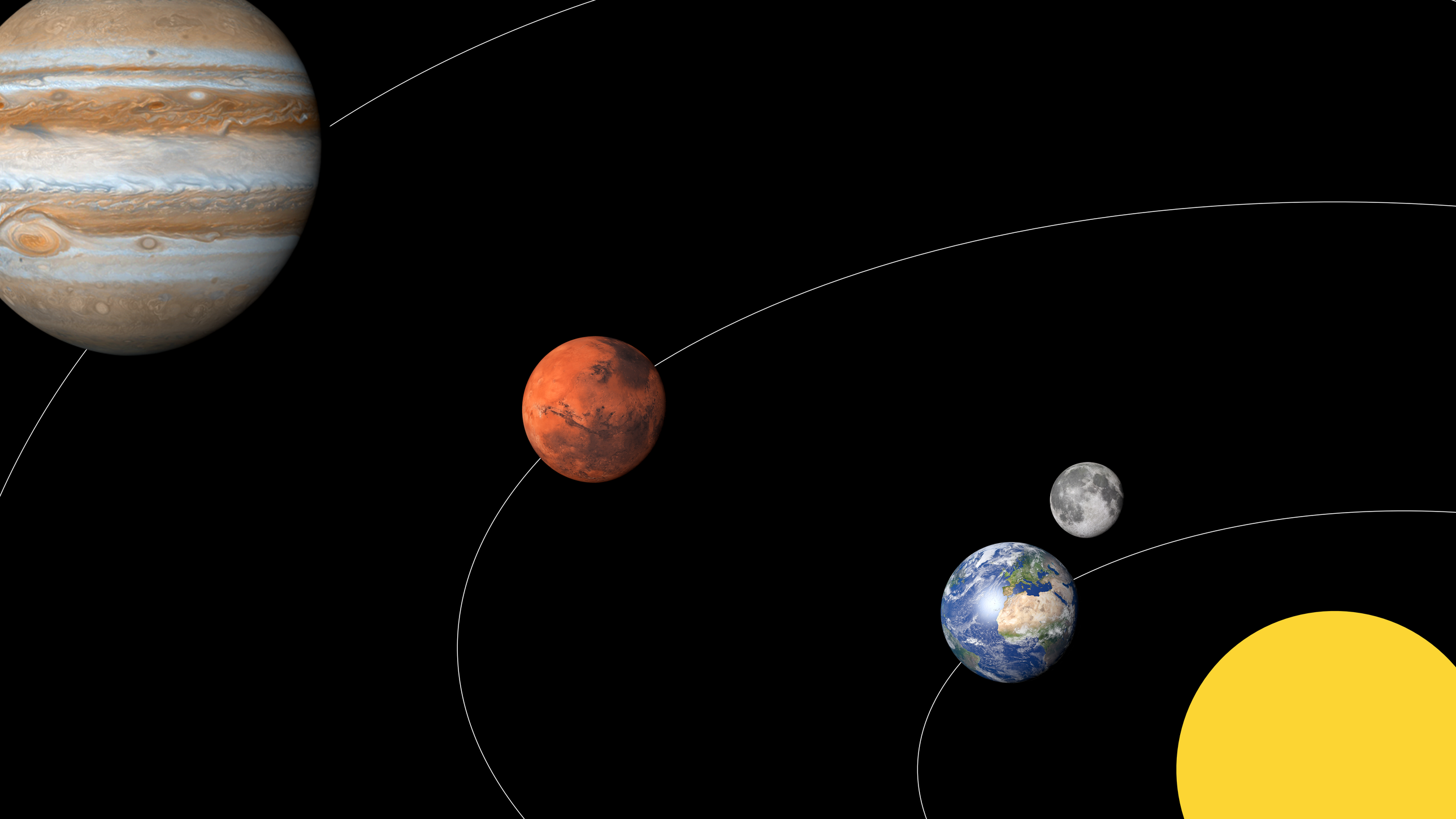
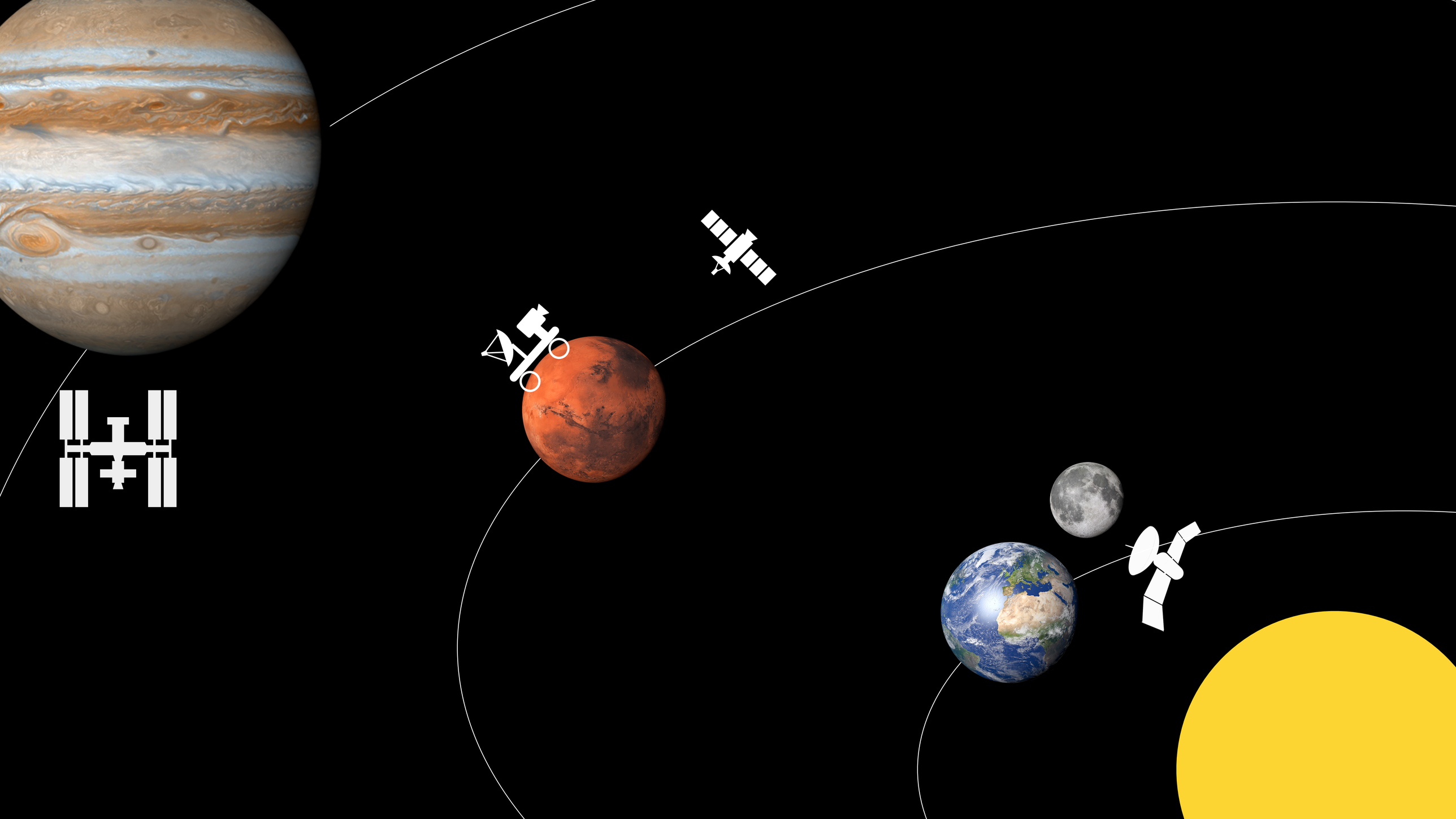
Towards Protecting Billions and Billions of Bits on the Interplanetary Internet

WILLIAM & MARY

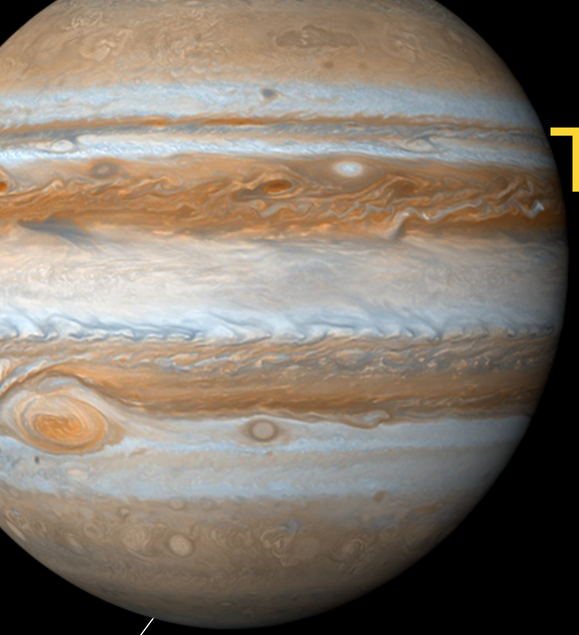
CHARTERED 1693

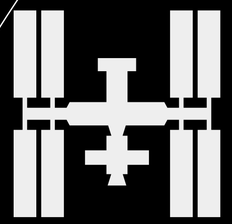
Stephen Herwig Feb 27, 2023

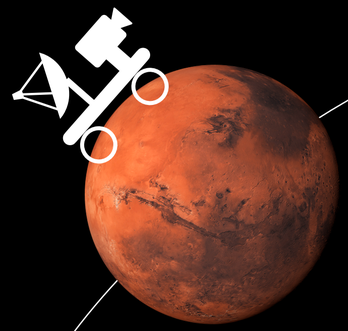


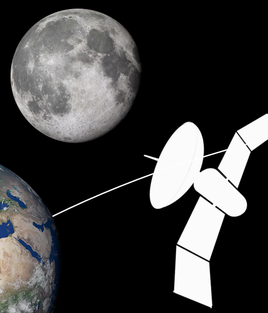


The Internet doesn't work in deep space

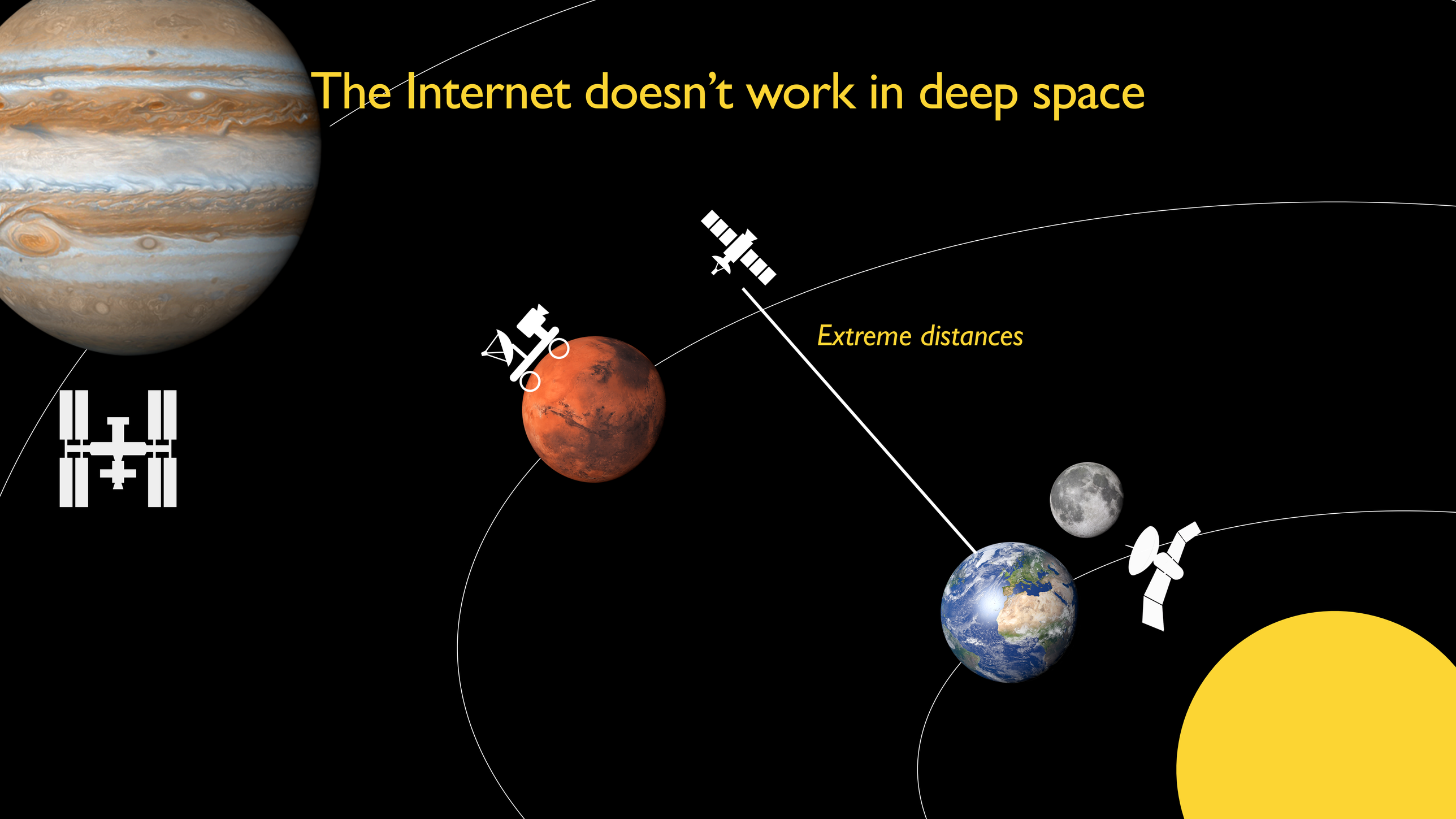




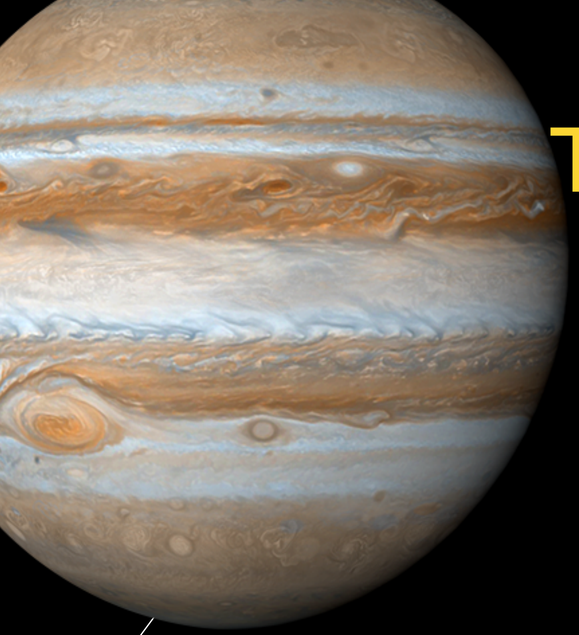


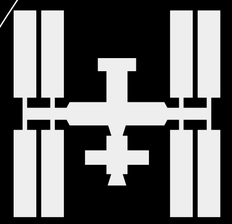


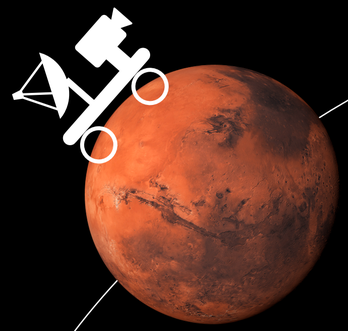
The Internet doesn't work in deep space



The Internet doesn't work in deep space



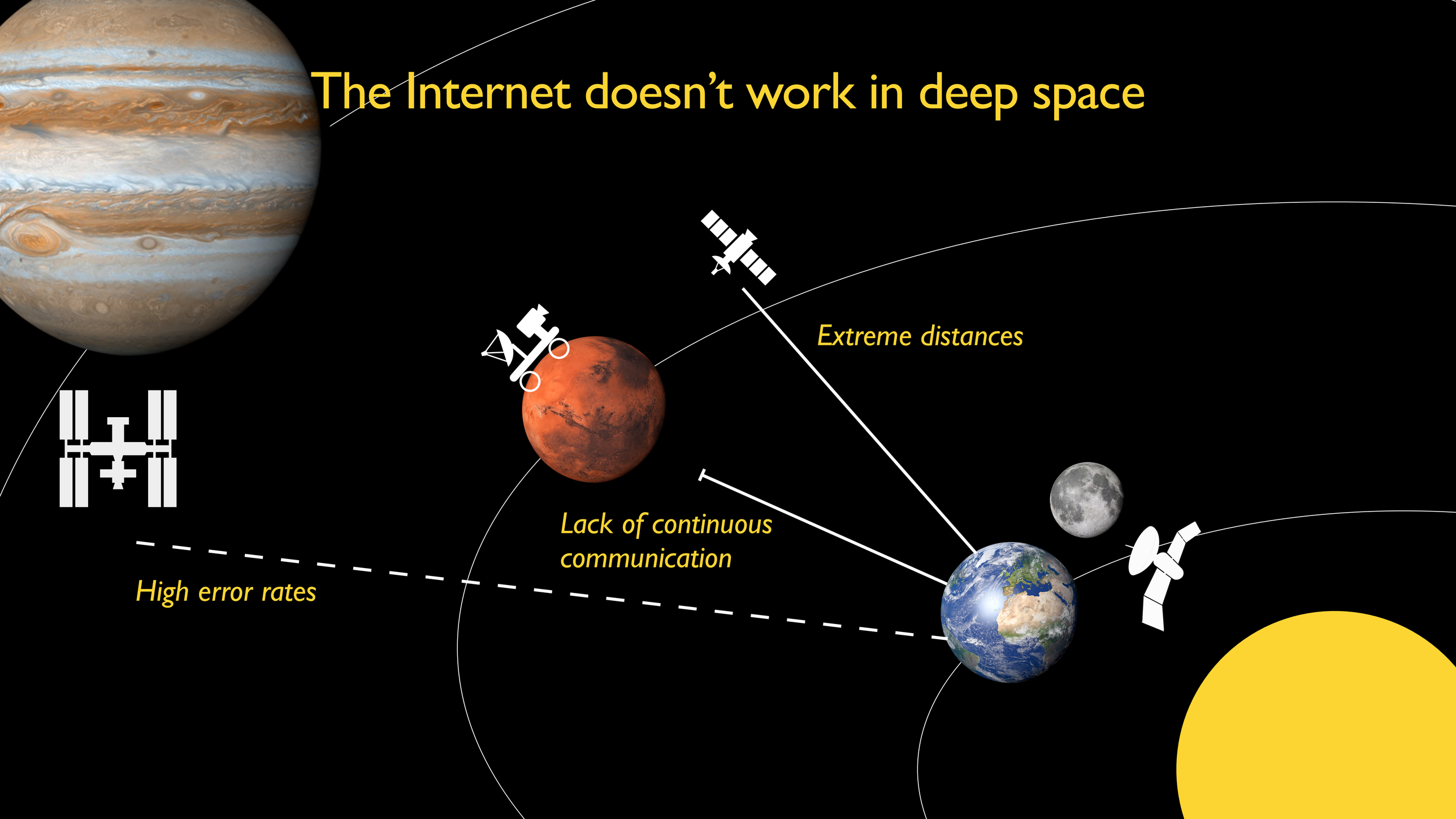




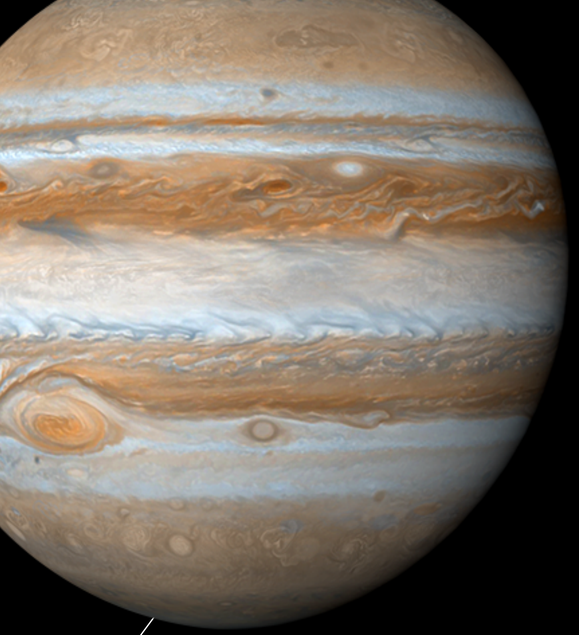
Extreme distances

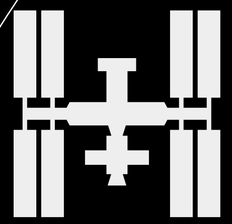
Lack of continuous communication

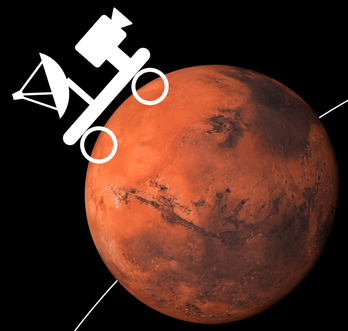
The Internet doesn't work in deep space

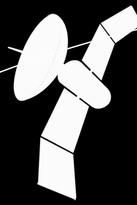


Interplanetary Internet (IPN)

