



Linux & IOT in the web era

Alessio Di Maria
CTO at In Time Link

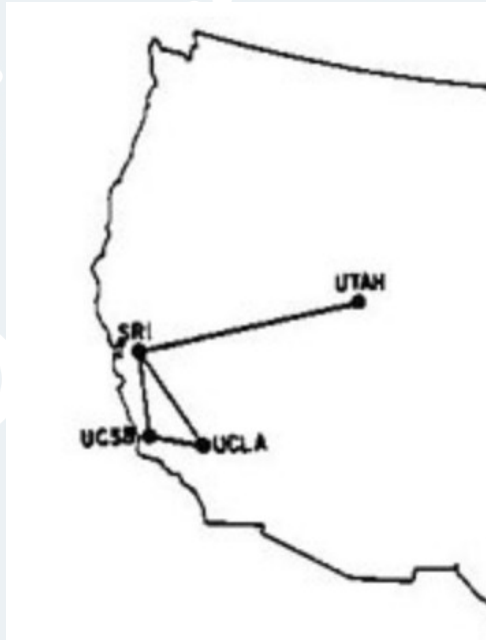
Cos'è l'Internet Of Things?

Una rete di oggetti connessi a internet in grado di collezionare e scambiare dati.



Un po' di storia

Arpanet 1969



Internet Toaster 1990



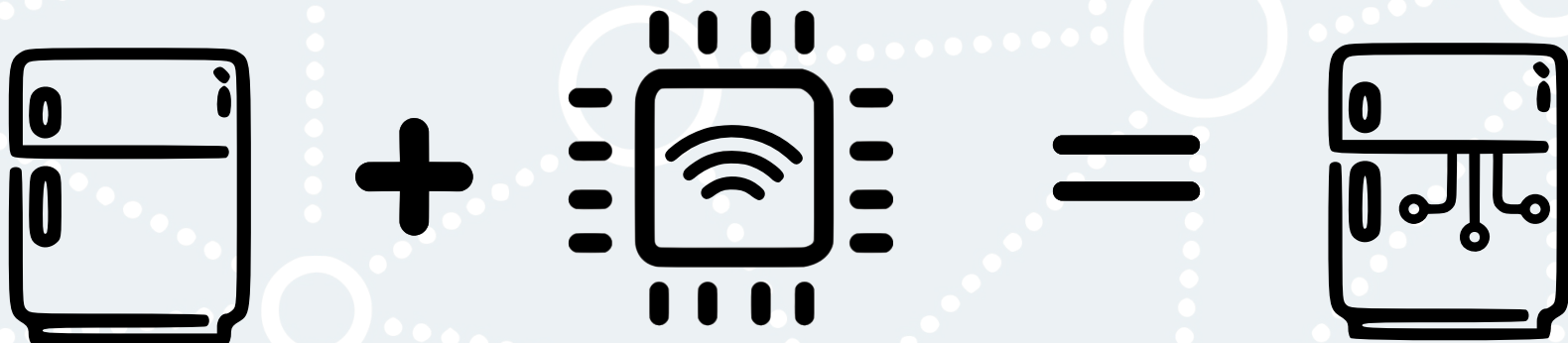
WIFI IEEE 802.11 1997



Bluetooth SIG 1998

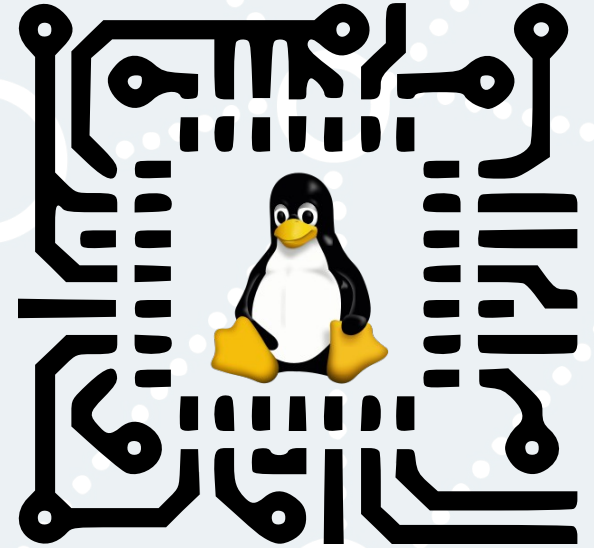


Sviluppo di device IoT



Perchè linux lato hardware?

