LoRa - the Long Range protocol

LoRa is one of the four main communication protocols used on the Chirp network. It is one of the main IoT technologies used in the Blackbird, designed to provide very long range IoT coverage for communications or applications that require small data streams, on the order the bytes or kilobytes.

How does it work?

LoRa uses very narrow radio impulses, often called chirps, to send information, in a method called the chirp spread spectrum technique. This strategy is unique in its ability to resist against the influence of noise or jamming when in crowded radio channels, making it resilient to interference.

What is it for?

LoRa has a large number of uses, usually related to its use in collecting data from a very large number of different sensors across a very large area. This includes examples such as weather, air quality, pollution, light, temperature, humidity sensors, or switches such as one that checks whether a door is closed.

On networks such as Chirp where type C is enabled, devices are also listening all of the time for signals sent by gateways, so they can also respond to commands such as turning on lights, closing circuits, starting motors and moving valves. These devices tend to have a much lower autonomy than normal type A devices, so they will need to be recharged more often, or have their battery changed.

How does it compare?

LoRa has the best range and cost compared to all of the other IoT protocols. It provides coverage for millions of devices over very long ranges, up to hundreds of kilometers at a fraction of the price, using only open, license free frequency bands.

However, in terms of bandwidth and data rate it is below Wi-fi, BLE and cellular, altough recent advances in AI-based algorithms have achieved breakthroughs in enabling new advanced applications of LoRa such as image, video and audio transmission.

Compared to other technologies, LoRa offer deep indoor penetration, essentially being able to penetrate concrete walls or cover an entire office building.

LoRa, especially with the SX1303 advanced chipset, can provide extremely precise location detection of any sensor on the network, such as a simple temperature sensor, without GPS, at meter-level accuracy.

LoRa Hardware

What is a LoRa **Device**?

Small edge devices such as sensors, locators, or other IoT devices transmit these signals over a very long range, sometimes as far as hundreds of kilometers in the form of chirps representing individual bytes of data. Most edge devices are battery-powered, being capable of functioning for as long as 2 years without being recharged, and provide a variety of functions.

Some devices are also capable to receive commands through LoRa, when the LoRa network supports it, and may even take part in simple automation tasks such as starting motors or switching on a smart plug.

What is a LoRa **Gateway**?

Specialised LoRa hardware, called Gateways, receive the chirps emitted by edge devices and decode it into usable digital data. These Gateways are capable of processing signals with powers lower than that of background noise, all because of the shape of the chirp signal. Different pieces of information are sent by varying the time in between chirp signals.

Gateway optimise themselves by making use of spreading factors, a method to either extend their range of connecting to devices or the amount of data they can receive (datarate).

Gateways, such as Chirp’s Blackbird, use an antenna to capture the radio signal emitted by LoRa end devices. The antenna needs to be placed as high up as possible, in a place with great view and no obstructions in its surroundings. Another requirement of a LoRa Gateway is for it to be connected to the internet through either WiFi or Ethernet cables, which in the case of Chirp is also the source of electrical power, removing the need for a power cable.

Dual-band LoRa

LoRa frequency bands

Just like any other radio technology, LoRa has to operate within a imited range of radio frequencies. These frequency are often the unlicensed frequency, where the user does not need to seek approval from governmental institutions. Older technologies used to be limited to a single unlicensed band, called the sub-GHz band, which depended on which country, continent or region the devices were installed.

Chirp uses the latest improvements in LoRa technology that make it possible to use LoRa on the 2.4GHz Industrial, Scientific and Medical frequency band, a newer unlicensed frequency band designed for data transfer and which is also used by the majority of WiFi routers, Bluetooth, Zigbee.

The 2.4GHz frequency band makes it possible to send more data and makes all devices compatible with the same LoRa Gateway, regardless of where the device is installed.

Chirp offers dual-band LoRa, so you can make use of both the benefits of the longer range of the sub-GHz regional band, smoothly transition your devices from existing LoRa installations to the Chirp network, as well as make use of the advanced, higher data-rate and bandwith, 2.4GHz ISM LoRa.

How does LoRa handle interferrence?

Despite the fact that the 2.4GHz band is shared between multiple communication and data transfer protocols, the creators and developers of LoRa made it very resilient to interference by making it so LoRa chirps are situated right in the space in between the frequency bands of other protocols, as well as by making sure that LoRa uses very different specifications regarding how often, at what power, and how different the radio signals are transmitted compared to other technologies .