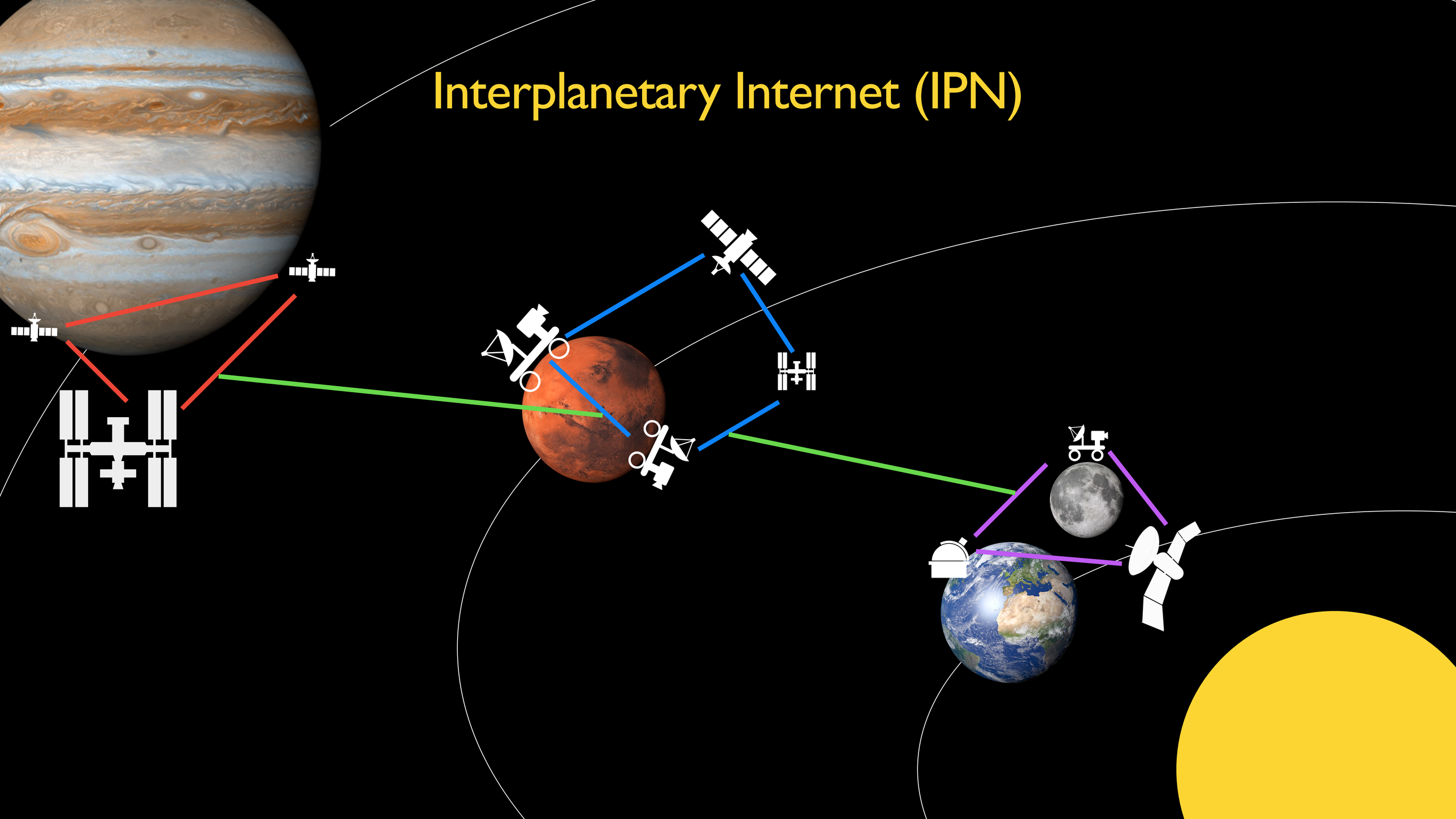




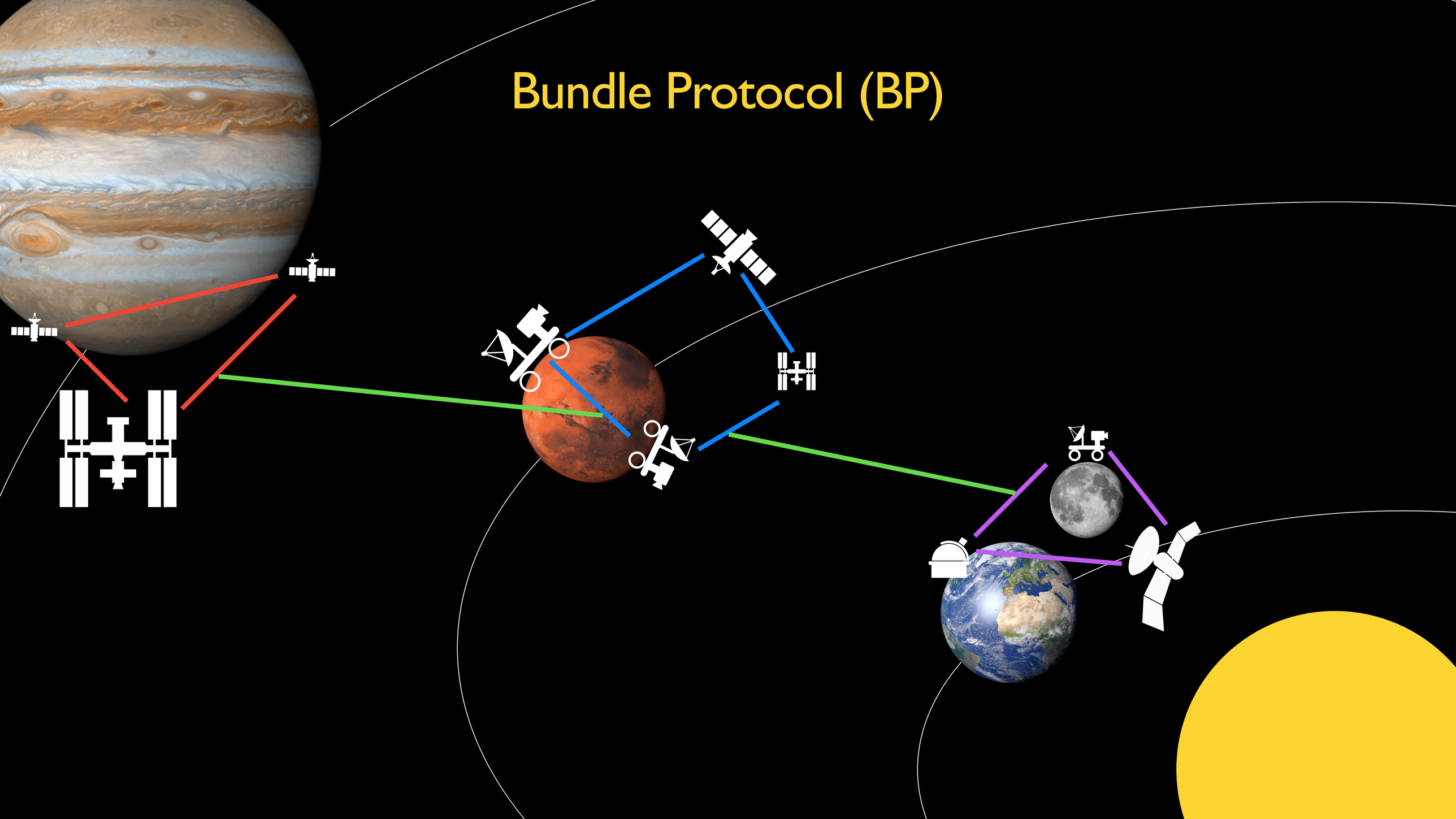




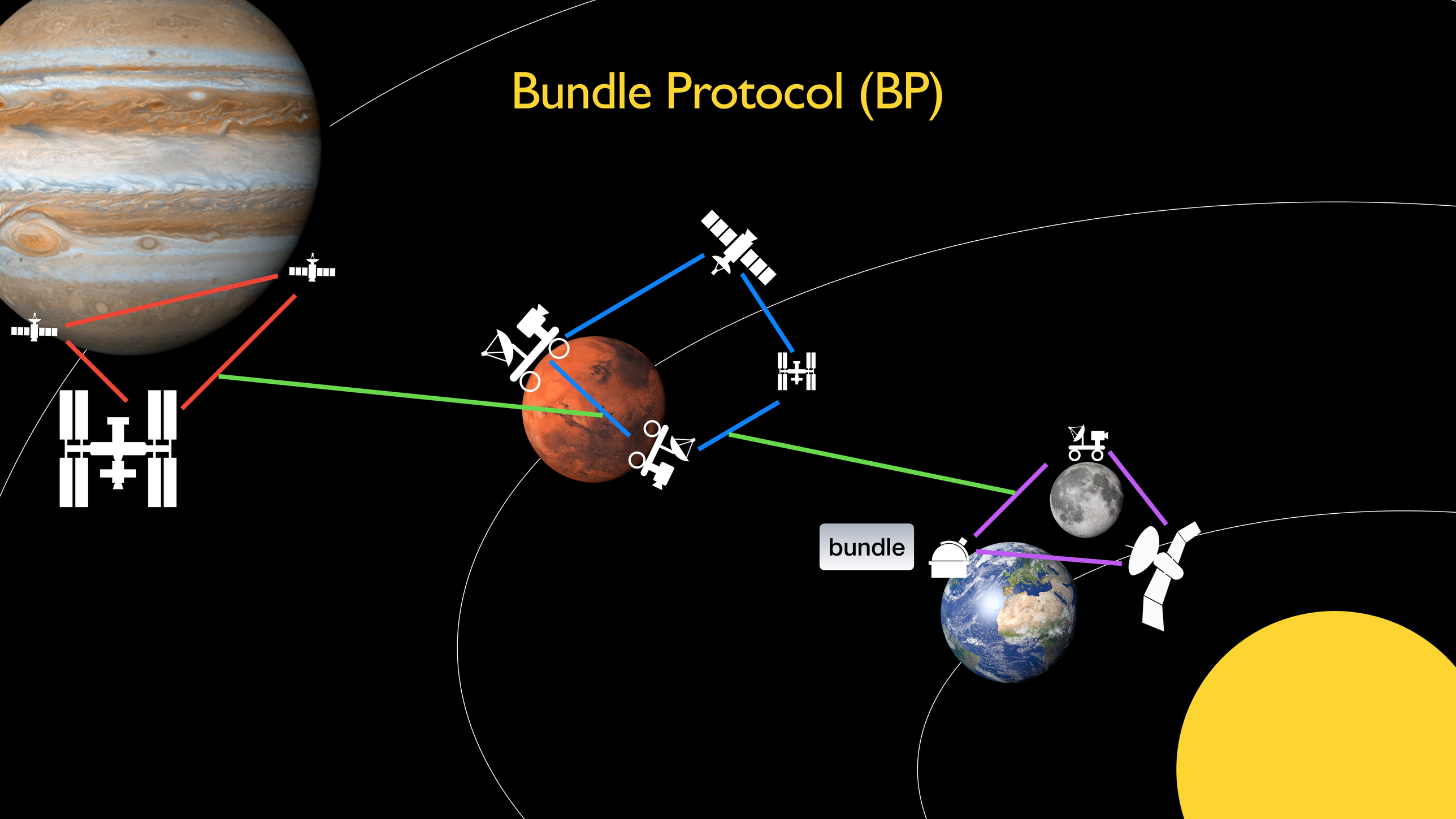
Interplanetary Internet (IPN)



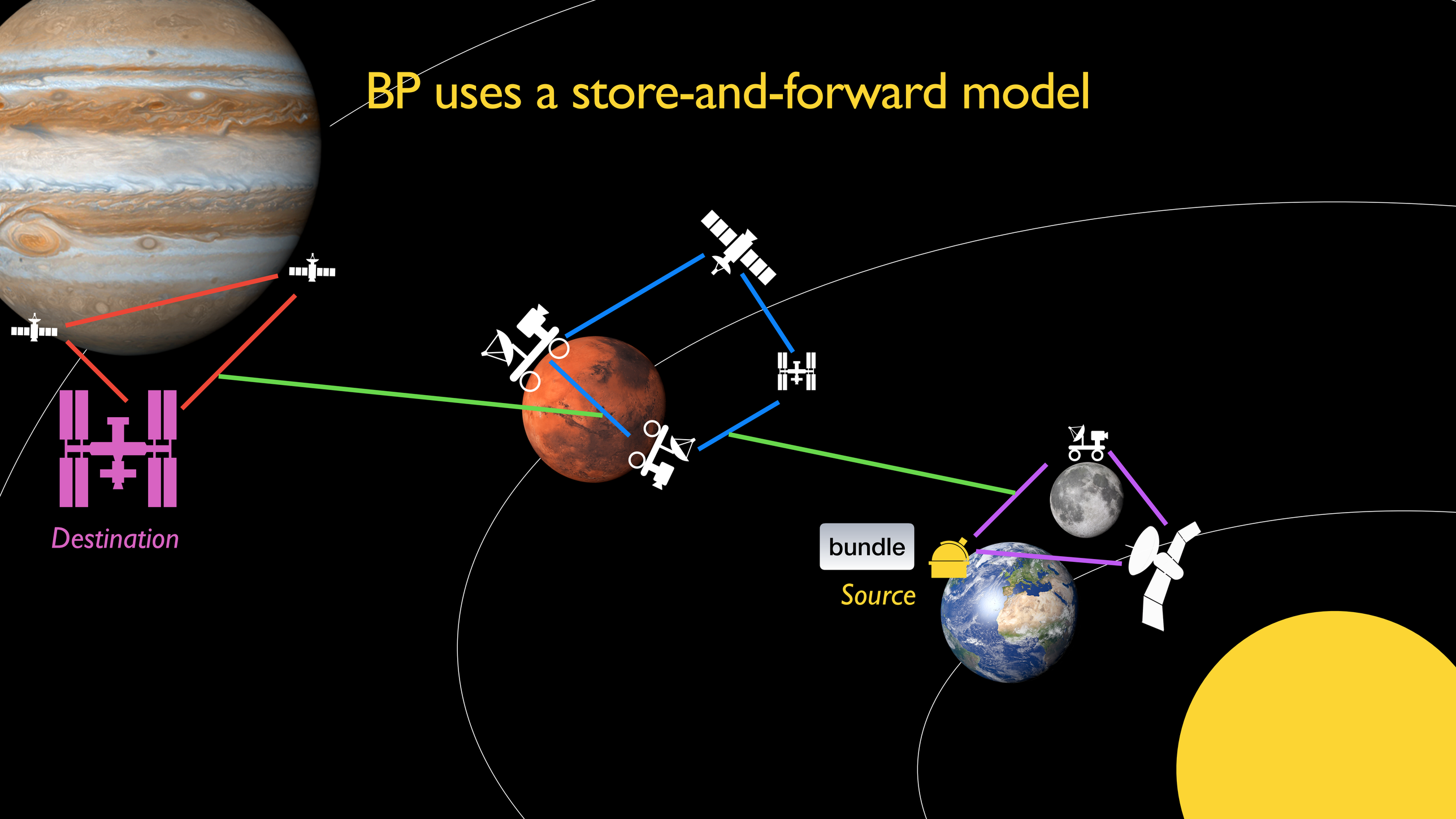
Bundle Protocol (BP)



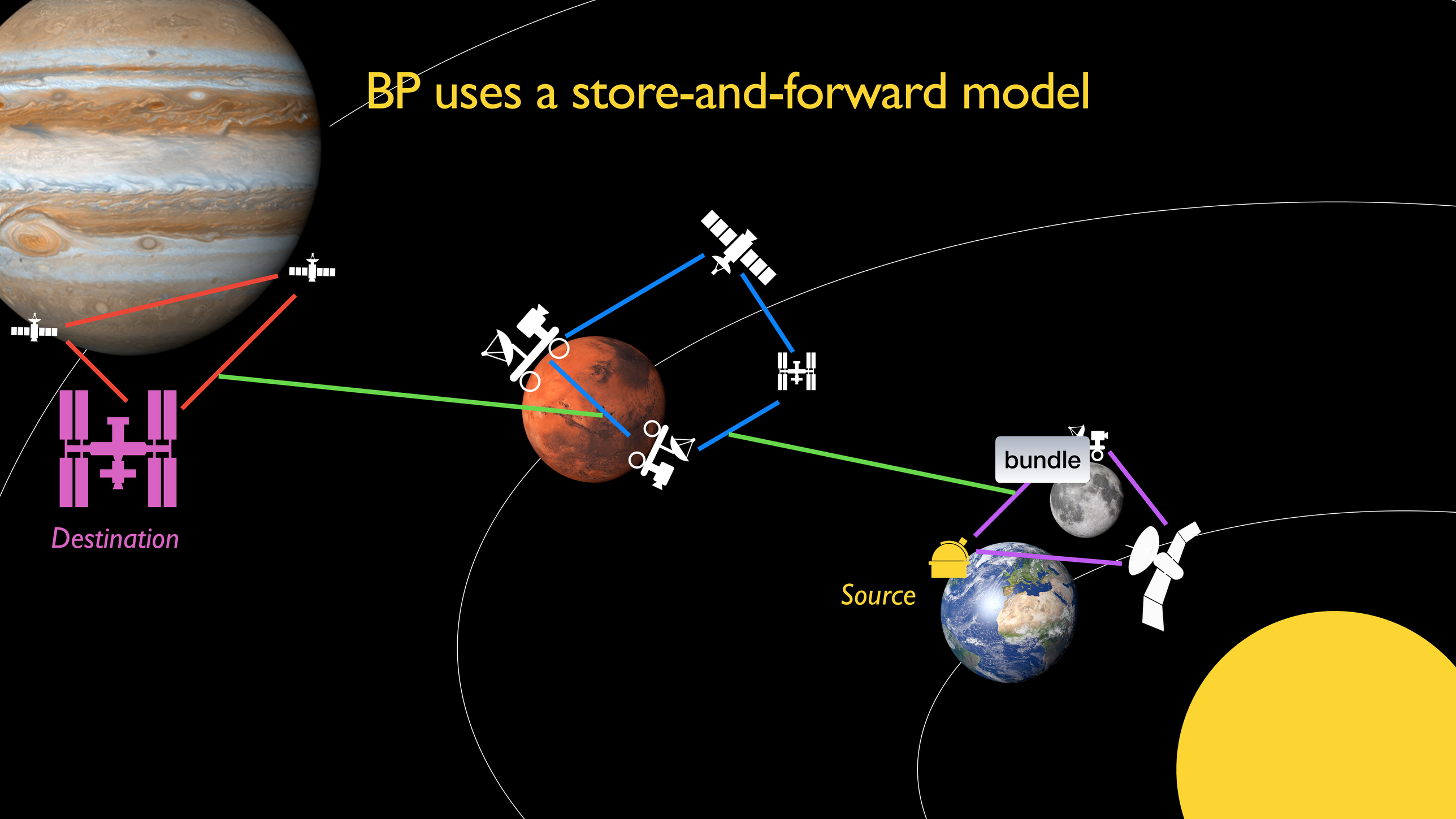
Bundle Protocol (BP)