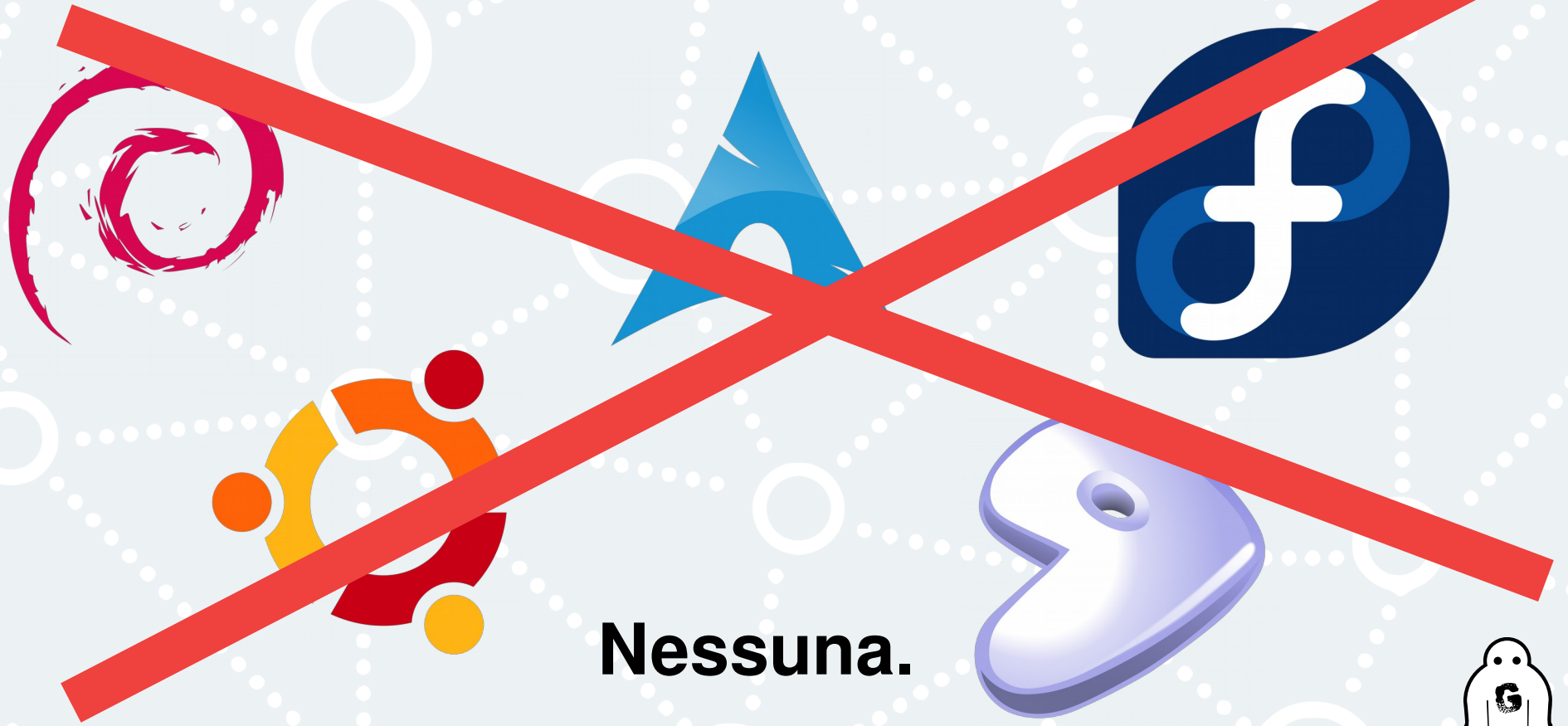
- Dimensioni ridotte
- Velocità di implementazione (Time to market)
- Supporto da parte dei produttori hardware
- Affidabilità e sicurezza
- Elevato numero di supporti



Quale distribuzione linux?



Quale distribuzione linux?



Nessuna.



Costruire la propria distro linux



“Buildroot is a simple, efficient and easy-to-use tool to generate embedded Linux systems through cross-compilation.”



Costruire la propria distro linux

Pro:

- Facile da usare
- Leggero
- Relativamente versatile

Contro:

- Poco supportato
- Difficile da automatizzare



Costruire la propria distro linux



“The Yoct Project. It’s not an embedded Linux distribution, it creates a custom one for you.”



Costruire la propria distro linux

Pro:

- Versatile
- Automatizzabile
- Estremamente supportato
- Toolkit di sviluppo
- Pacchetti RPM

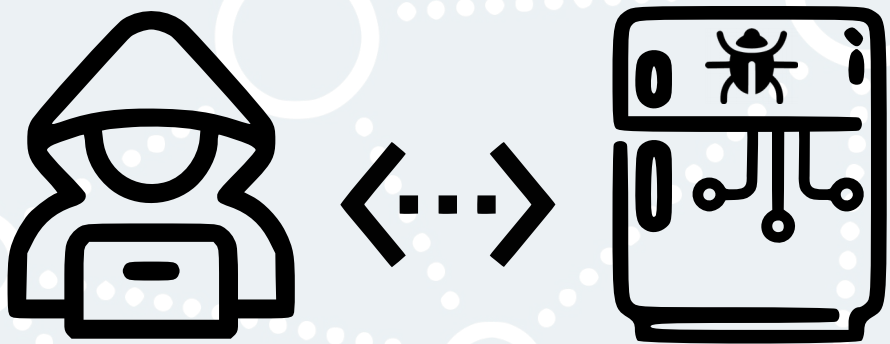
Contro:

- Complicato
- Pesante

yocto
PROJECT



Cosa succede se un device viene compromesso?