According to Semtech, the creators of the SX1280 chip that enabled 2.4GHz LoRa, the only way in which interference between LoRa and BLE can be created is if the two chips transmitting the full amount of data possible are less than a few centimeters from one another. ([The Immune System | Avoiding RF Interference with LoRa | DEVELOPER PORTAL (semtech.com)](https://lora-developers.semtech.com/documentation/tech-papers-and-guides/interference-immunity))

LoRa classes

What are the types of LoRa?

Besides the classification of LoRa on the basis of frequency, disgussed in [LoRa Frequency Bands], a LoRa-enabled network can also be classified according to the classes of devices that it supports, namely Class A, B or C.

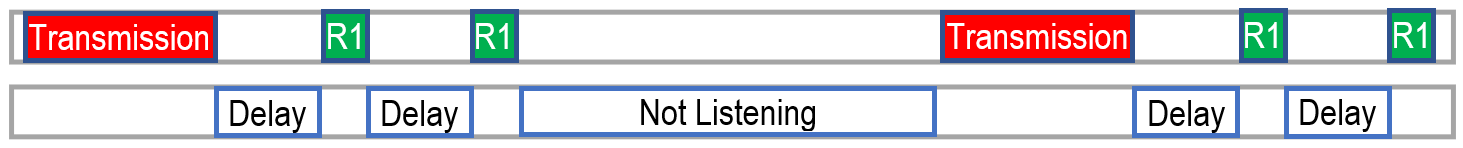
Altough all LoRa devices can communicate in both directions (receive and send messages), there is a difference in how often a device listens for messages sent from the Network/Cloud Applications through the Gateway that mediates between the internet and LoRa. Class A devices only listen in two short periods after its transmission window, Class B schedules additional receiving windows at fixed time periods regardless of whether transmissions were sent by the device in the meantime, and class C is always on, with the only exception being when the device itself is transmitting.

Classes B and C are not found in some of the popular, existing, networks in the IoT space. By enabling them from the get-go, Chirp extends the usability of its ecosystem by making the devices you can connect actually control the environment and respond to it, rather than just monitoring it and logging bytes when neccesary.

Altough support for Classes B and C is a network property, and it is enabled in part by Chirp’s use of a DLT blockchain architecture capable to scale to the amount of transmissions logged by a class B or C device, end devices themselves, as well as their firmware, needs to have class B and C operation set-up and enabled for it to work. Transition between classes is possible, and most devices have open-source firmware that can be edited or updated when needed to enable additional functionality and uses.

Class A

LoRa Type A is the simplest one, and the only one that older, legacy networks support.



Lora Type A devices are only capable to listen for a response from the Gateway after transmitting data during two open communication windows separated by a fixed delay. If the device does not receive anything in these limited windows of time when it is listening, it will not be able to receive anyhing until after it transmits data again and two new downlink windows are opened, identical to the previous ones.

The second Receive/downlink window is only openned in case nothing is received during the first window. It acts as a backup in case packets were lost or communication was not properly established.

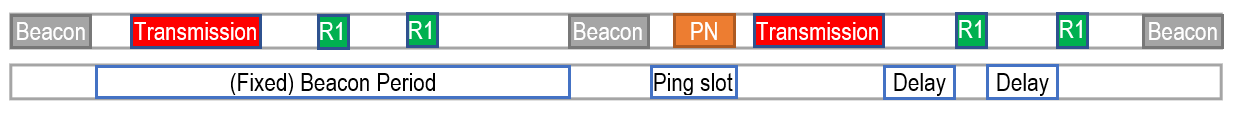
If anything is received during either downlink window, its duration extends until the full content of the received message is transmitted. The duration of the window is only fixed in the case where nothing is received.

Class A devices have the lowest energy consumption and tend to be battery powered with very long autonomy, up to years of operation. As the period in which they are not listening is arbitrary and they can only receive something after they transmit a signal themselves, they can be in sleep mode for the vast majority of their lifetimes. They have artificially high latency because of the arbitrary delays that separate downlink windows.

Example devices: a simple sensor, a a fixed period location tracking device, fire detection, cattle movement tracker.