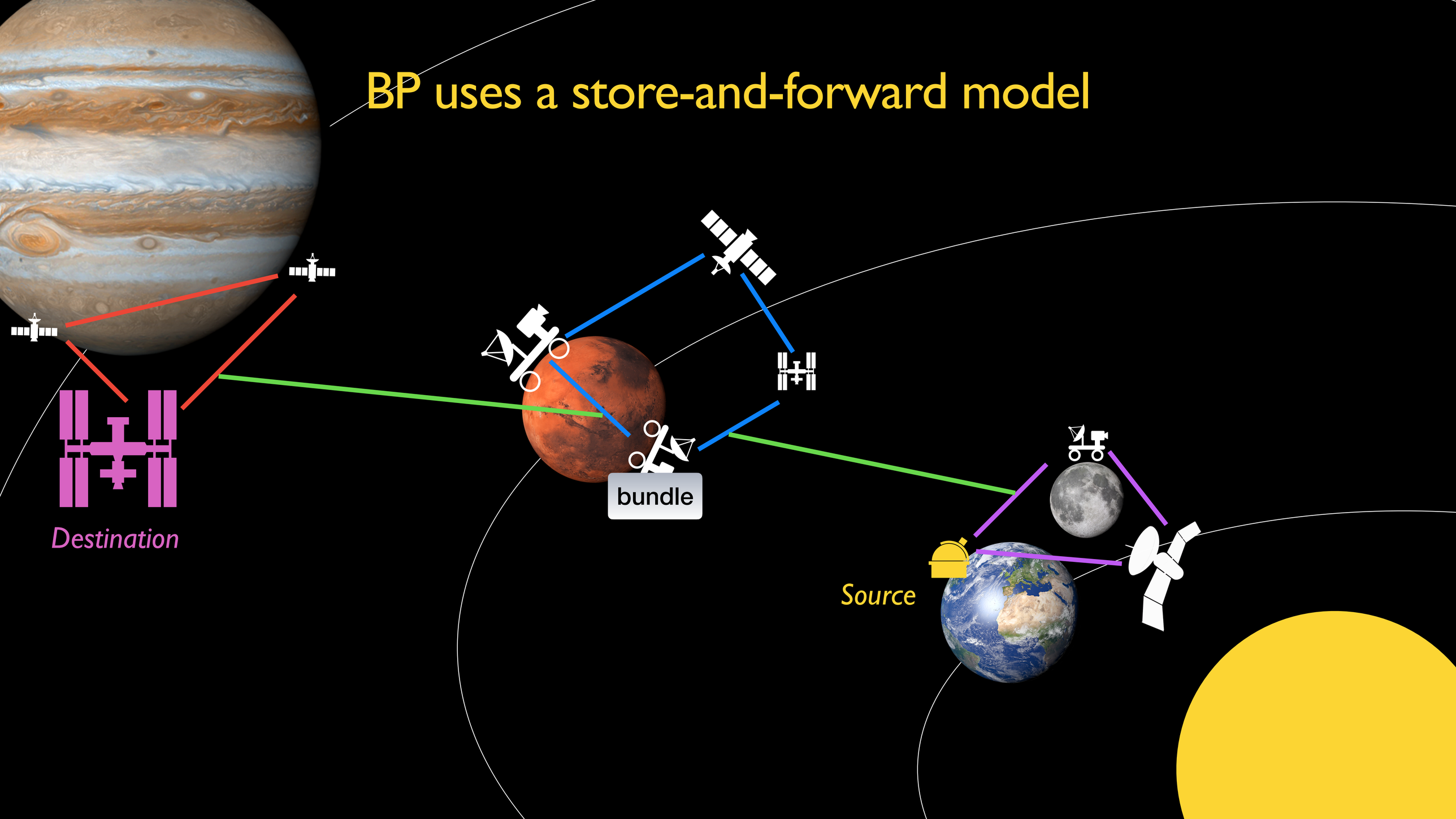
BP uses a store-and-forward model



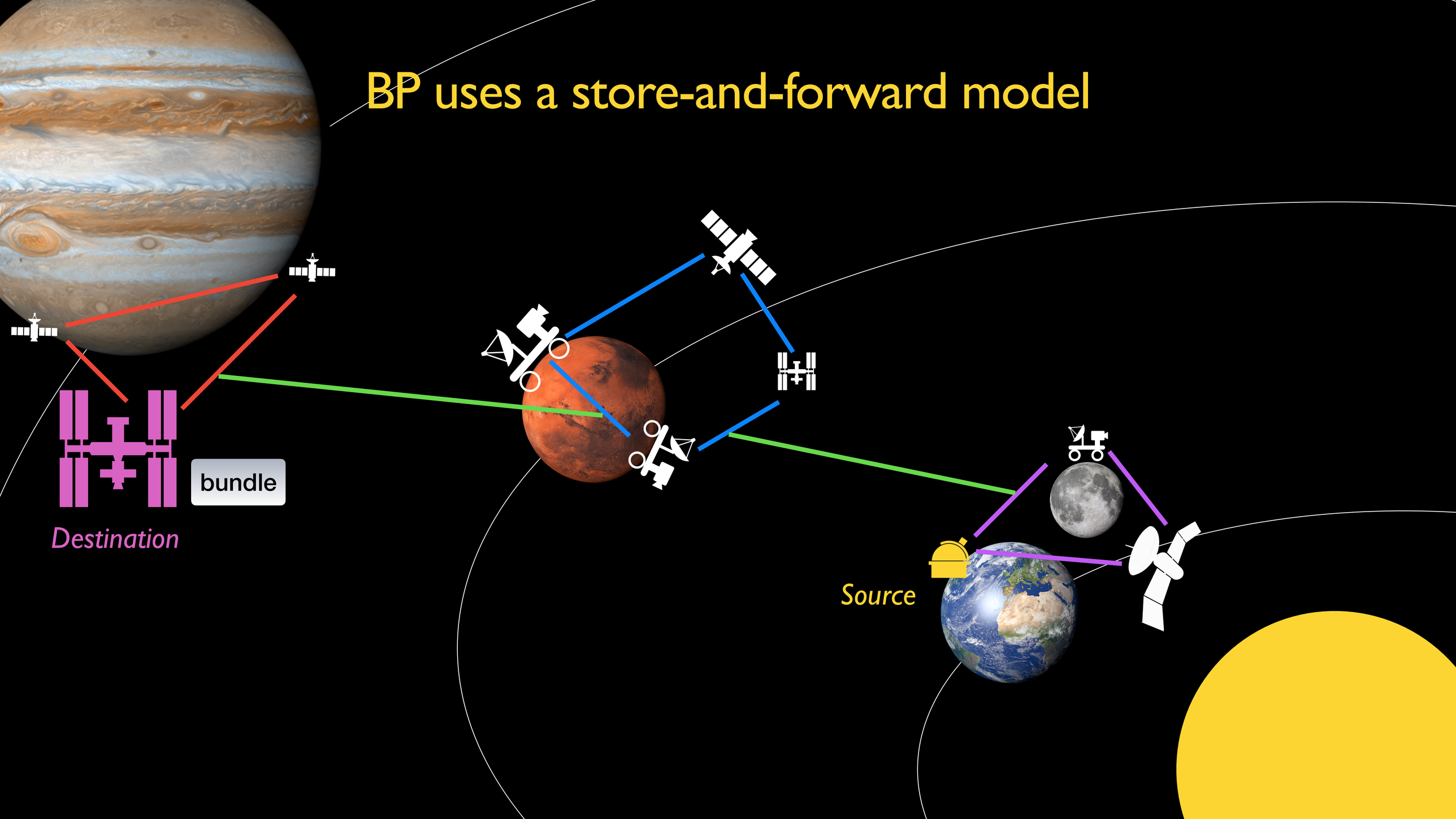
BP uses a store-and-forward model



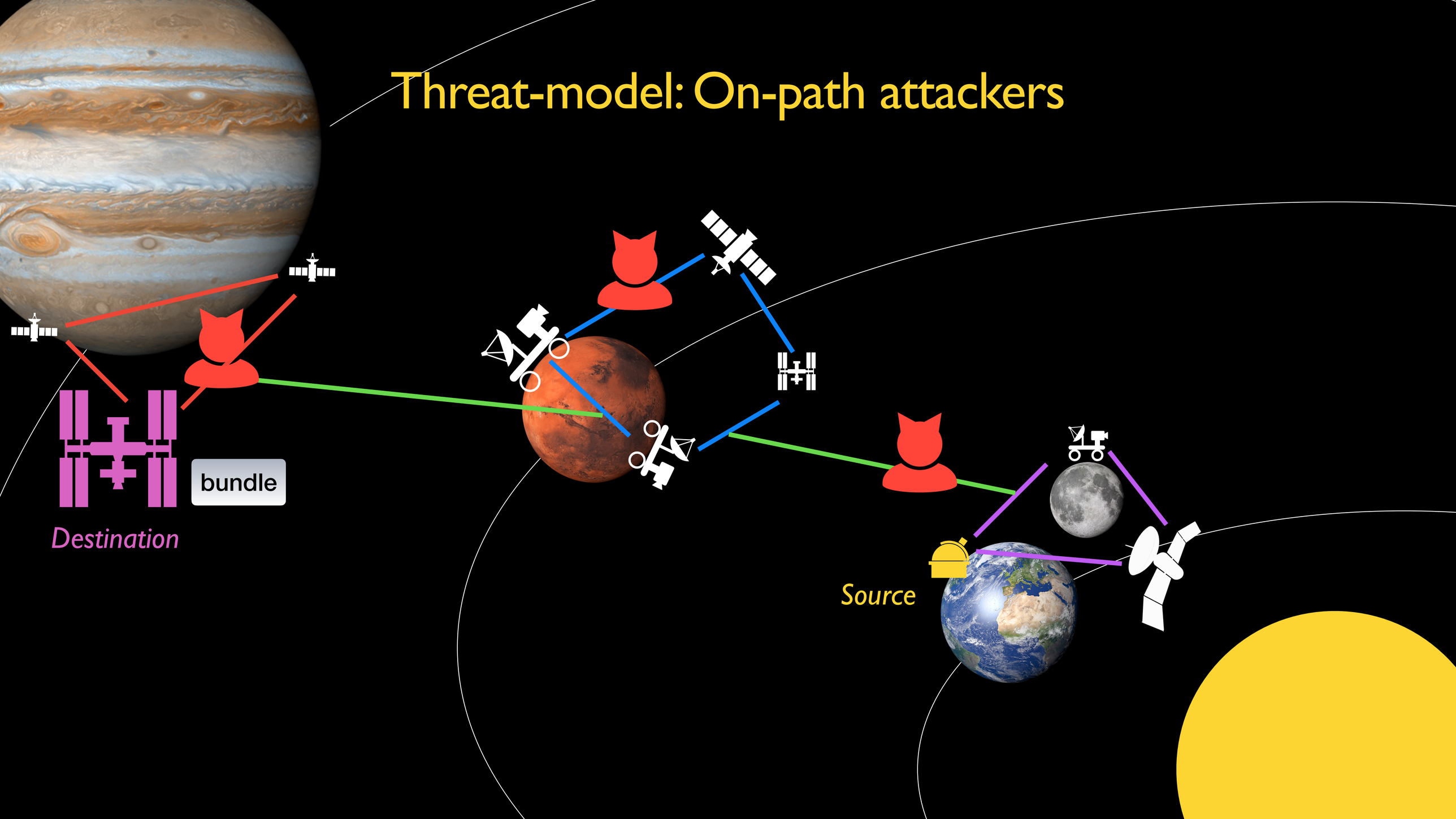
BP uses a store-and-forward model



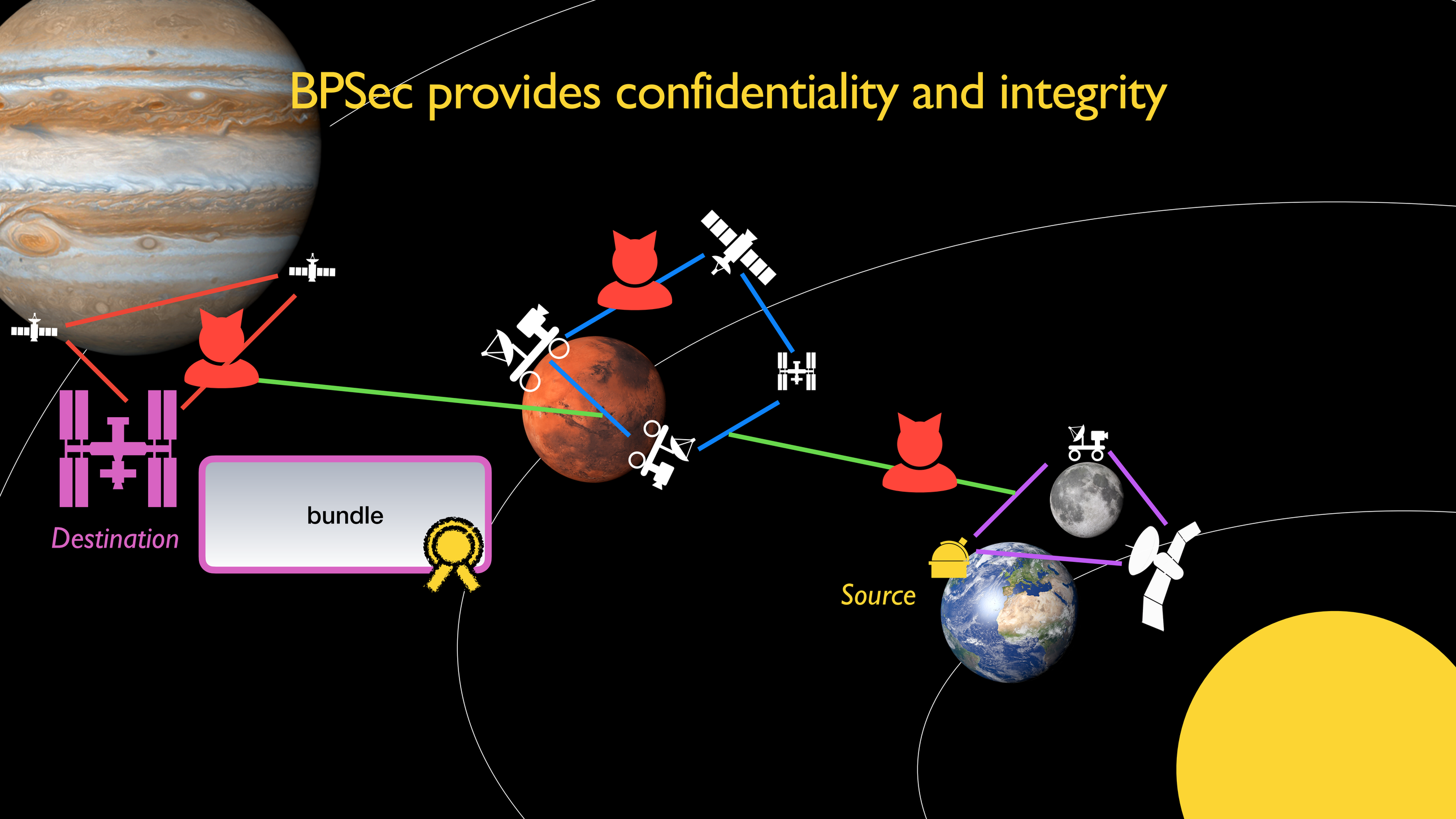
BP uses a store-and-forward model



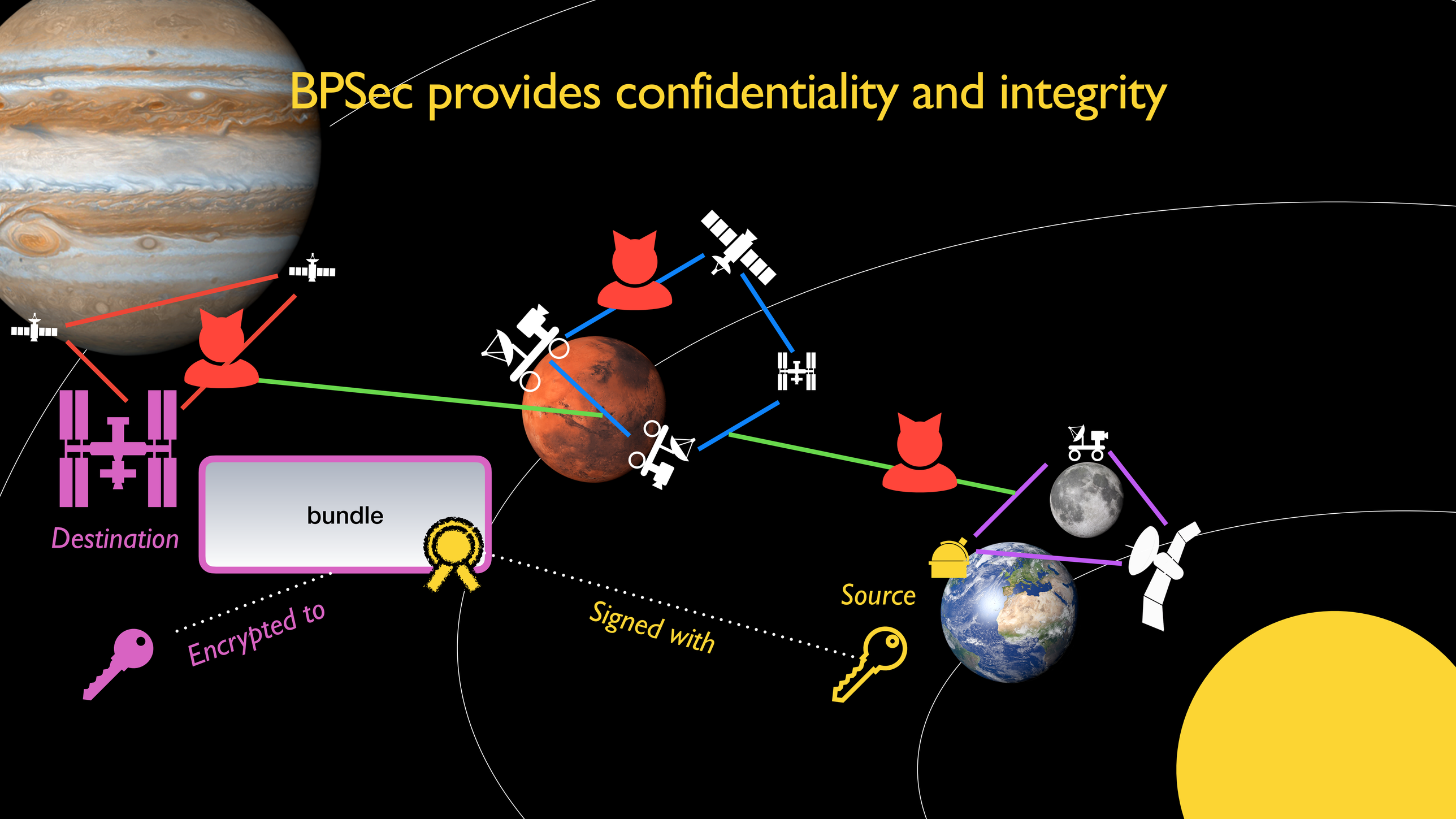
Threat-model: On-path attackers



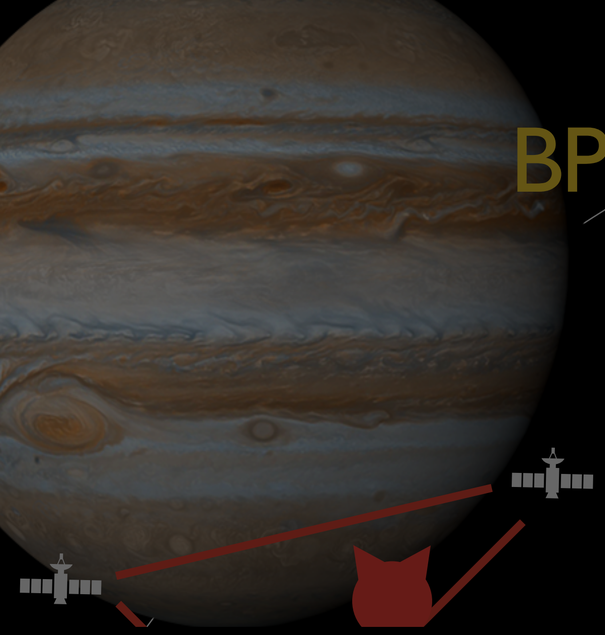
BPSec provides confidentiality and integrity