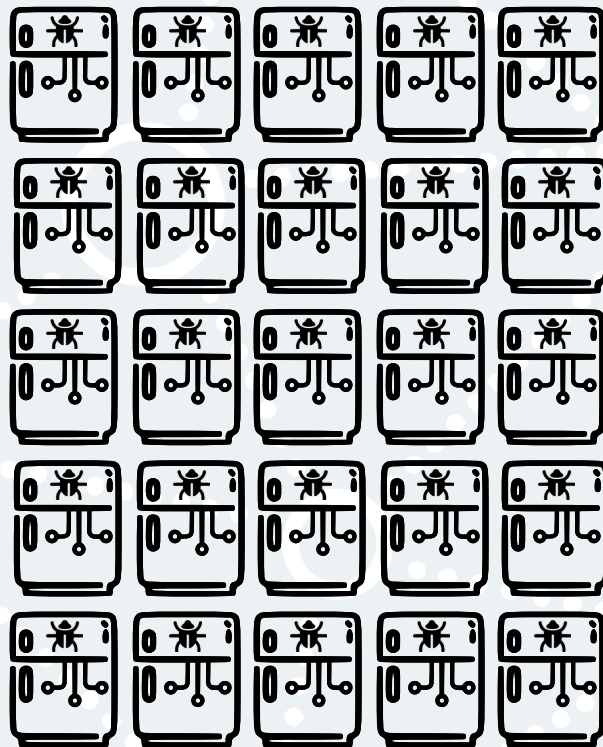


Criticità aggiornamenti “Over the air”

- Validazione del package
- Meccanismo di recovery
- Aggiornamenti parziali
- Aggiornamento firmware MCU
- Parzializzazione del download
- CDN



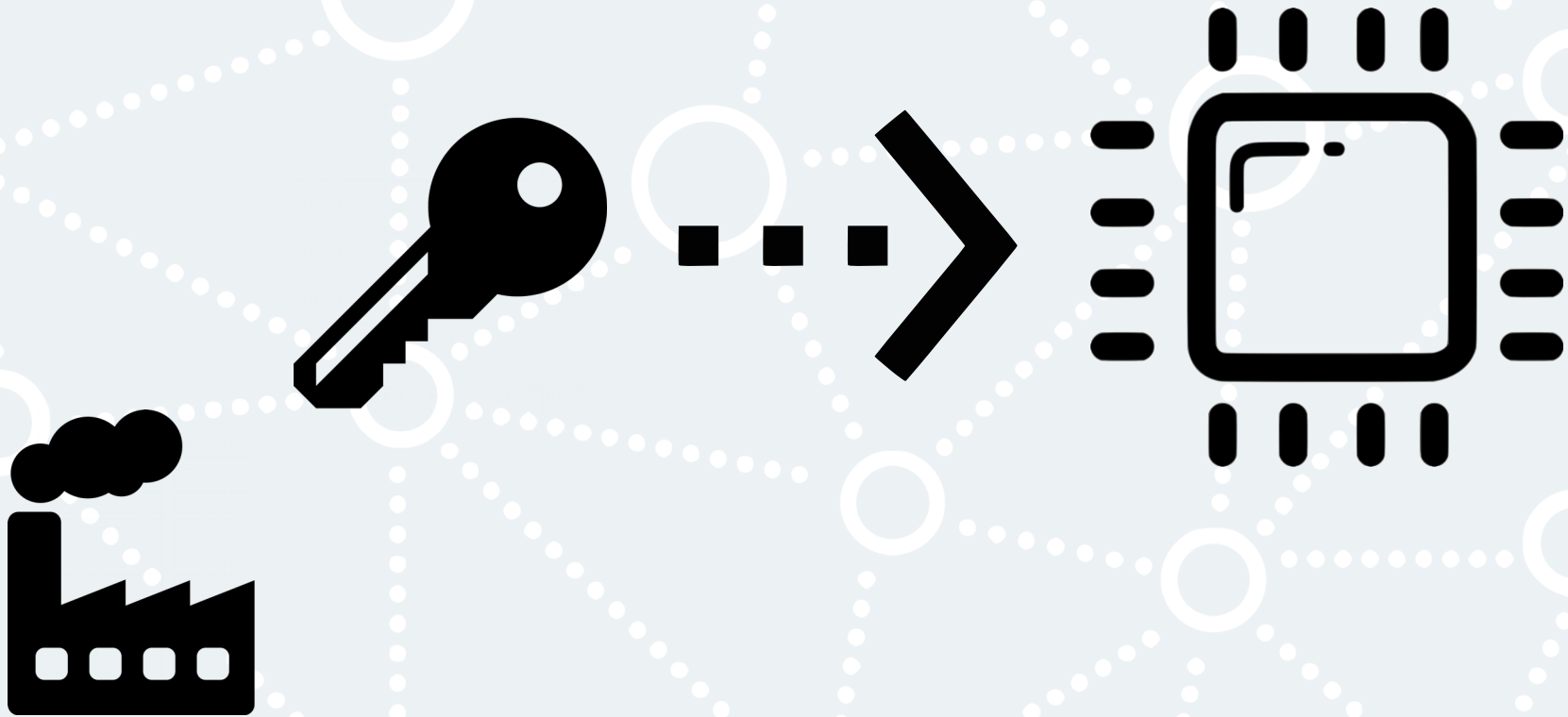
Cosa succede se più device vengono permanentemente compromessi?