Class B

LoRa Type B keeps the same behaviours as Type A devices, but in addition it schedules a special downlink window, called a Beacon, at fixed intervals, called the Beacon Period, that will be opened to receive data from the Cloud/Server Applications through a Gateway, regardless of whether or when the device sent a Transmission. When at the scheduled Beacon, an announcement that data will be sent to the device, a downlink period called the Ping slot is created.

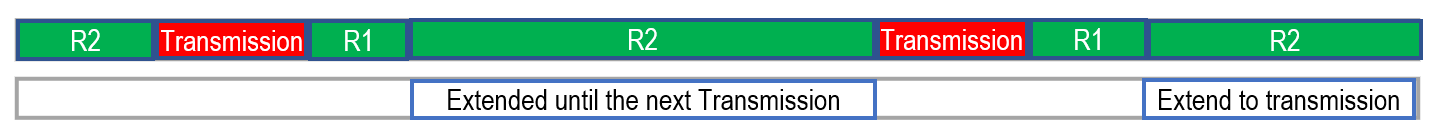


Unlike Type A devices which can have extremely long time periods where no up- or downlinks are created (no signals are sent or received from the device), a Type B device will always wake up to open a receive window for the scheduled Beacon transmissions. Even when no data is exchanged for long periods of time, the Beacon transmissions will still take place at the scheduled Beacon Periods.

This makes Type B devices more energy consuming but will lower latency and with the ability to push firmware upgrades, and they can switch to class A at any time. They are often used for applications such as smart utility meters, temperature reporting or accurate GPS location across time.

Class C

Class C devices are always on. Their receiving window is only stopped when they are transmitting themselves, and are otherwise always listening. They are the only ones that are usually plugged in rather than battery powered because of their increased power consumption, but have significantly reduced latency. This enables type C devices to control physical devices such as valves and switches in real time, opening and closing faucets, turning on and off streetlights, handling a smart irrigation system from a long distance or controlling plenty of other IoT devices.



Still in work

LoRa usage scenarios

Intro

Pizza delivery tracker

Cattle ranch livestock tracker

Weather model data acquisition

Smart Home automation – turning on/off heaters, Acs, ovens, heated blankets, light switches

Tracking shipments across oceans

Bluetooth Low Energy (BLE)

Bluetooth Low Energy (or BLE) is one of the most widely used wireless protocols in the IoT space, completely independent from classical Bluetooth and optimised for small devices with the same range as the original, which makes it a short range, 10-100m, protocol.

The usual BLE device can last somewhere in between a couple of months and a few years on a button cell battery, and they tend to be small and affordable.

The main driver of BLE adoption is the fact that it is compatible with the Bluetooth 4.0 chipsets installed on existing mobile phones and tablets. Some estimates show that up to 1-10 billion BLE devices might be currently in use.

Altough the usual BLE device has very short range but very long lasting battery life, it’s main benefit compared to LoRa or Zigbee is that it is much better optimised for the devices that need to send data often. It is easy to make a BLE device that sends lots of data on a higher frequency but at short range, with almost (but not exactly) continuous data streams possible for small durations or data burts. Compared to Bluetooth that has actual continuous connections, and is will most often be used for a wireless keyboard and mouse, some BLE applications also exist where battery is more important than the 100ms latency.

BLE uses the same 2.4 GHz radio frequency band as other protocols installed on the Blackbird, which makes it possible to share a single antenna with the other chipsets.

NOTE: Unlike classical Bluetooth, BLE has a much higher latency between connections (100ms compared to 6ms), a single BLE communication only transmits data in short bursts, it is not voice-capable, has a slightly lower datarate, but slightly higher than 2.4GHz LoRa.

BLE Applications

Applications include:

|  |  |
| --- | --- |
| MESH | Passing data short-range between devices across longer distances |
| Healthcare | * Blood Pressure * Health Thermometer Measurement Devices * Glucose Level Monitors * Continuous Glucode Level Monitors |
| Sports | * Body Composition Measurement * Cycling Speed and Cadence (sensors attached to bikes) * Cycling Power Profile (including exercise bikes) * Heart Rate Monitoring * Location, Navigation, Tracking using GPS |
| Environmental | * Enironmental Sensors * User Data Acquisition (e.g. heat in the room from a radiator) |
| Hardware | * Connecting a Keyboard (but not as precise due to latency) * Battery Level and Battery State of batteries in a device |
| Proximity | * Electronic Leash (check if another device goes out of range) * „Find Me!” (issues an alert on a second device) * Proximity estimation (detect if a connected device is close) |
| Audio (LE Audio) | * Headphones * Hearing Aids   (Lower Quality, better battery life compared to classic Bluetooth) |