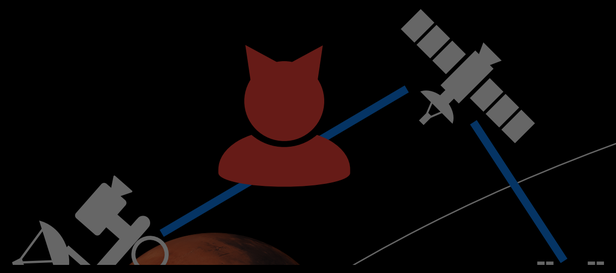


BPSec provides confidentiality and integrity

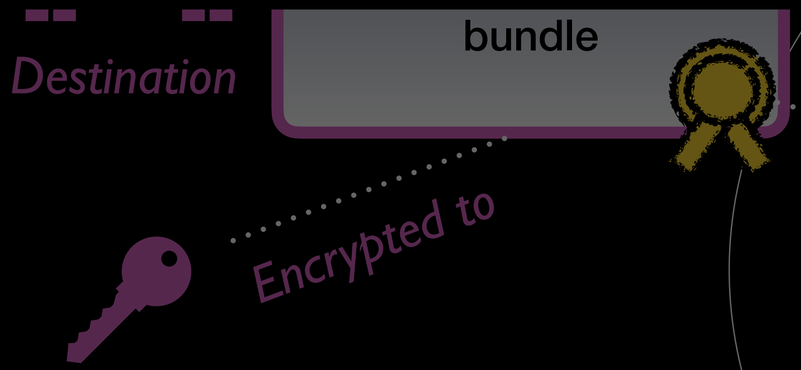


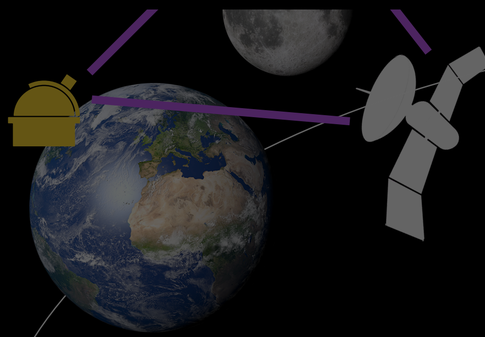
BPSec provides confidentiality and integrity





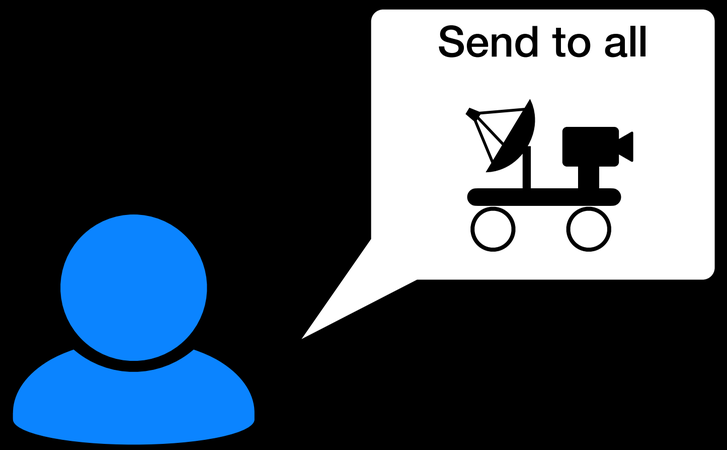
Is BPSec sufficient?