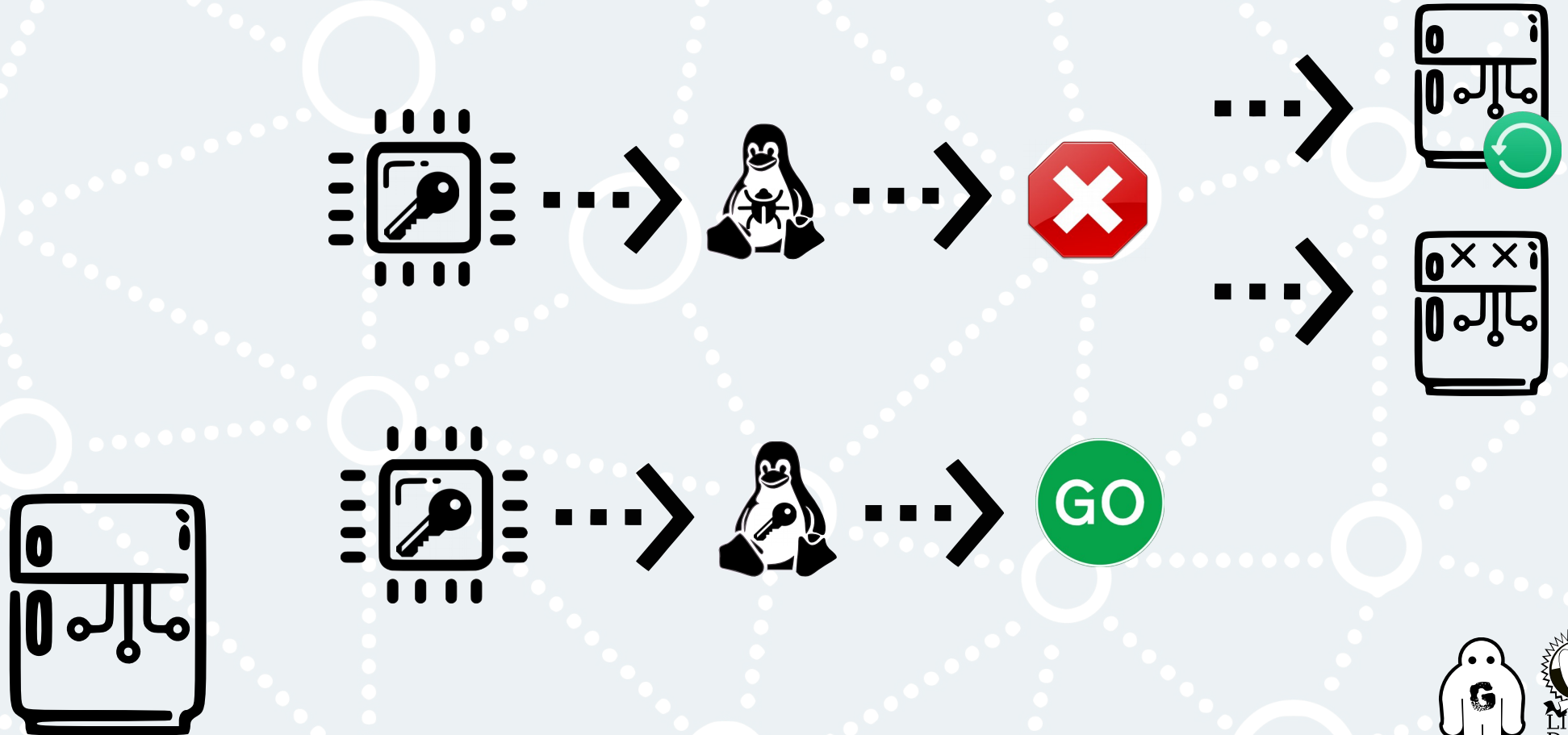
**Come evitare che i device vengano
permanentemente infettati?**



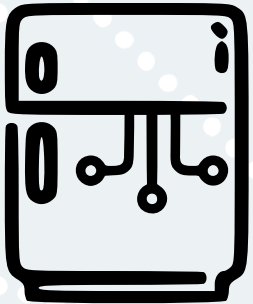
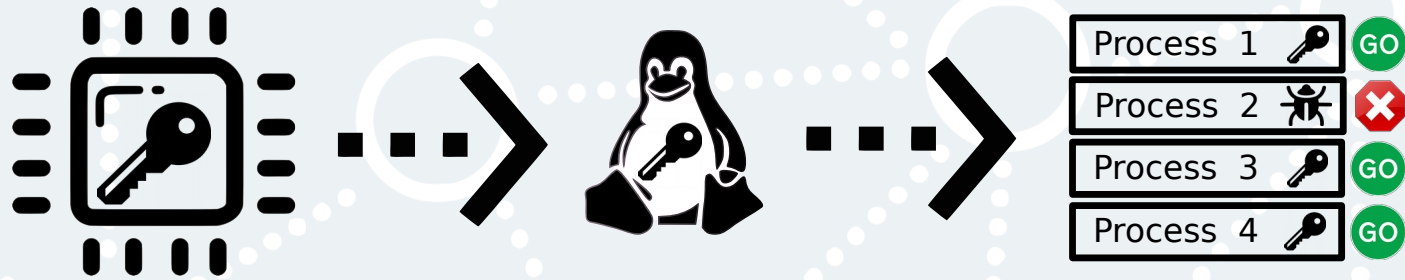
High Assurance Boot – Produzione