Becase of the unique fact that BLE is installed on almost evert single smartphone built since 2012, it can create unique use cases that involve smartphones and beacons. A Beacon is a BLE enabled device that sends and receives BLE signals and can validate whether it should connect to a device using a unique ID. This makes it possible to directly target smartphones using BLE beacons, for example by sending off a notification or service some specific apps.

For example, a store can use this functionality to send users, who enable notifications from their app, a targeted promotional message as soon as they enter the store, or a welcome message, or a link to some useful information that they may need, such as where departments are located or where to find the closest customer service advisor.

Altough BLE can be used to assign unique IDs to real items using BLE tags, and a BLE Beacon (such as a Blackbird) can read off the tags to detect which item exists, it is not able to easily locate items up to meter-level accuracy due to it being limited to the use of RSSI

Zigbee

Similar to BLE, Zigbee is a short-range IoT protocol specialised in low-power radio devices at a range of 10 to 100m. Zigbee operates in the same 2.4 GHz ISM band as the other IoT protocols installed on the Blackbird. Unlike BLE and LoRa, the Zigbee module comes installed as an external, optional dongle that can be ommited when it is not required by a Blackbird’s Keeper.

Unlike BLE and LoRa, Zigbee is especially optimised for home automation, with its most common uses being in remote light switches, smart plugs, smoke and intruder detection, local sensors, and does not come with the same versatility as other IoT protocols.

Zigbee offers a capped data rate of 250 kbit/s, but it does not have the same long range properties of LoRa, as well as the ability to trade-off, when needed, between range, power consumption and data-rate, without external input, as dual-band LoRa. Neither does it have the ability to reach high data rates as BLE for the same range.

To put this comparison in numbers, BLE can reach up to 2Mbit/s in data rate, 8 times higher than Zigbee, whilst LoRa can reach 100-1000 times the range, and it’s not much different even when considering a configuration using the equivalent data rate.

However, the strong suit of Zigbee is that it was devised from the start to be easy to integrate in a Mesh Network, particularly suited for wireless control and monitoring, similar to LoRa class C. This makes it extremely simple to work with even if you are a complete stranger to IoT, and this simplicity made it a top IoT protocol for home low complexity home automation solutions, with more than 2 billion devices currently on the market.

Blackbird

## What is the Blackbird?

The Blackbird is Chirp’s flagship IoT Gateway, joining together in a single plug-and-play box all of the major IoT protocols: [**LoRa**](/chirpwireless/docs/-/blob/Chirp-Wiki/IoT-Protocols/LoRa/LoRa-intro.md) , [**BLE**](/chirpwireless/docs/-/blob/Chirp-Wiki/IoT-Protocols/BLE/BLE-intro.md) , [**Zigbee**](/chirpwireless/docs/-/blob/Chirp-Wiki/IoT-Protocols/Zigbee/Zigbee-intro.md) . The Blackbird doubles down as a IoT Gateway, an antenna device that provides wireless coverage for the IoT, as well as a Crypto miner.

To find out more about generating tokens, check out [**Generating Chirp Tokens**](/chirpwireless/docs/-/blob/Chirp-Wiki/Chirp-Tokens/blackbird-tokens.md)

## What is a Keeper

As each device that pays to connect to the Chirp Network routes its traffic through one of the user-installed Blackbirds around the world, and the traffic is transformed into rewards for the Owner and Operator of the Blackbird, its [**Keeper**](/chirpwireless/docs/-/blob/Chirp-Wiki/Chirp-Technology/keepers.md).

## What does the Blackbird do?

The Blackbird is a point of communication between IoT devices, which transmit radio signals containing a variety of data types and information, and the end-user. In essence, the Blackbird translates the language of the IoT (the communication protocols) and transforms it in a way in which it can be transmitted to the internet, and then understood and used by the [**Chirp Dashboard**](/chirpwireless/docs/-/blob/Chirp-Wiki/Chirp-Technology/dashboard.md), the webpage and mobile application where all of your IoT functionality is concentrated.