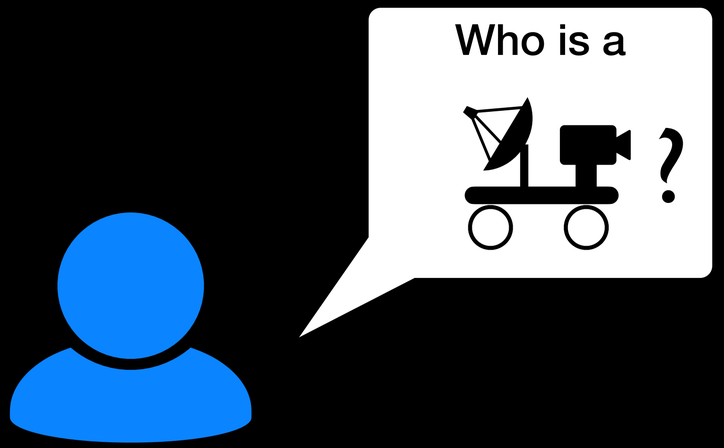


Group Communication

Group Communication



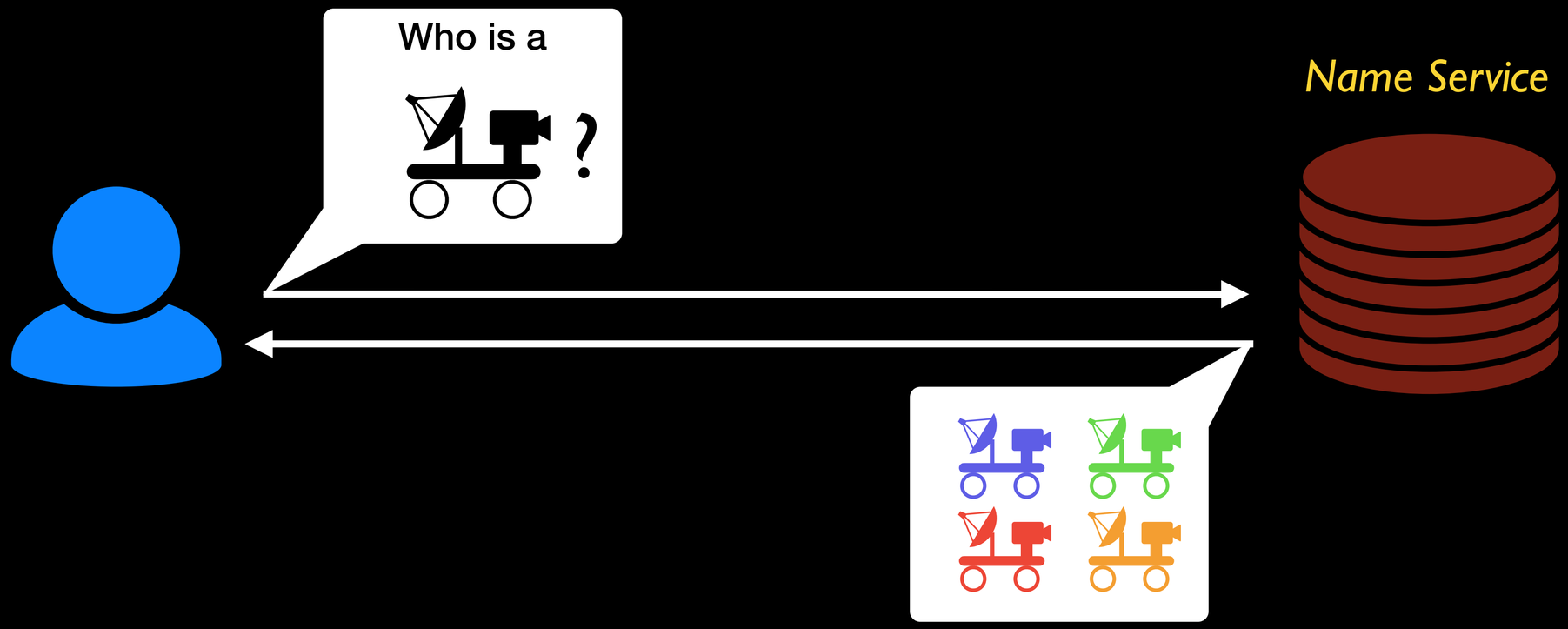
Group Communication



Group Communication

Group Communication

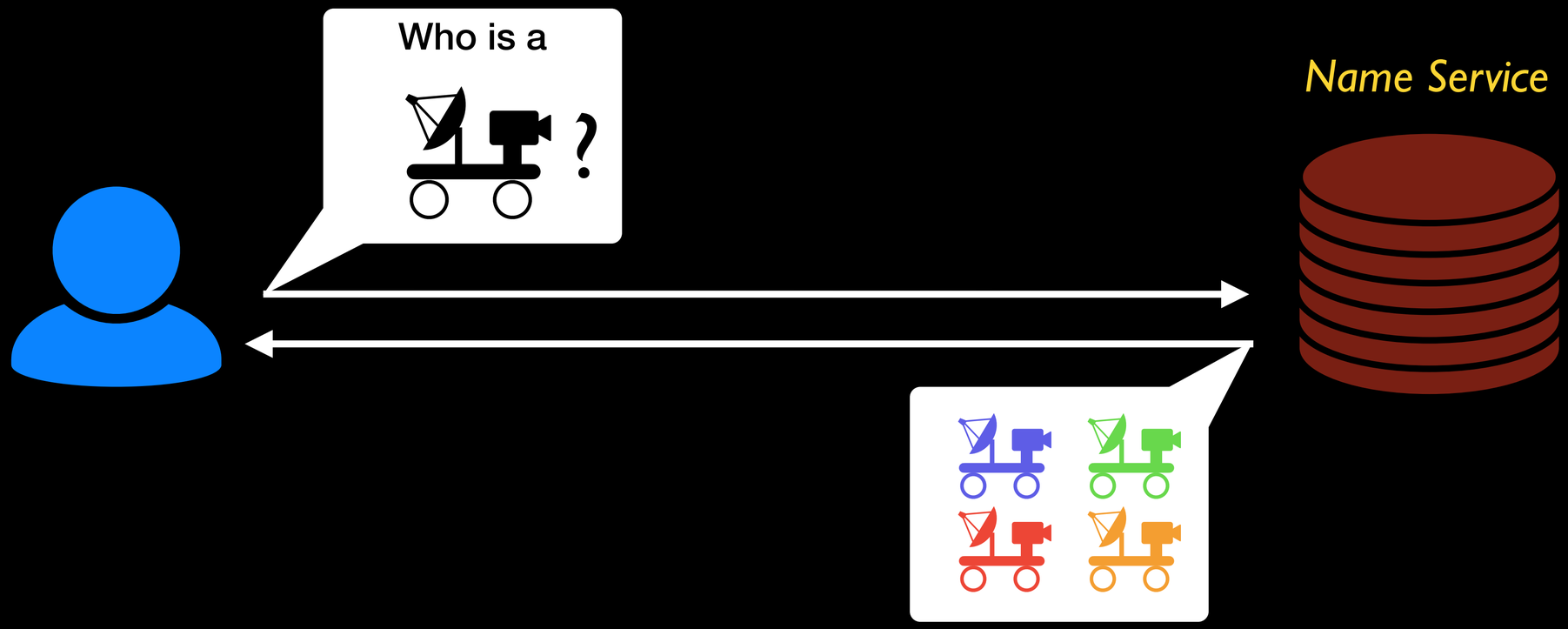
Group Communication



Group Communication

Requirements

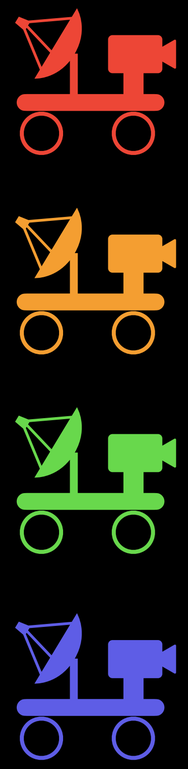
Minimize round-trips



Group Communication

Requirements

Minimize round-trips

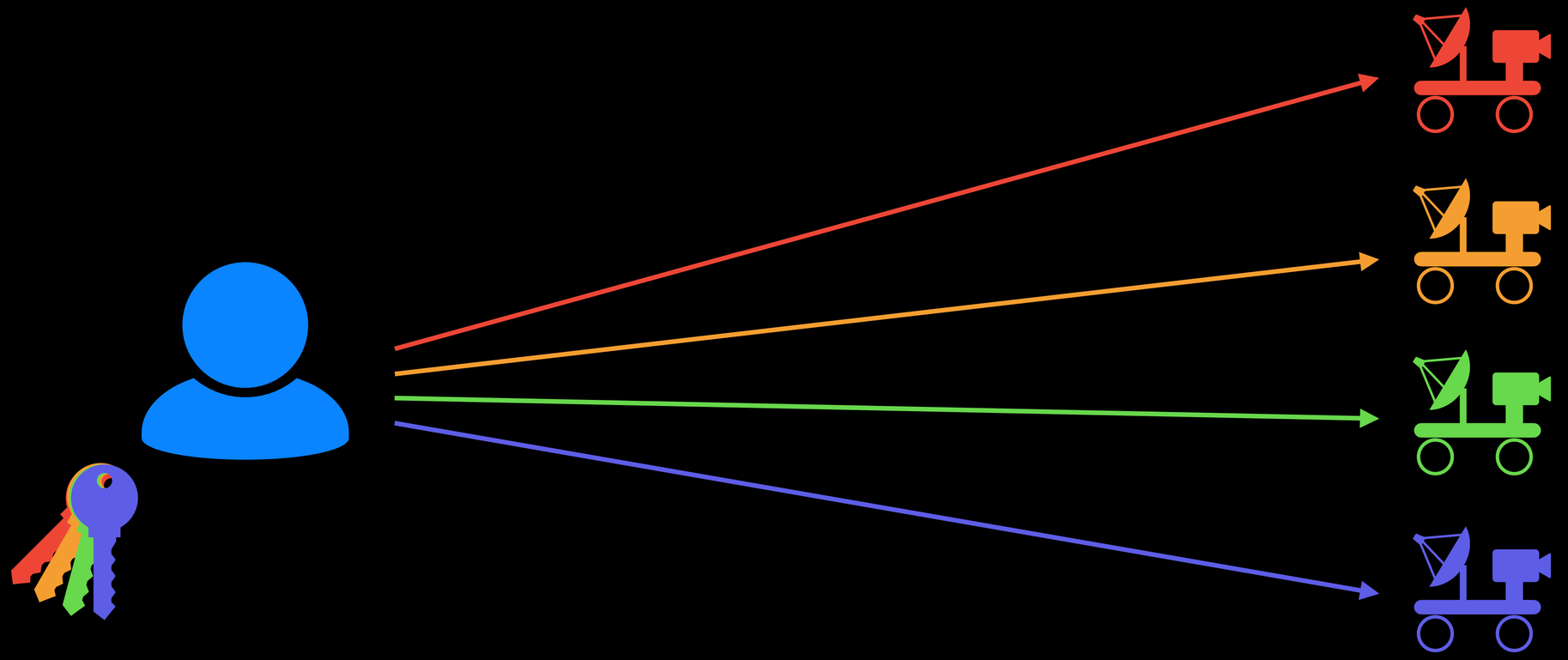


Group Communication

Requirements

Minimize round-trips

Minimize bandwidth

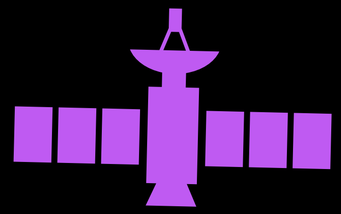


In-Network Processing

Requirements

Minimize round-trips

Minimize bandwidth



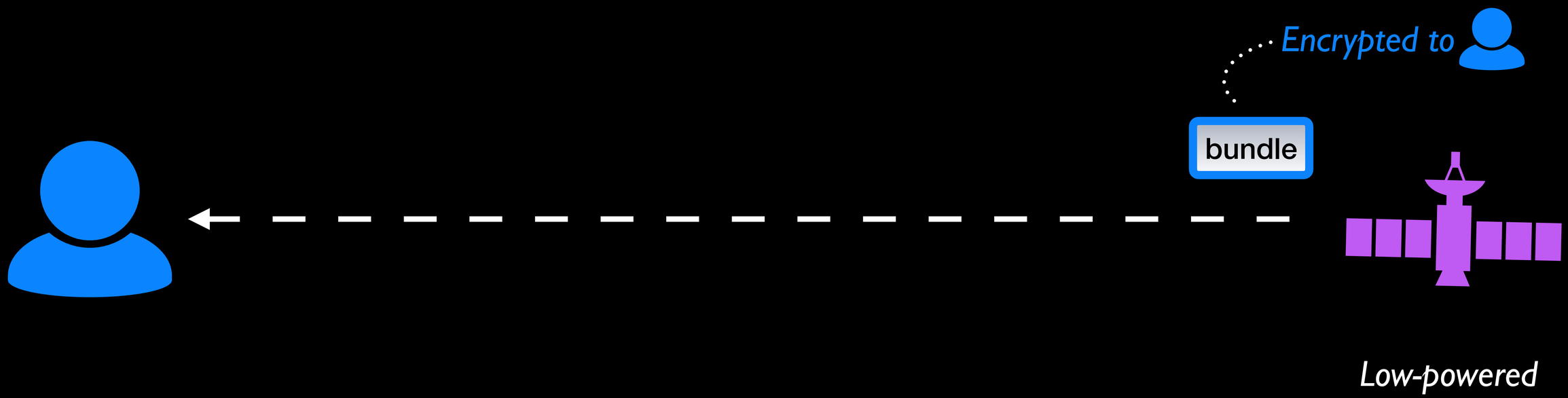
Low-powered

In-Network Processing

Requirements

Minimize round-trips

Minimize bandwidth

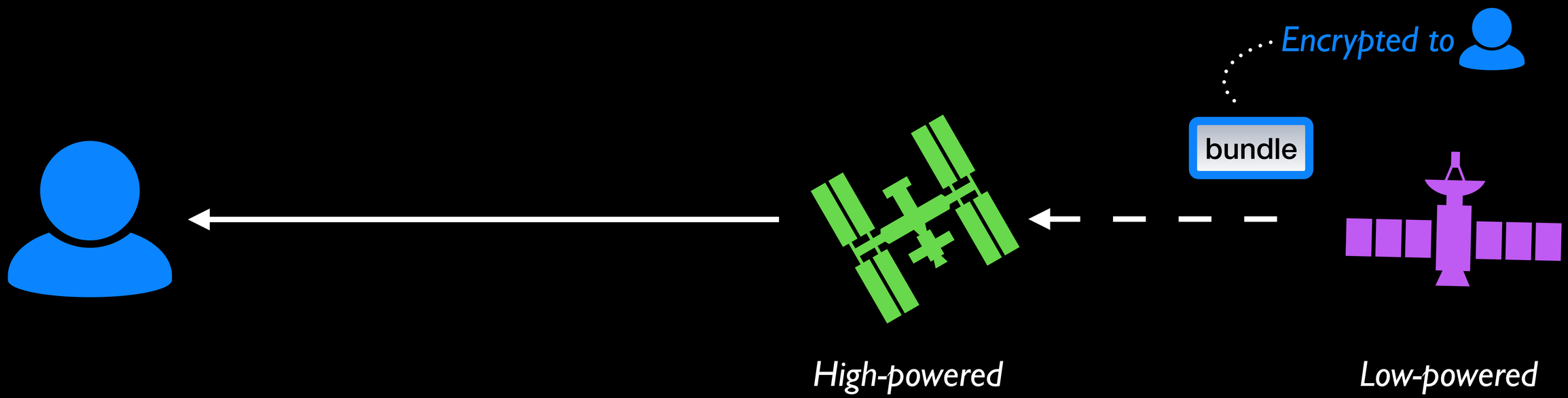


In-Network Processing

Requirements

Minimize round-trips

Minimize bandwidth

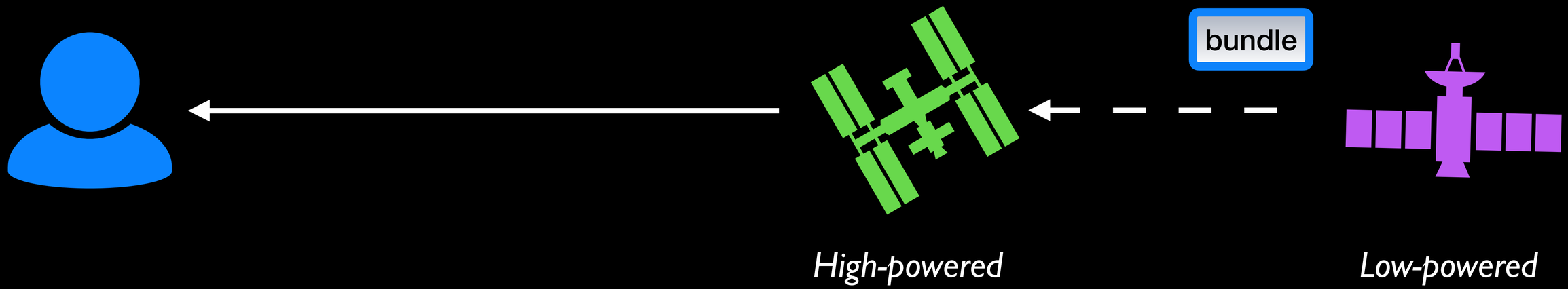


In-Network Processing

Requirements

Minimize round-trips

Minimize bandwidth

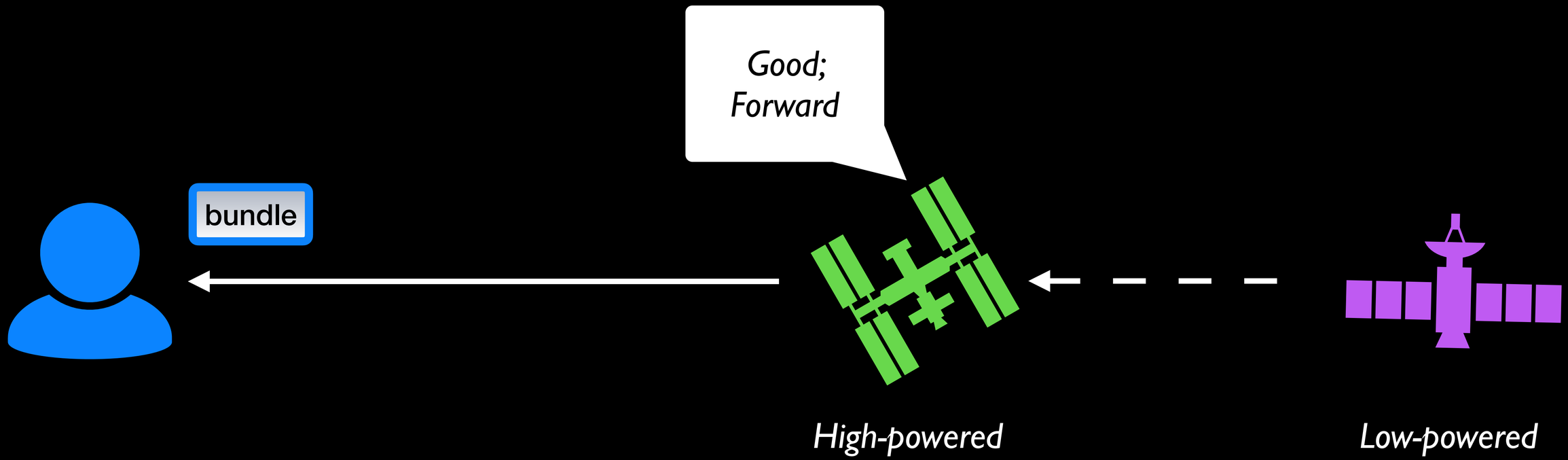


In-Network Processing

Requirements

Minimize round-trips

Minimize bandwidth

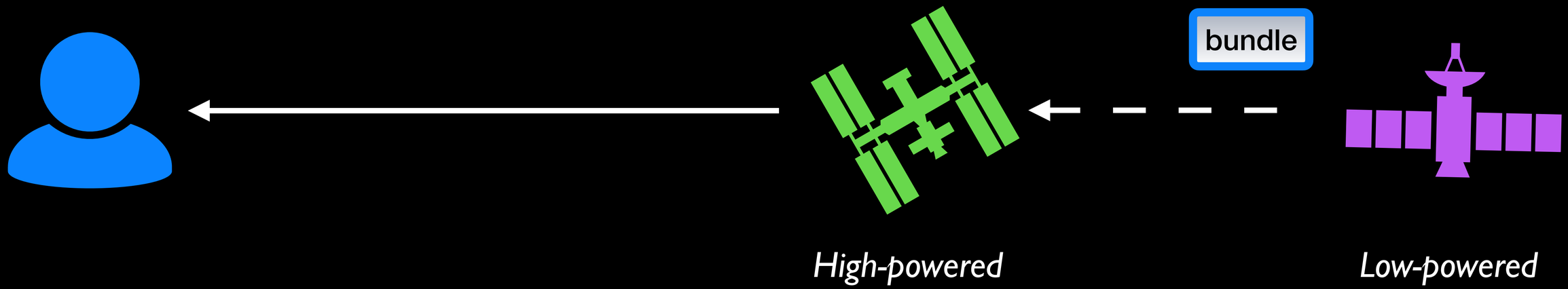


In-Network Processing

Requirements

Minimize round-trips

Minimize bandwidth

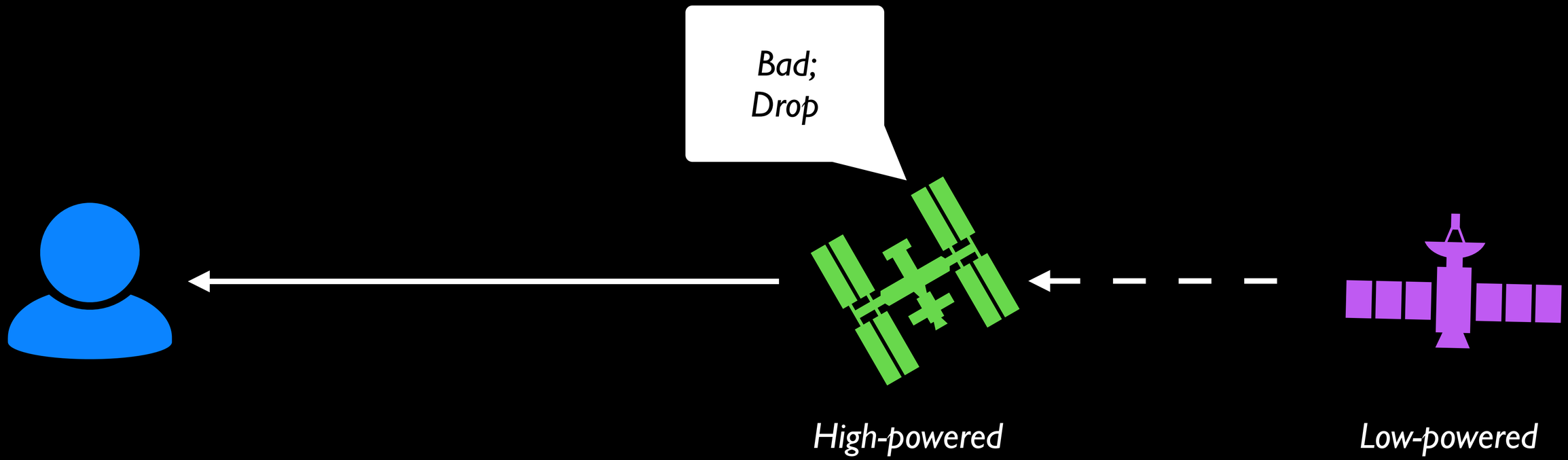


In-Network Processing

Requirements

Minimize round-trips

Minimize bandwidth



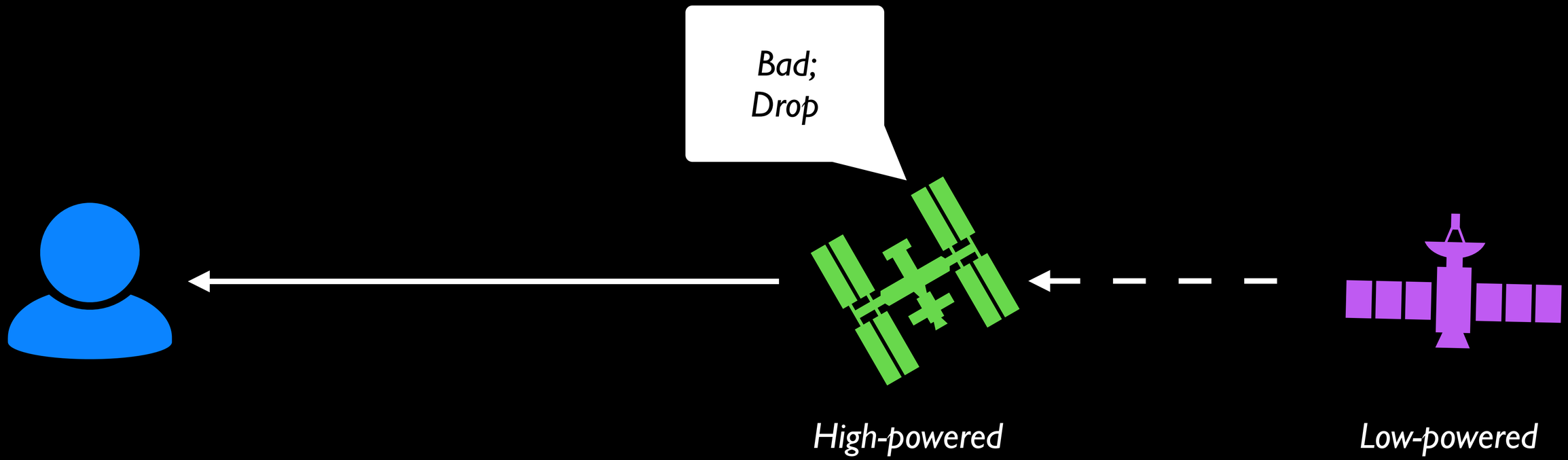
In-Network Processing

Requirements

Minimize round-trips

Minimize bandwidth

Securely delegate functions to the network



Anonymity

Requirements

Minimize round-trips

Minimize bandwidth

Securely delegate functions to the network

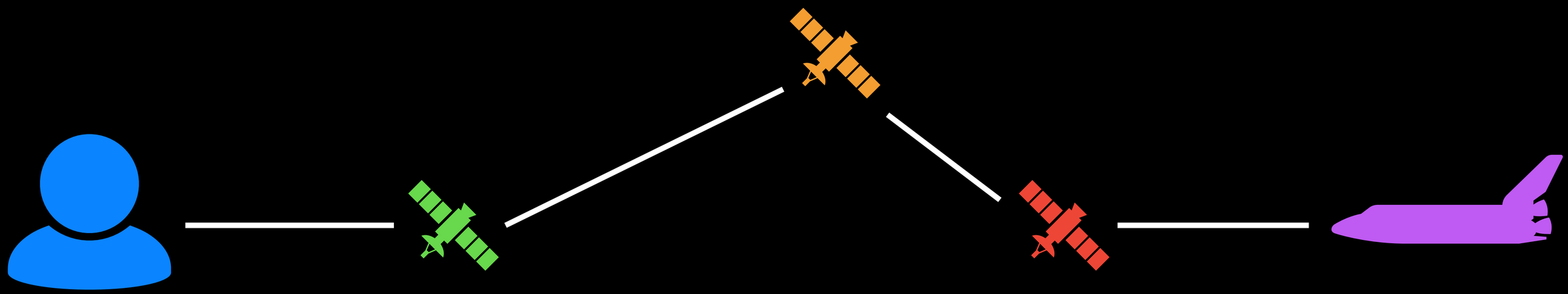
Anonymity

Requirements

Minimize round-trips

Minimize bandwidth

Securely delegate functions to the network



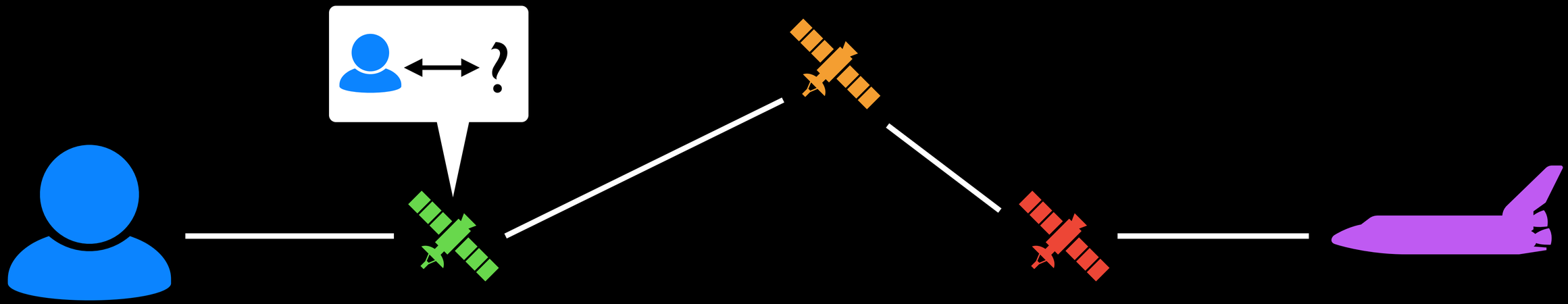
Anonymity

Requirements

Minimize round-trips

Minimize bandwidth

Securely delegate functions to the network



Anonymity

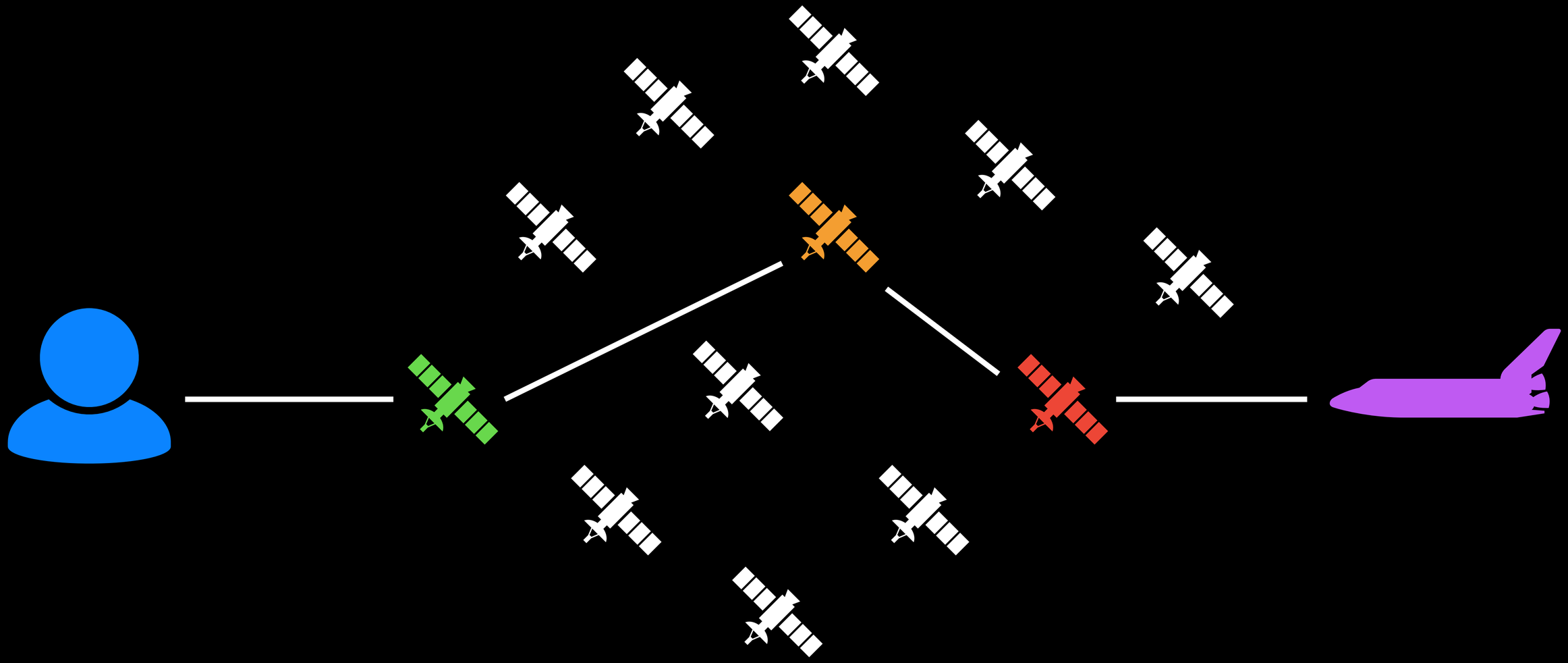
Requirements

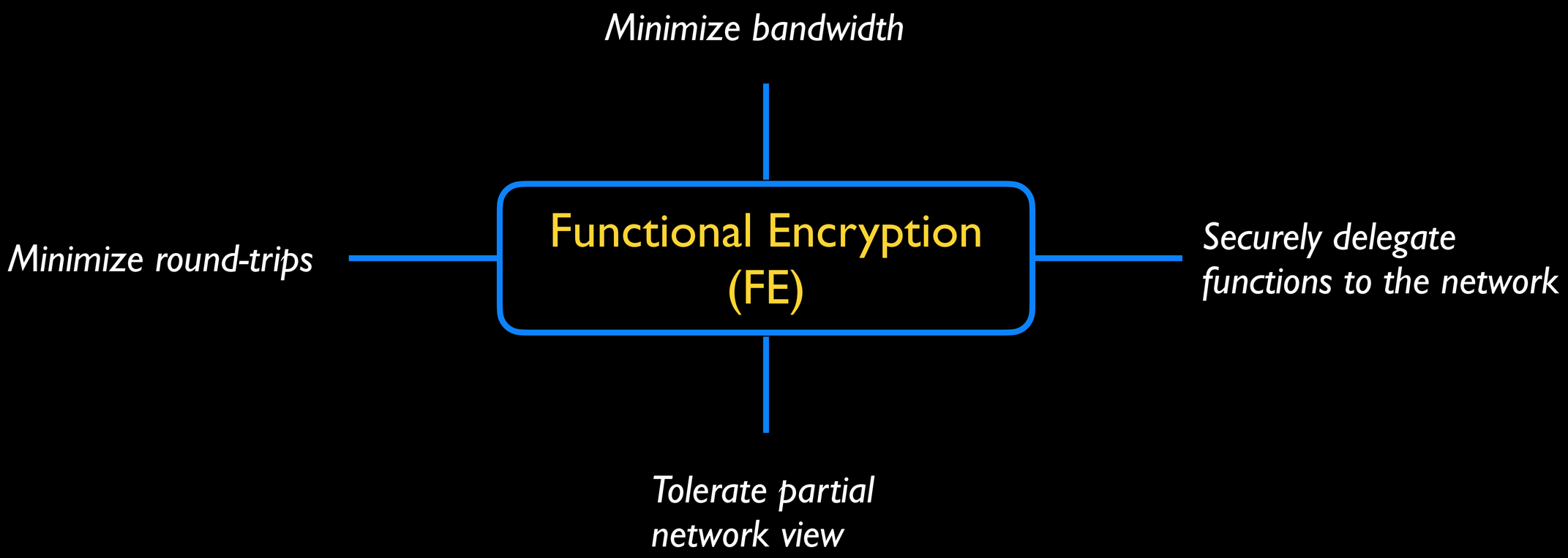
Minimize round-trips

Minimize bandwidth

Securely delegate functions to the network

Tolerate partial network view




Minimize bandwidth
Minimize round-trips
Functional Encryption (FE)
Securely delegate functions to the network
Tolerate partial network view