High Assurance Boot – Secure Boot



Secure boot – Chain of trust

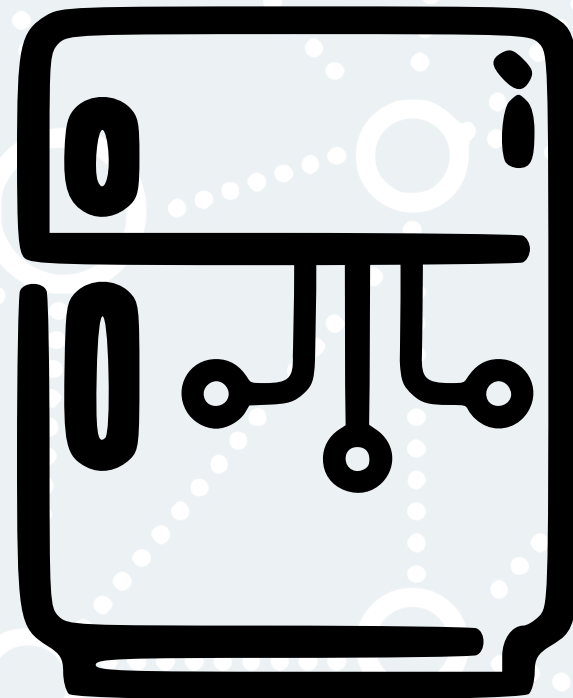


Stack di una rete IOT - “Thing” verso internet



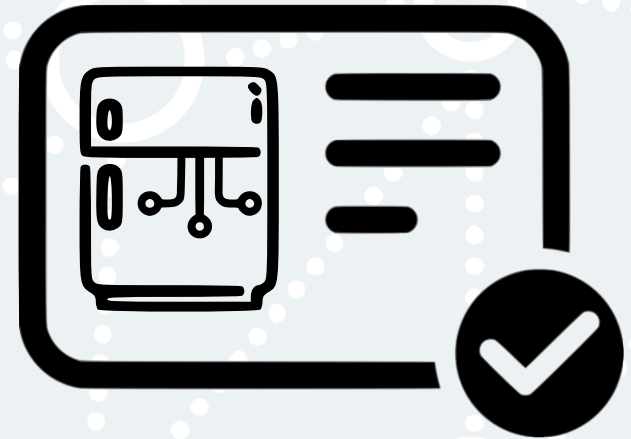
Criticità lato “Dispositivo”

- Interoperabilità
- Connettività intermittente
- Costi di produzione
- Aggiornamenti di sicurezza



Metodi di Autenticazione lato Dispositivo

- Autenticazione tramite modulo hardware
- Autenticazione tramite certificato software



Autenticazione Dispositivo via software

Pro:

- Facilità di implementazione
- Costi ridotti

Contro:

- Rischio di compromissione della chiave
- Elevato consumo di risorse

OpenSSL
Cryptography and SSL/TLS Toolkit



Autenticazione Dispositivo via hardware

Pro:

- Sicurezza elevata
- Utilizzo di risorse ridotto

Contro:

- Aumento dei costi di produzione



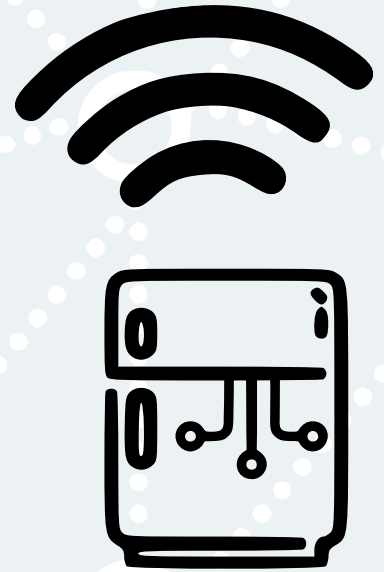
Sicurezza del dato

- Utilizzare SSL
- Utilizzare il certificate pinning
- Mantenere attivo un RTC a bordo



Instabilità di rete

- Implementare procedure “*fault tollerant*”
- Ridurre l'MTU e la dimensione dei payload
- Preferire protocolli p2p



Open Thread – 6lowpan

- Implementazione opensource di Thread
- Rete mesh
- Ipv6 su IEEE 802.15.4
- Border routers
- Low Power Long Range (100m/1km)