For the latter stage, different applications can be run remotely on the cloud using [**Cloud Applications**](/chirpwireless/docs/-/blob/Chirp-Wiki/Chirp-Technology/CLAs.md) and [**Smart Contracts**](/chirpwireless/docs/-/blob/Chirp-Wiki/Chirp-Technology/smart-contracts.md), and this will be further discussed on their own Wiki Entries.

## How can I become a Keeper?

Installing a Blackbird is simplified to its core, as it was entirely developed and designed in-house by the Chirp Team.

It functions as a plug-and-play device, connected to an antenna on one side, the internet through an ethernet cable or WiFi, and powered up using the same ethernet cable. Only on the Blackbirds operated using WiFi, a separate power cable needs to be connected.

For enthusiasts and maximizers, it is possible to use either the antenna provided in the kit or a custom one of your choosing, perhaps one that provides higher gain, is bigger or already installed.

# Blackbird Token Generation

## Chirp Tokens

\*\*[Blackbirds](../)\*\* are IoT \*\*[Gateways](../)\*\* as well and Chirp \*\*[Miners](../)\*\*, able to generate Chirp’s proprietary crypto token as rewards for providing IoT coverage for nearby users, or by facilitating the transfer of data and information on the Chirp Network.

## Proof-of-Coverage

The first method through which a Blackbird generates tokens, and the dominant way in which these will be distributed for the first few years from the launch of the Chirp Network, is Proof-of-Coverage.

This is a mechanism that rewards users for providing IoT coverage in a way that can be validated and proven by other Gateways or Master Gateways on the Chirp Network, even when no IoT user uses the network to transfer data around this time.

The validation process involves an algorithm where multiple Blackbirds interact in order to test the validity of each one of them, in addition to a series of validation tests on the internet connection and through GPS.

## Data Transfer Rewards

\*\*[Blackbirds]()\*\* listen for IoT devices that communite with the Chirp Network using either one of the installed communication protocols. When a connection is established, and data is transferred from an IoT device to a Blackbird, to be then interpreted and sent through the internet, the Keeper that owns the Blackbird that mediated this interaction will be rewarded with tokens proportional to the number of bits that were sent by the IoT device.

The User who owns the IoT Device pays for the use of the Chirp Network by buying Chirp Tokens using fiat money, which once they are used transform into Data Credits. These are only partially reminted into Chirp Tokens when they are received by the Keeper, so the total supply of Chirp tokens in circulattion will always reduce in time.

## A spoofing-free network

A spoofed Blackbird, or a Blackbird that was hacked and tempered with, will be unable to pass through these validation tests, and will therefore not generate any tokens to its owner.

Stolen Blackbirds that can be validated will continue to generate tokens for the original Keeper. A thief cannot register the Blackbird to their own wallet or account, and the location of the Blackbird can be verified through GPS and LoRa at extreme accuracy.

# Chirp Tokens

Chirp tokens are the cryptocurrency used to consolidate value on the Chirp Network. It is used by Users of both the IoT and the ISP side to access the network and buy IoT coverage or wireless broadband connection, and it is also used to reward Keepers or Cardinal DAO investors.

## Chirp Token Creation

The Chirp token is created through mining by owning and correctly operating proprietary Chirp Hardware such as the IoT Blackbird or the Cardinal. The mining process involves providing wireless coverage to nearby Users who wish to access the network, and making it possible for them to transfer and exchange data between IoT devices and the internet, or connecting them to the internet at fiber speeds.

Chirp Tokens created from the Proof-of-Coverage process early on are newly minted tokens that first appear at the time when they are bought by the User who buys IoT Data Credits or a Wireless Broadband Subscription using Fiat Money through, for example, a Credit Card on-ramp.

Chirp Tokens that are received by the Keepers who facilitate the transfer of data through the Blackbird they own, or participants in the installation of a Cardinal through the DAO, are Tokens that are reminted from the burning of Data Credits, the fixed price utility token that translates between the variable price of the Chirp token and the amount of data that someone can transmit through the Network. Thus, increasing the usage of the Chirp Network does not inflate the amount of tokens in circulation, but rather burns existing tokens and deflates the total supply.

R2

R2

R1

R2

R1

Transmission

Transmission

Extend to transmission

Extended until the next Transmission