Functional Encryption (FE) enables selective sharing

Alice

Functional Encryption (FE) enables selective sharing

Alice

Primary Secret Key

Public Key

Functional Encryption (FE) enables selective sharing

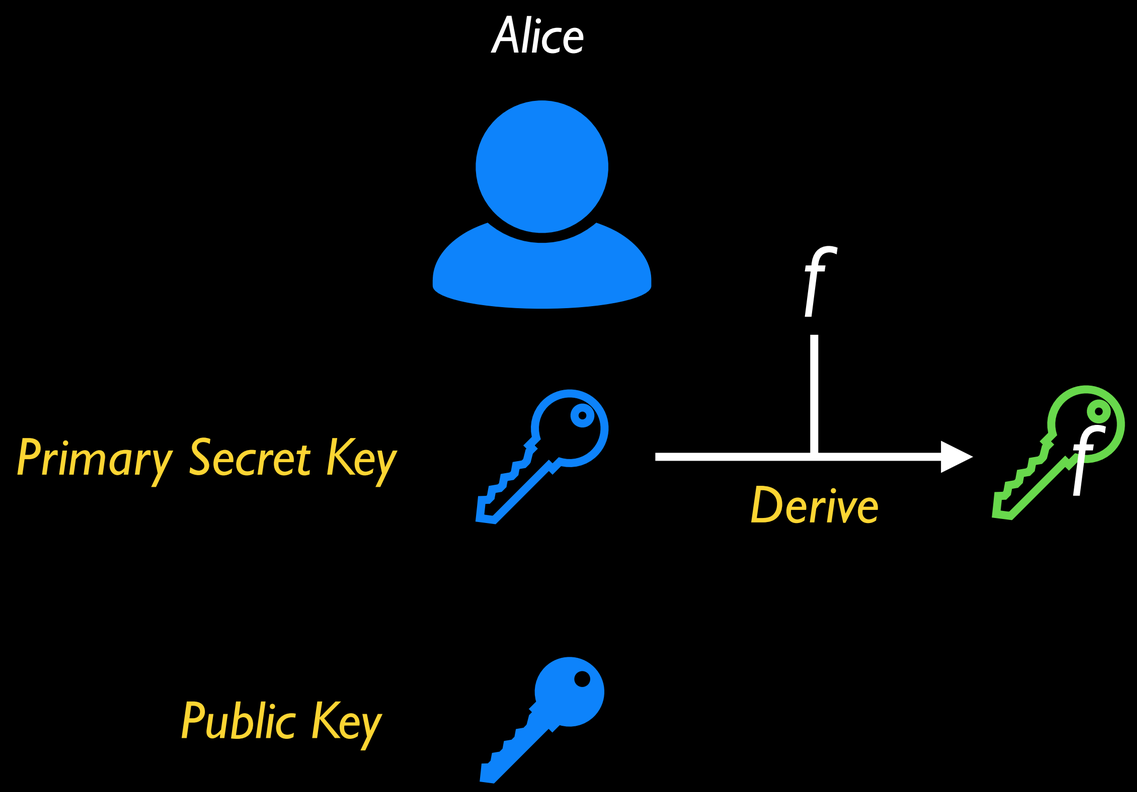
Alice

f

Primary Secret Key

Public Key

Functional Encryption (FE) enables selective sharing



Functional Encryption (FE) enables selective sharing

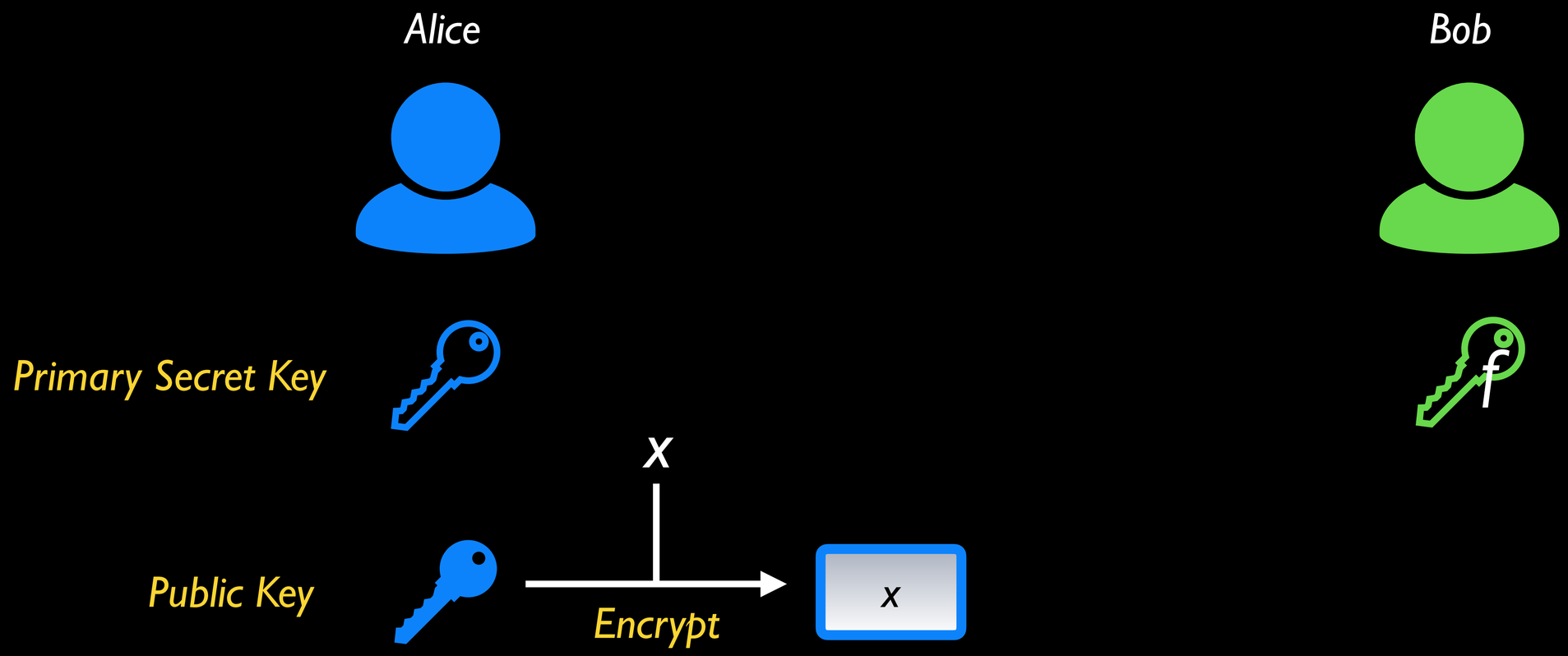
Alice

Primary Secret Key

Public Key

Bob

Functional Encryption (FE) enables selective sharing



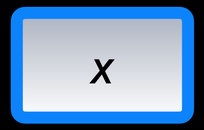
Functional Encryption (FE) enables selective sharing

Alice

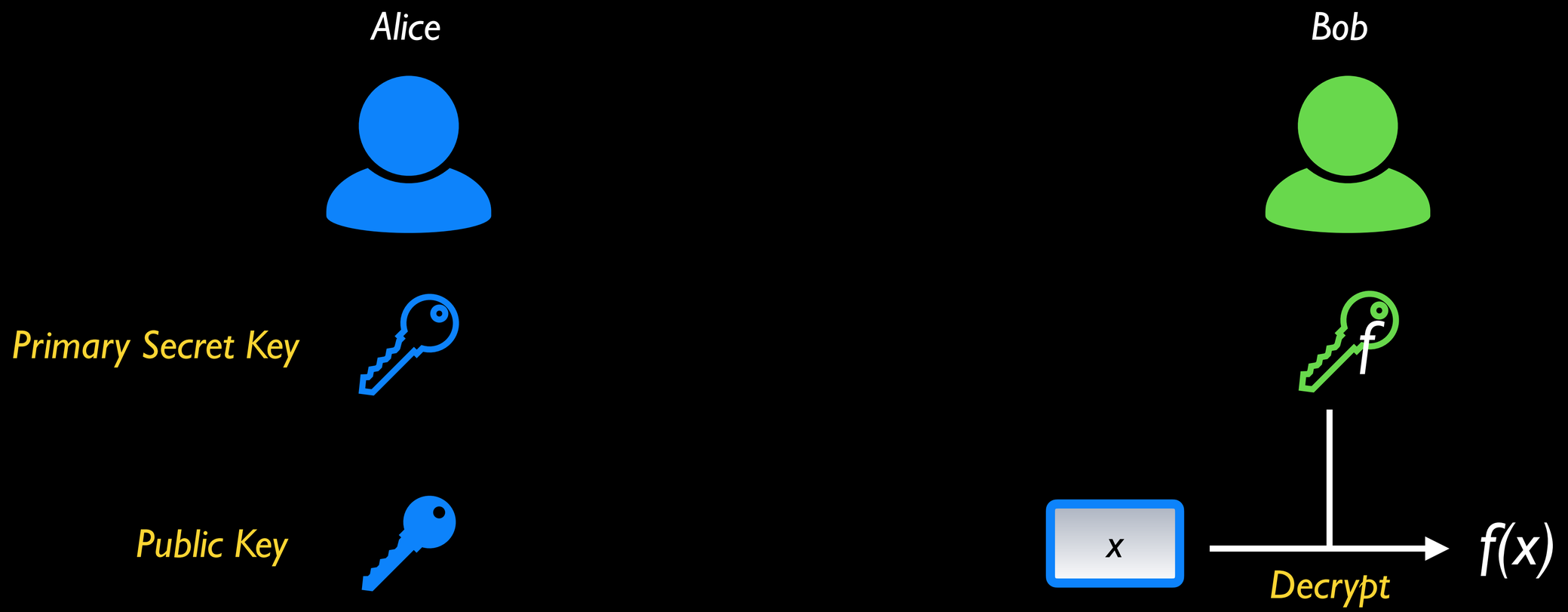
Bob

Primary Secret Key

Public Key



Functional Encryption (FE) enables selective sharing



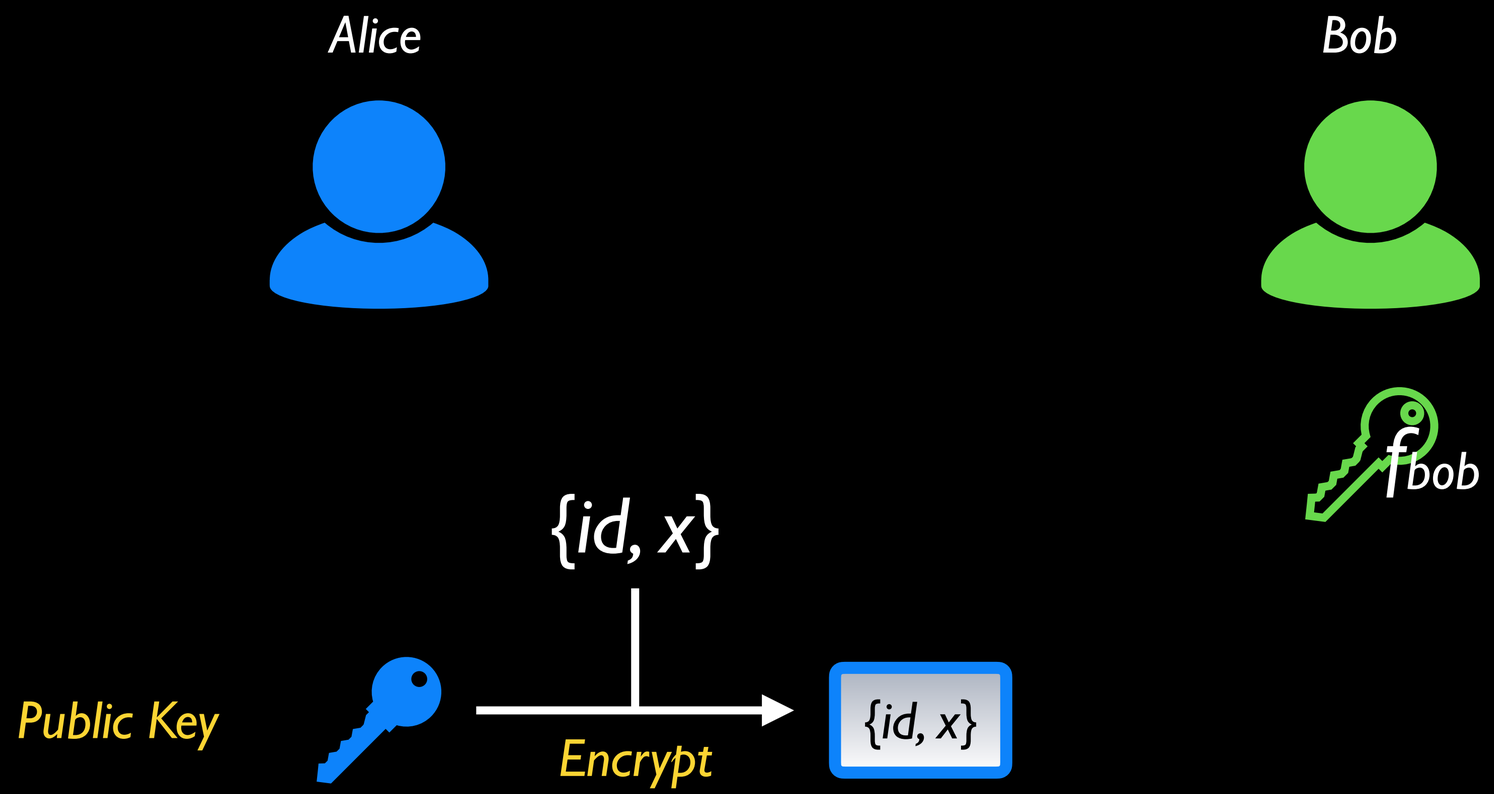
Identity-Based Encryption (IBE)
IBE ⊂ FE

Alice

Bob

Public Key

Identity-Based Encryption (IBE)
IBE ⊂ FE

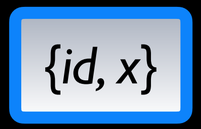


Identity-Based Encryption (IBE)
IBE ⊂ FE

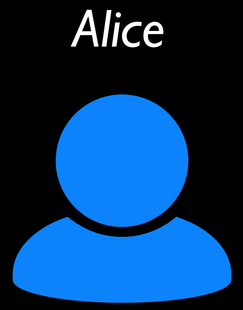
Alice

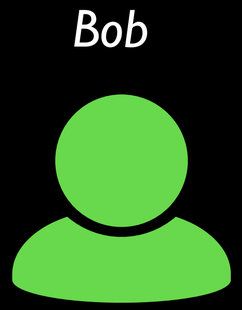
Bob

Public Key

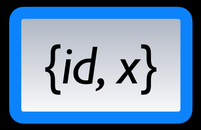


Identity-Based Encryption (IBE)
IBE ⊂ FE





Public Key

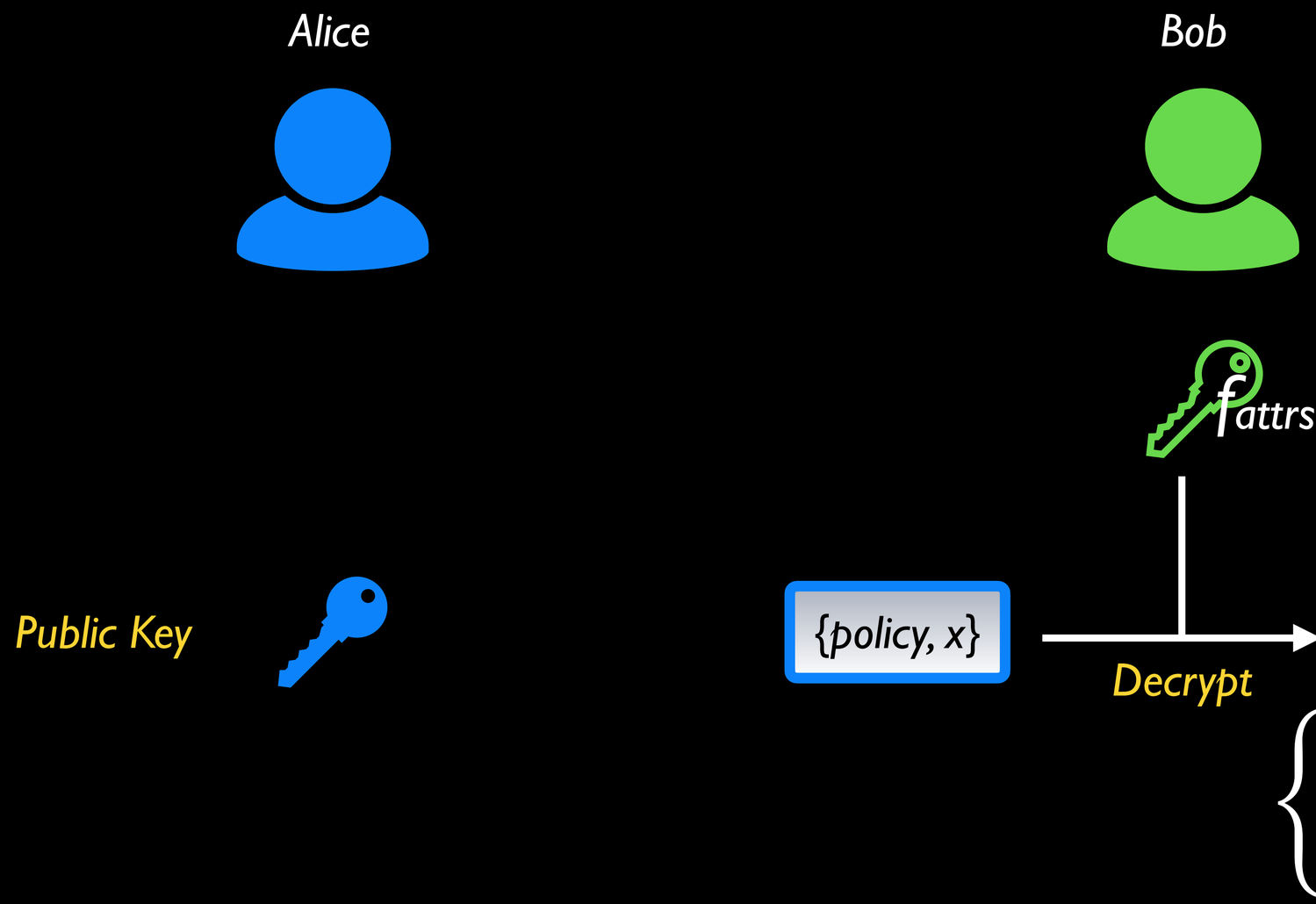


Decrypt

$f_{bob}(x)$

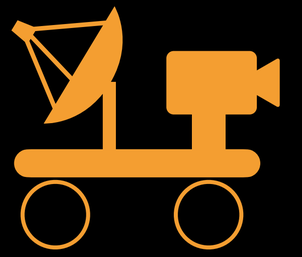
$$\begin{cases} x & \text{if } id == bob \\ \perp & \text{otherwise} \end{cases}$$