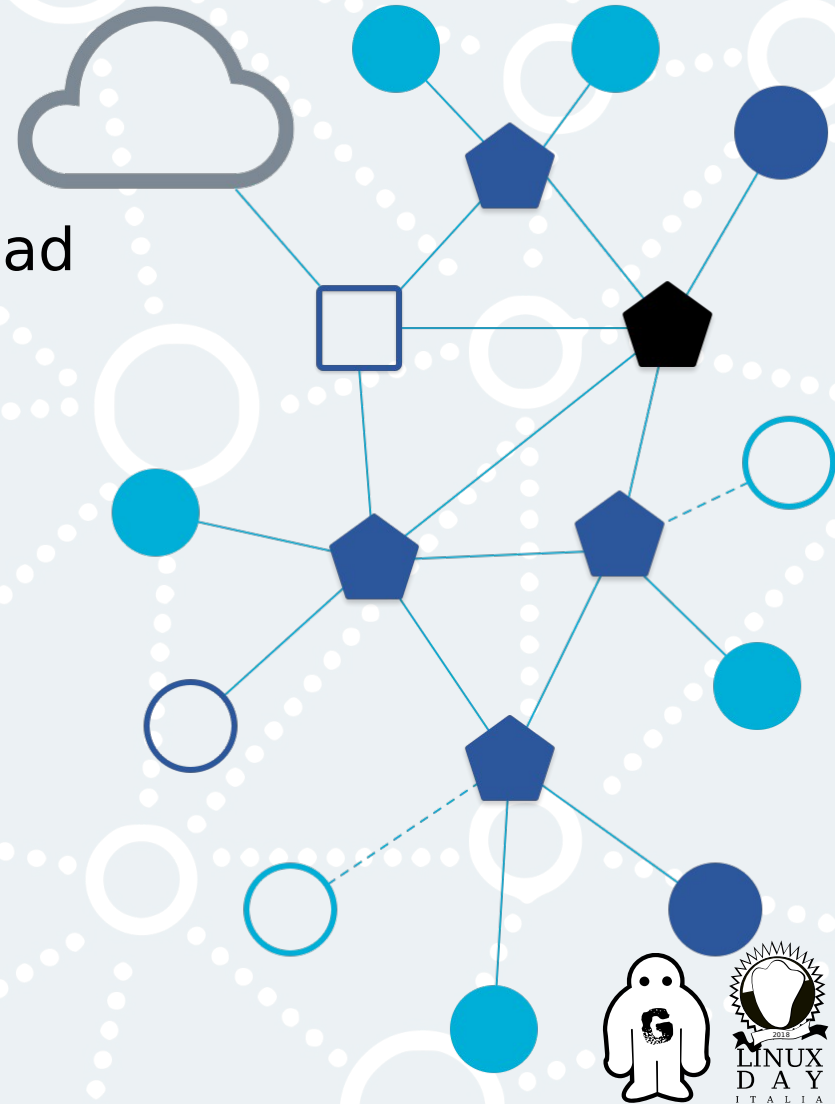
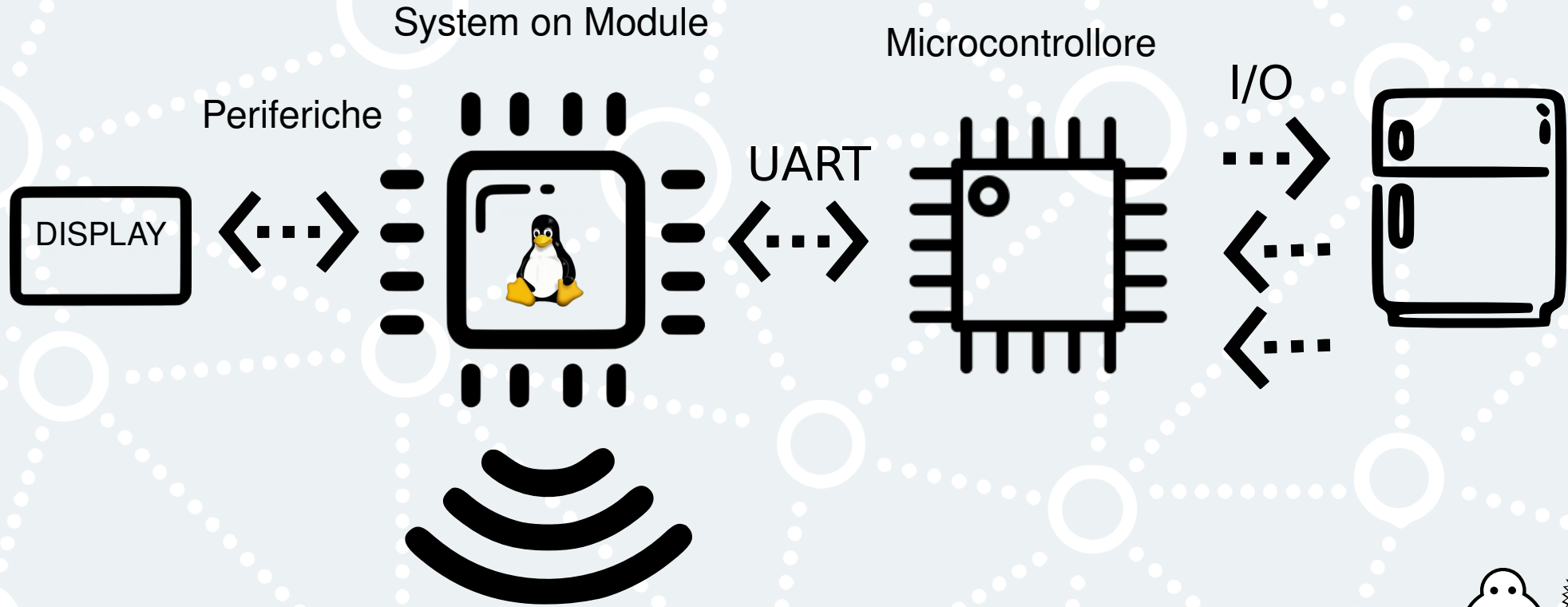


