially become a bridge, available to the entire cluster
- Other devices automatically learn to make use of this bridge
- Payloads and location data remain end-to-end encrypted, but TLS is also supported as an additional layer of encryption