Attribute-Based Encryption (ABE)
ABE ⊂ FE



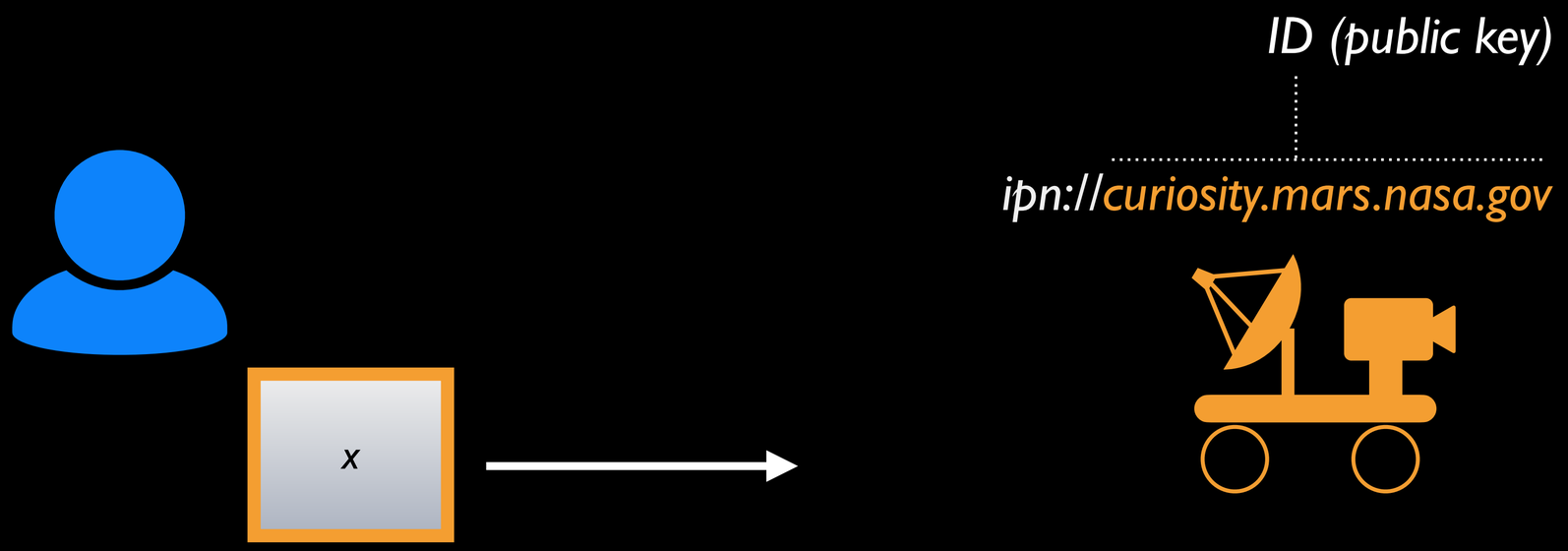
Endpoint Identifiers

ipn://curiosity.mars.nasa.gov

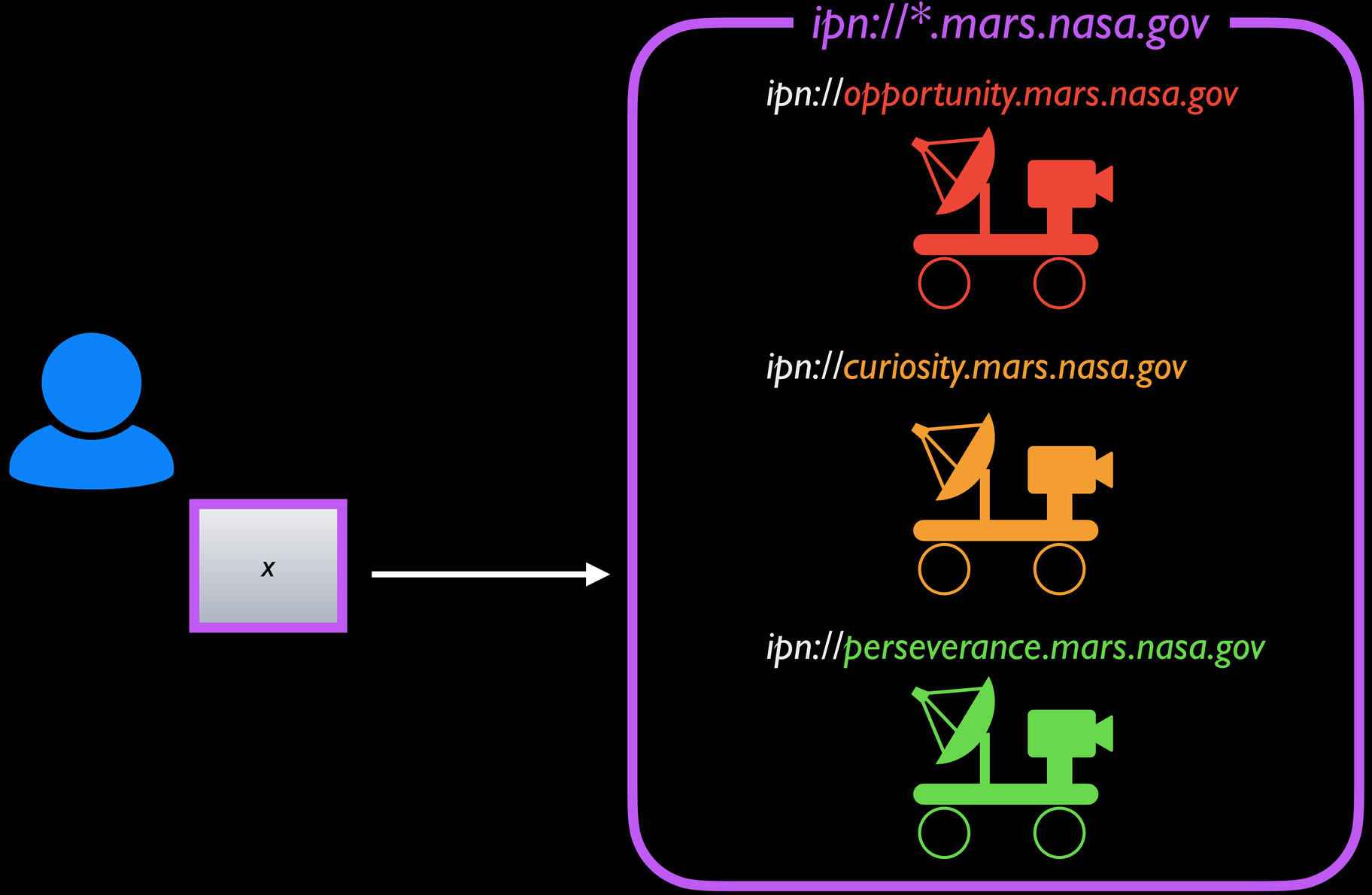


Endpoint Identifiers

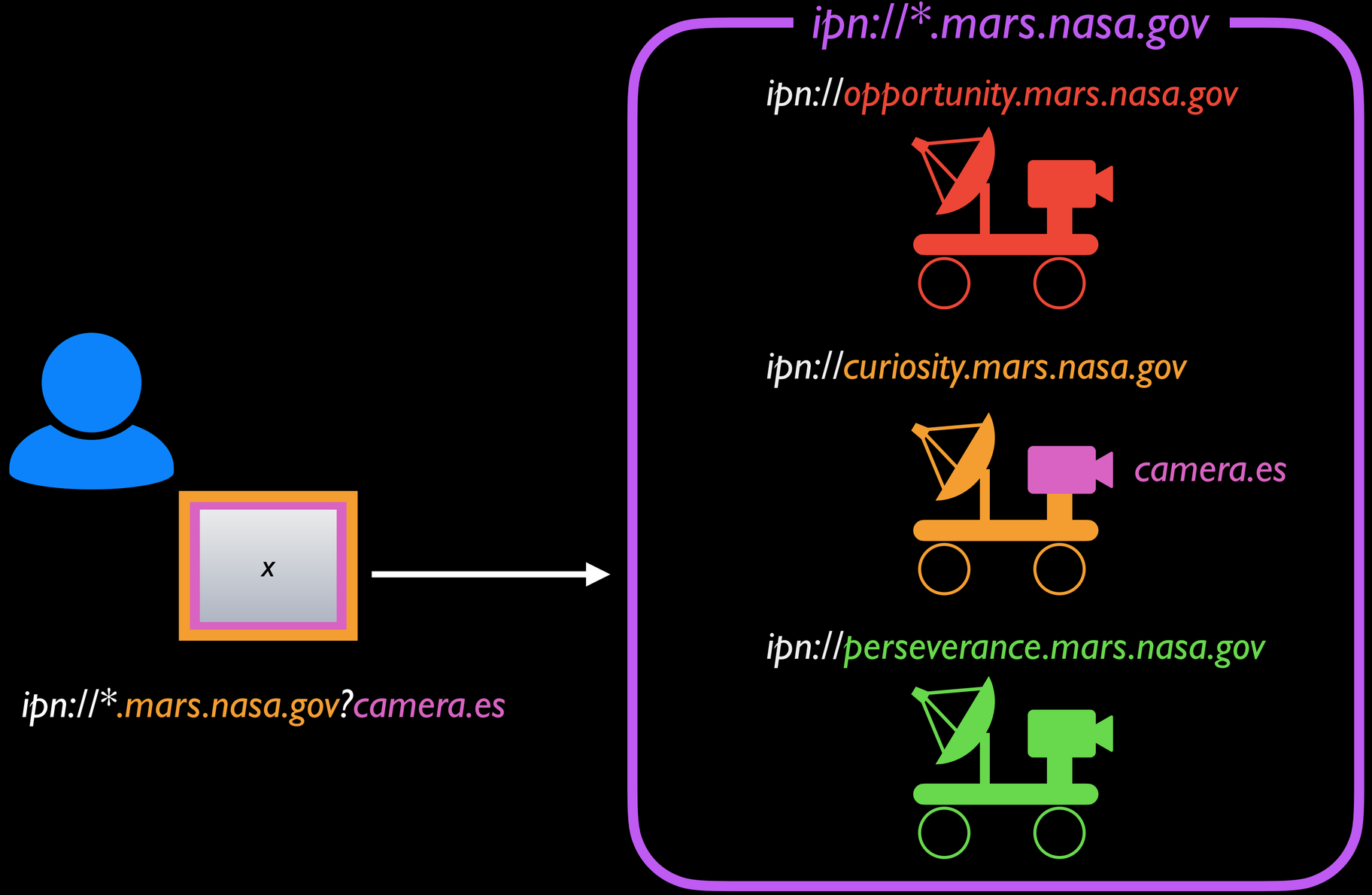
Endpoint Identifiers



Endpoint Identifiers

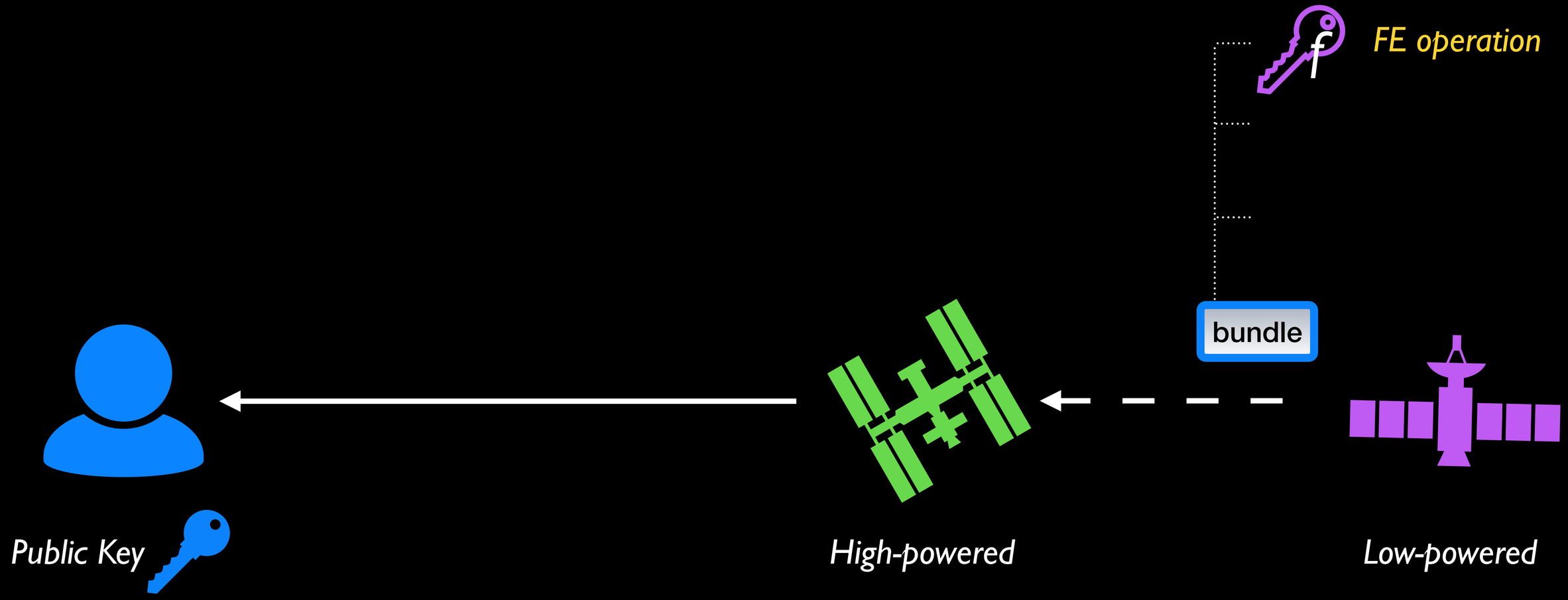


Endpoint Identifiers

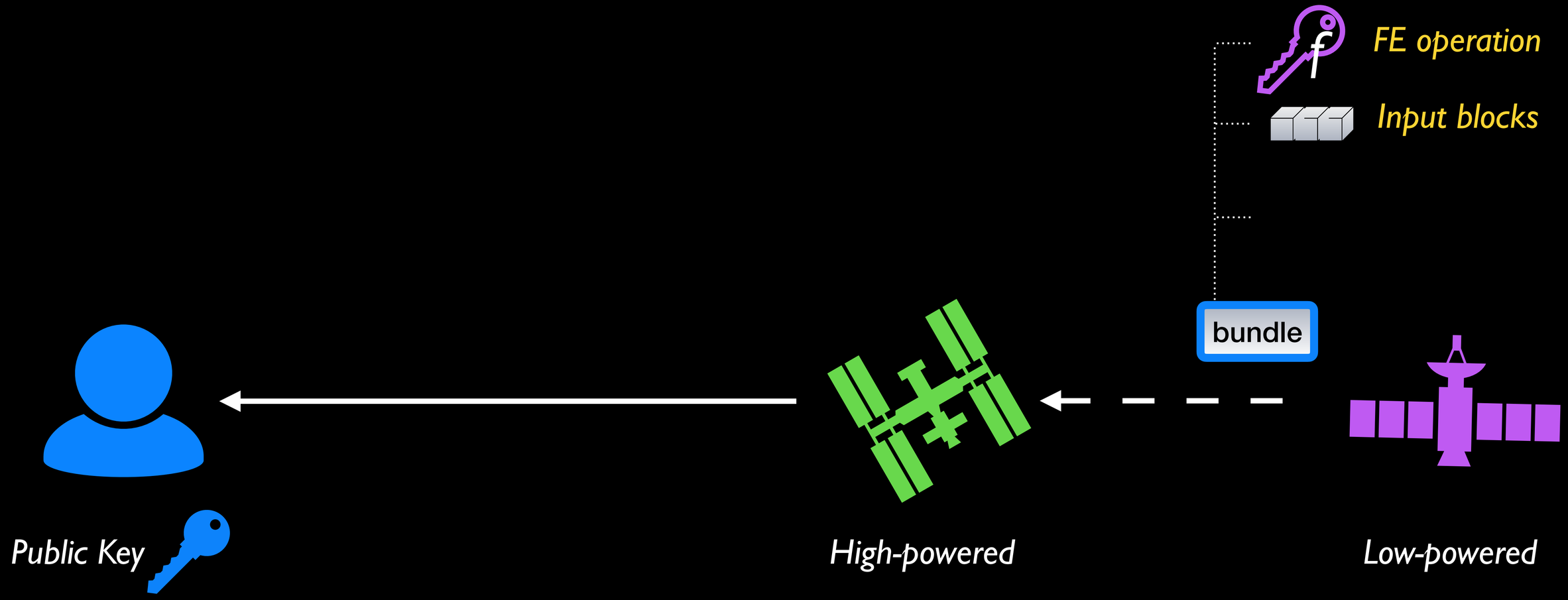


Bundle-Specified FE Programs

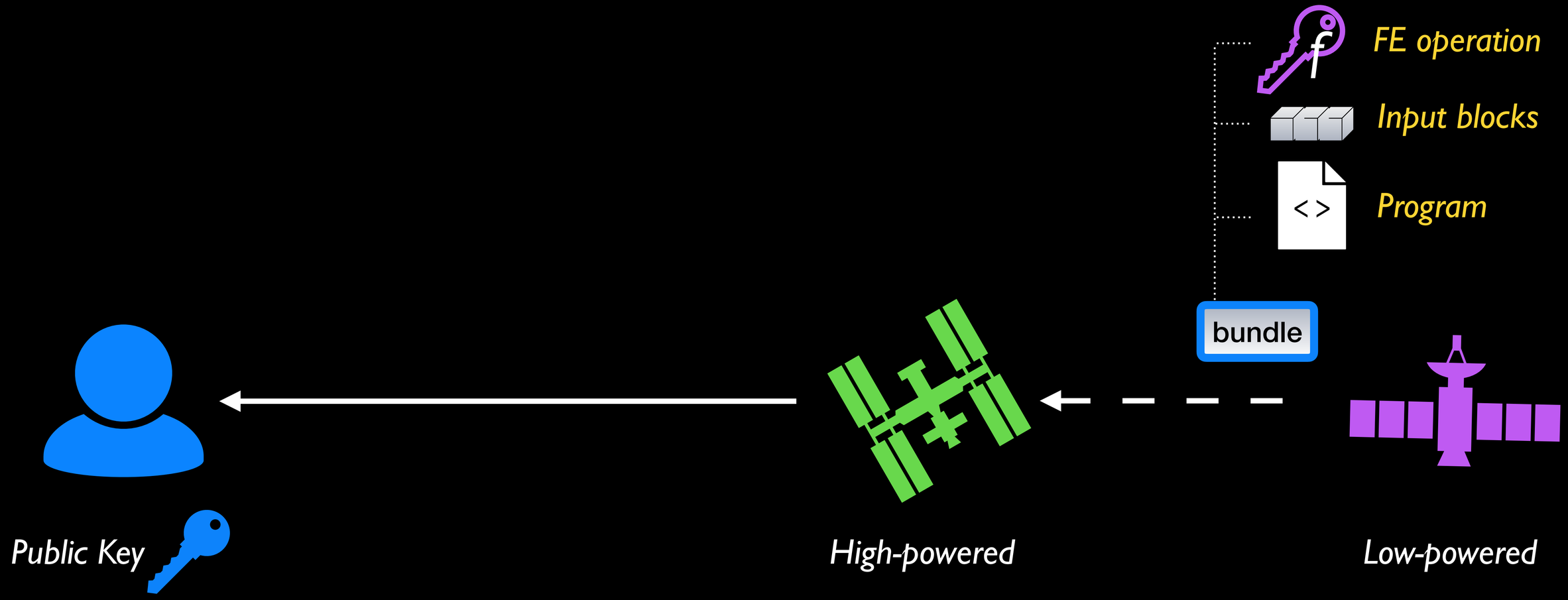
Bundle-Specified FE Programs