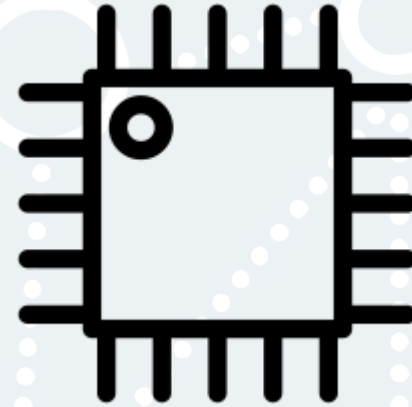
Diagramma hardware



Perchè un microcontrollore esterno

- Più IO
- Più affidabile
- Accensione immediata
- Risposte real time

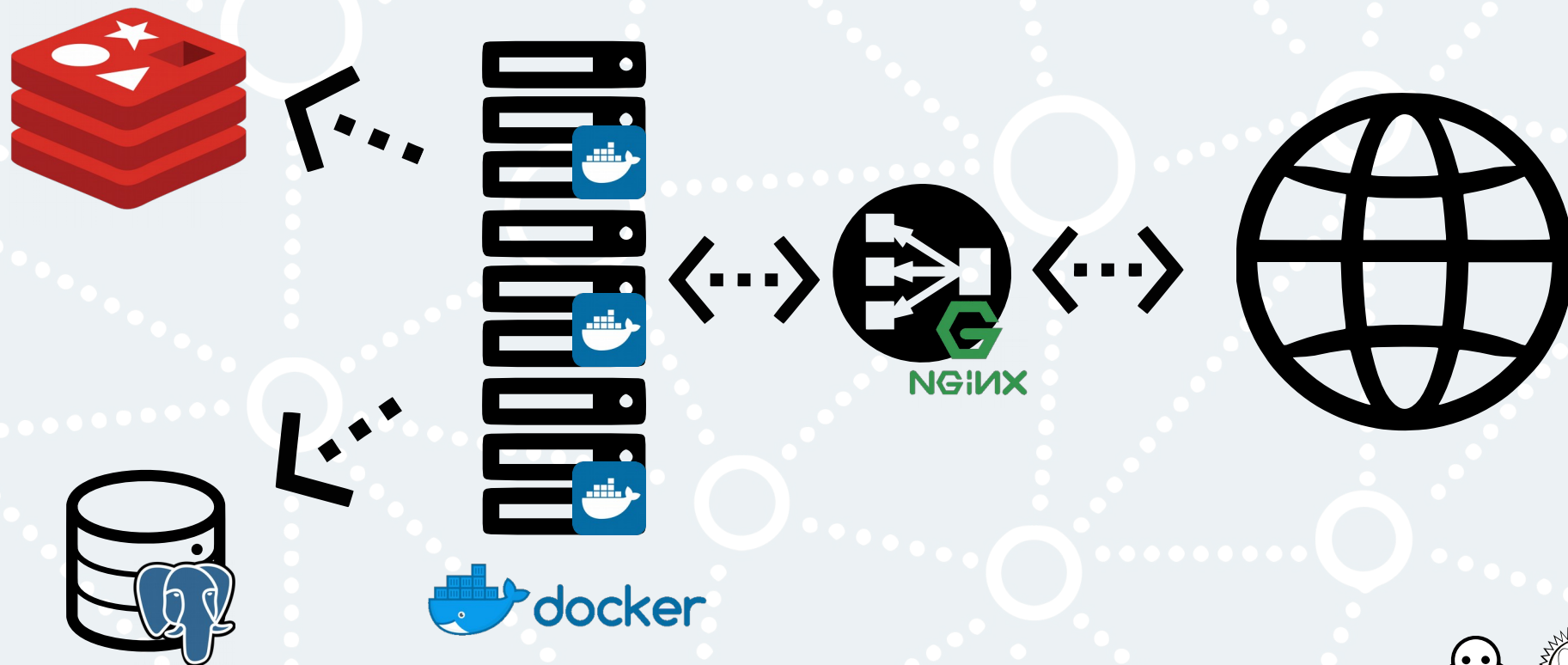
Microcontrollore



Stack di una rete IOT - Overview



Stack di una rete IOT - Lato cloud

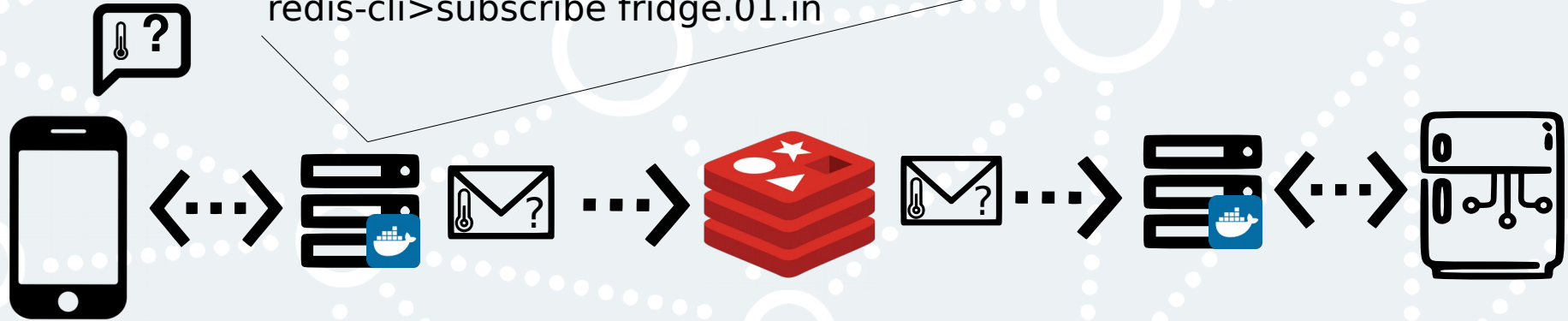


Message Bus – Real time messaging 1/3

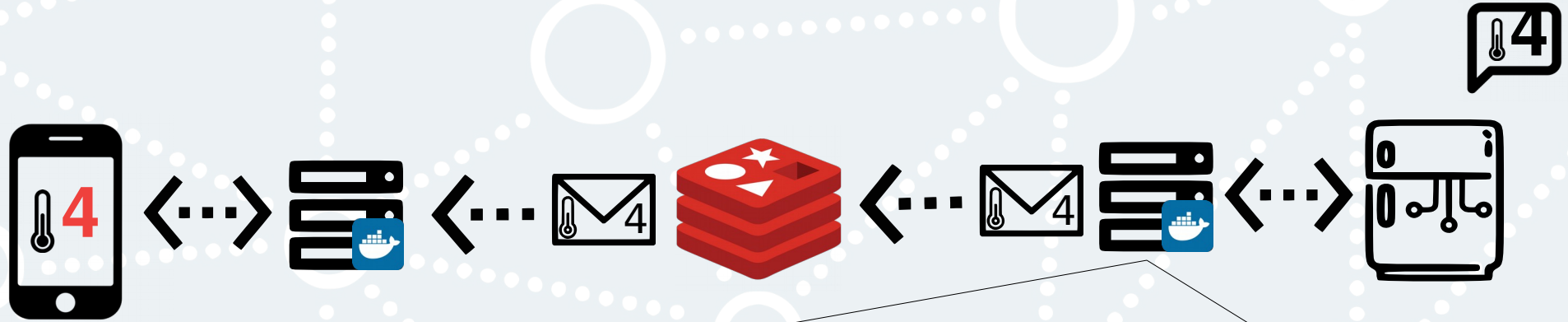


Message Bus – Real time messaging 2/3

```
redis-cli>publish fridge.01.out "temp ?"  
redis-cli>subscribe fridge.01.in
```



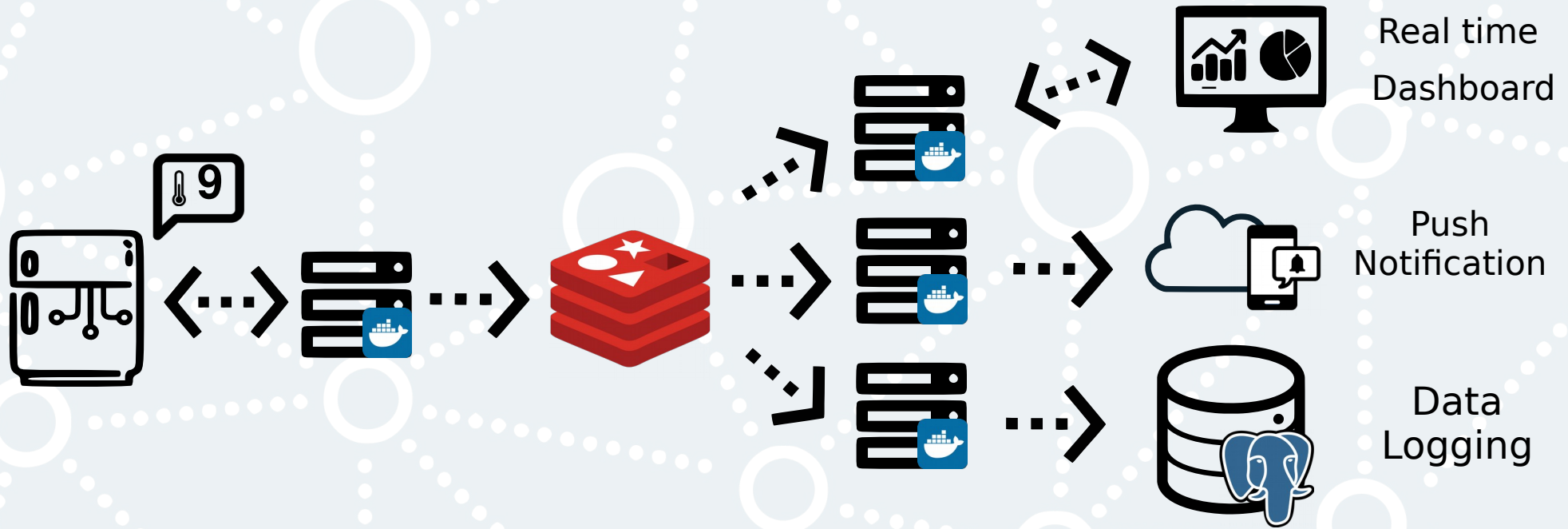
Message Bus – Real time messaging 3/3



`redis-cli>publish fridge.01.in "temp is 4"`



Message Bus – Microservices





Grazie!

Alessio Di Maria

alessio.dimaria@gmail.com

+39 3397113695