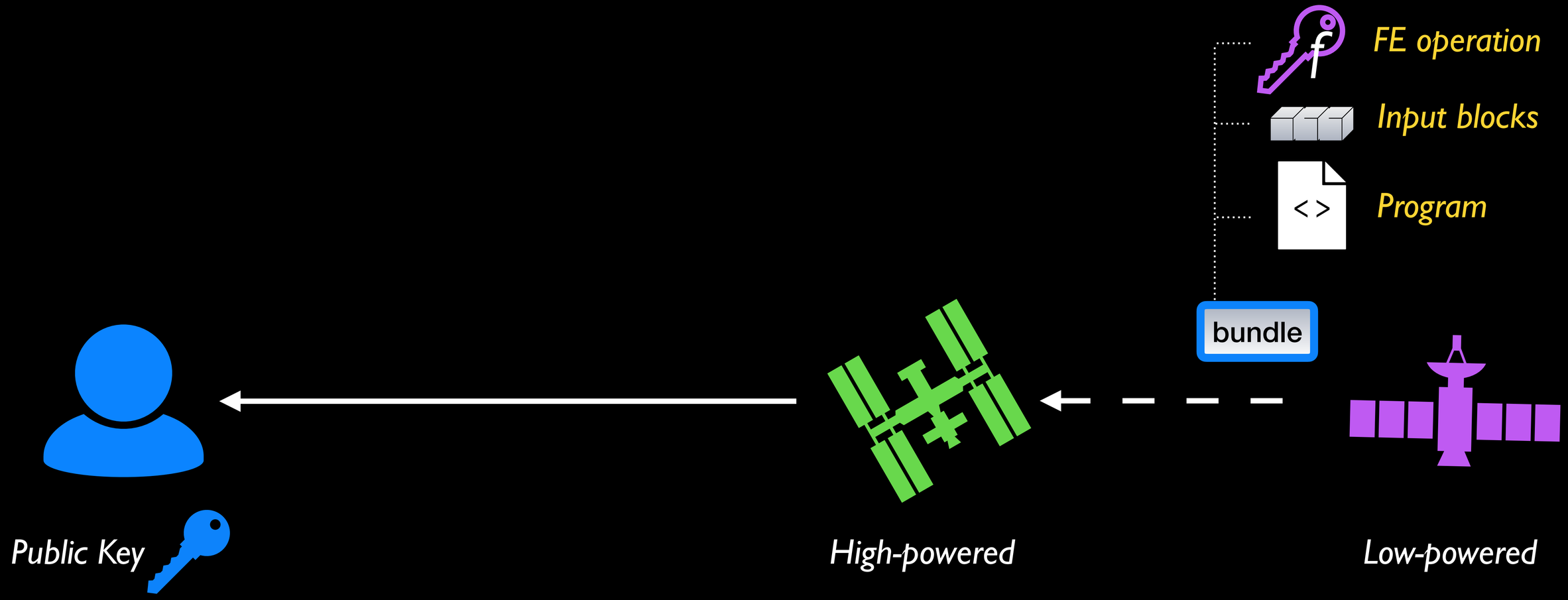
Bundle-Specified FE Programs



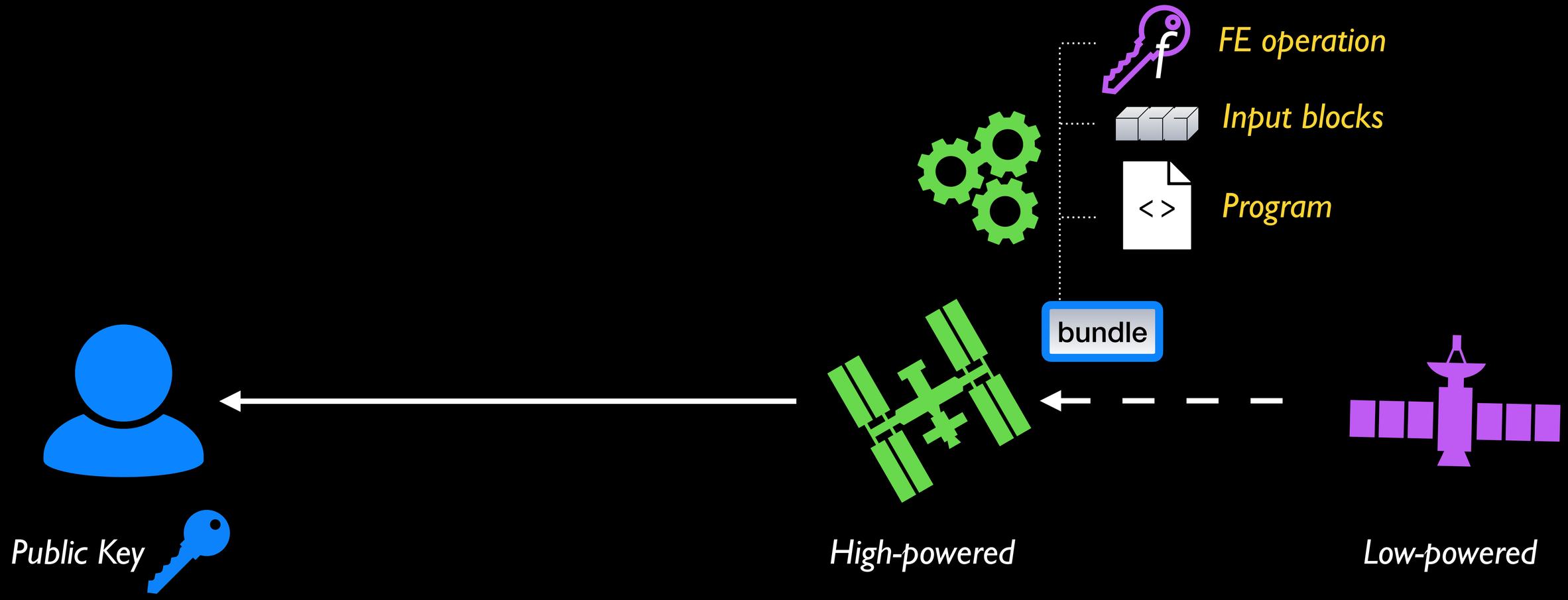
Bundle-Specified FE Programs



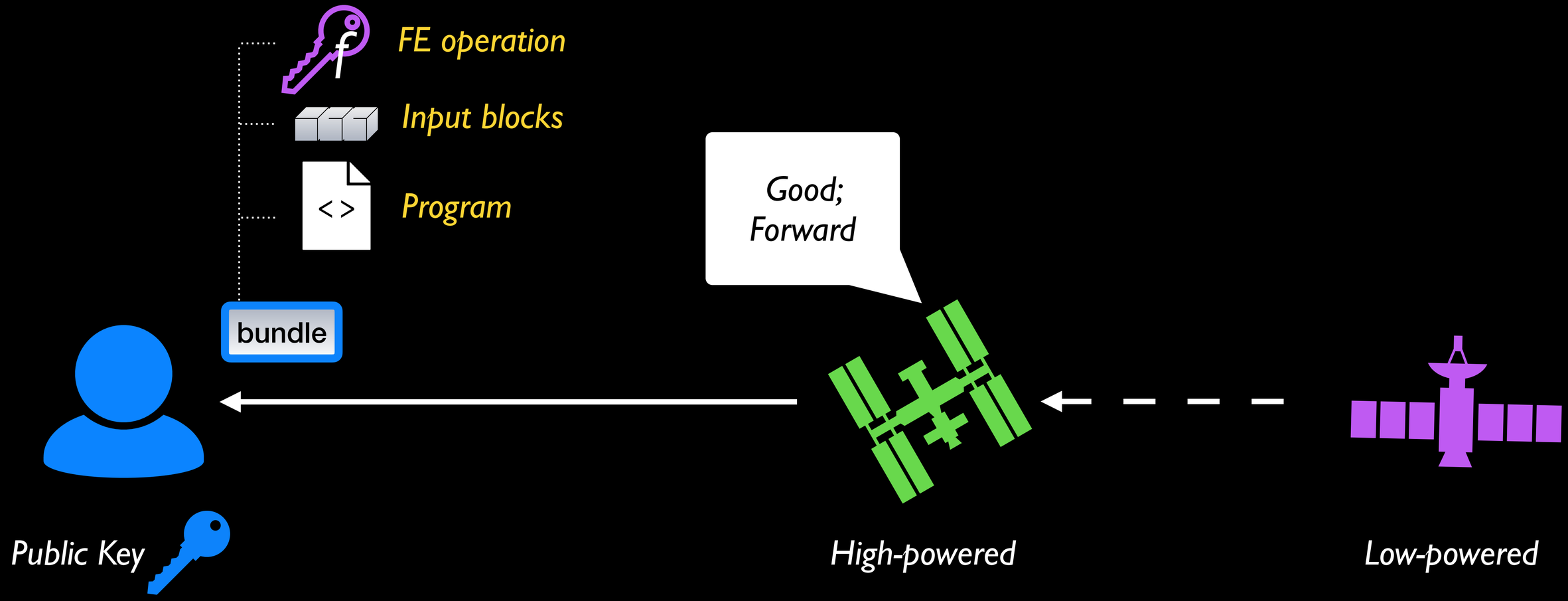
Bundle-Specified FE Programs



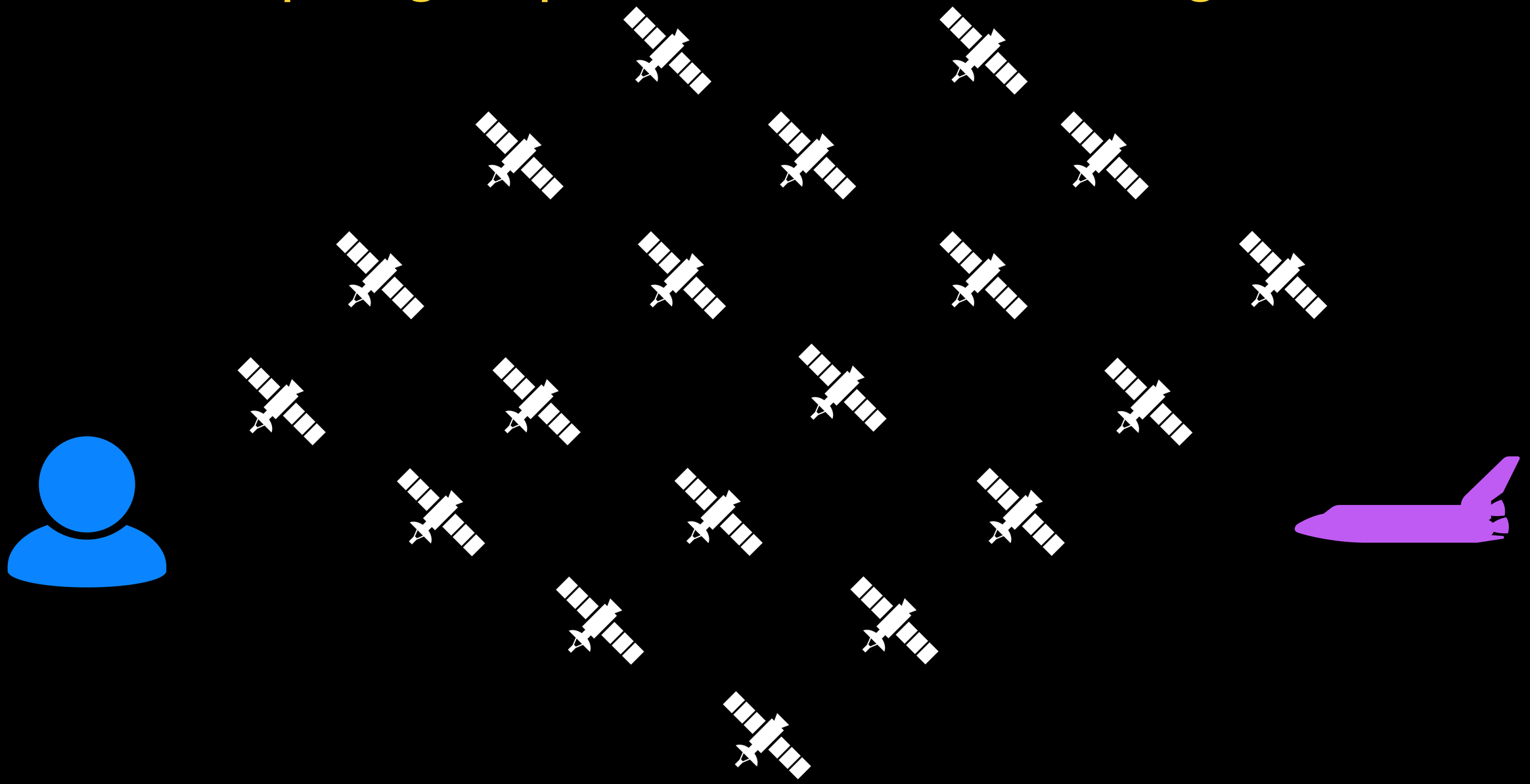
Bundle-Specified FE Programs



Bundle-Specified FE Programs

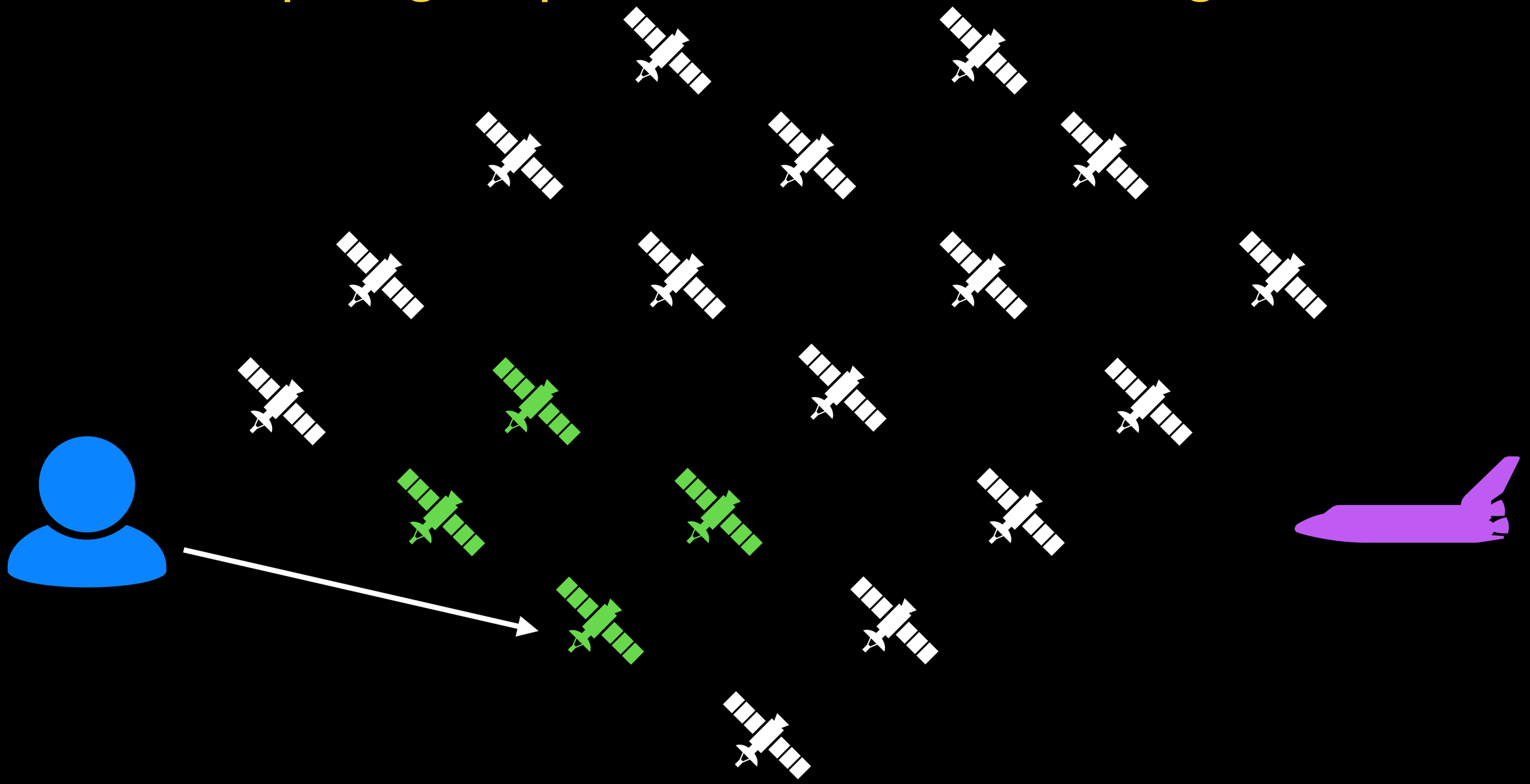


Composing Endpoint Identifiers and FE Programs

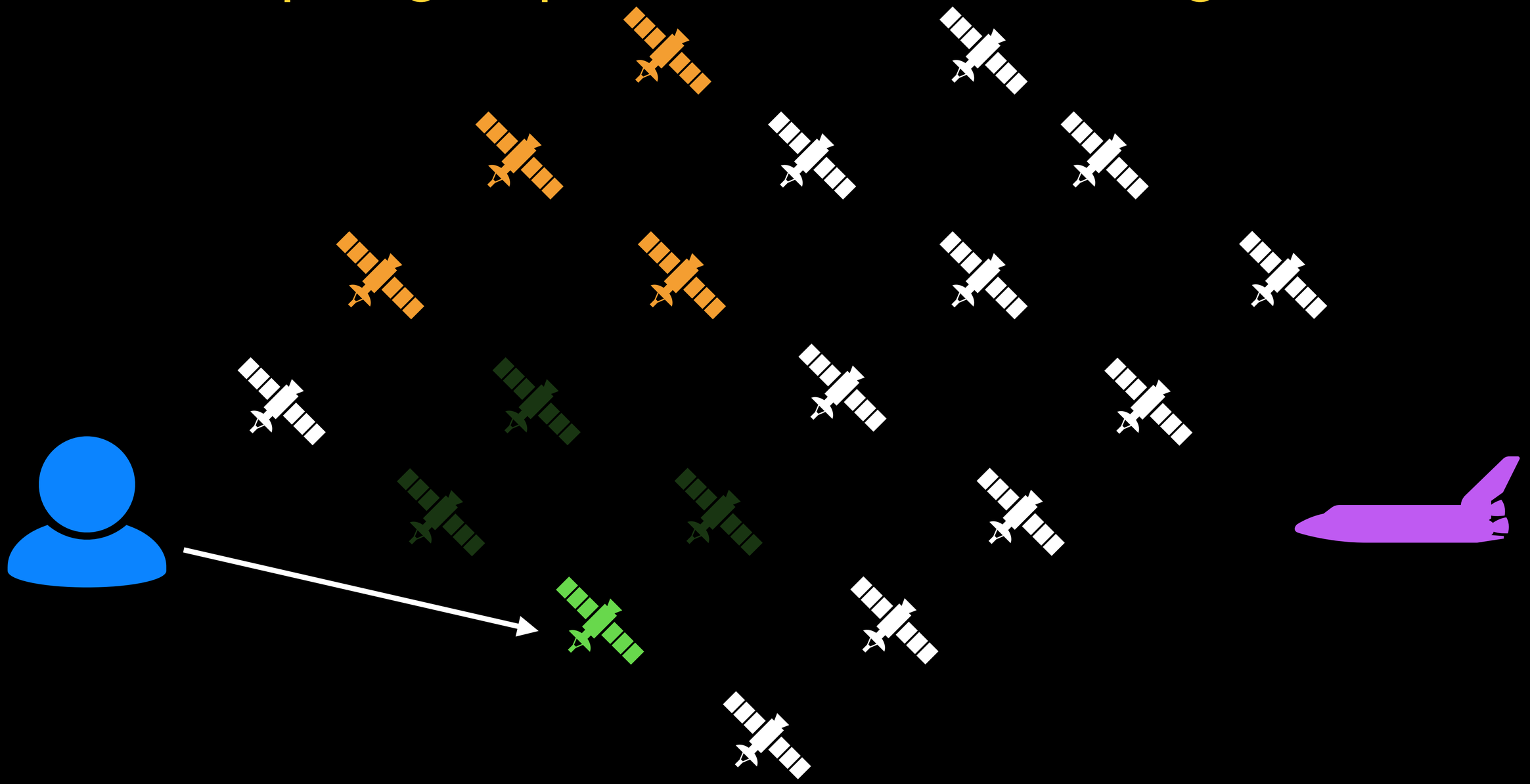


Composing Endpoint Identifiers and FE Programs

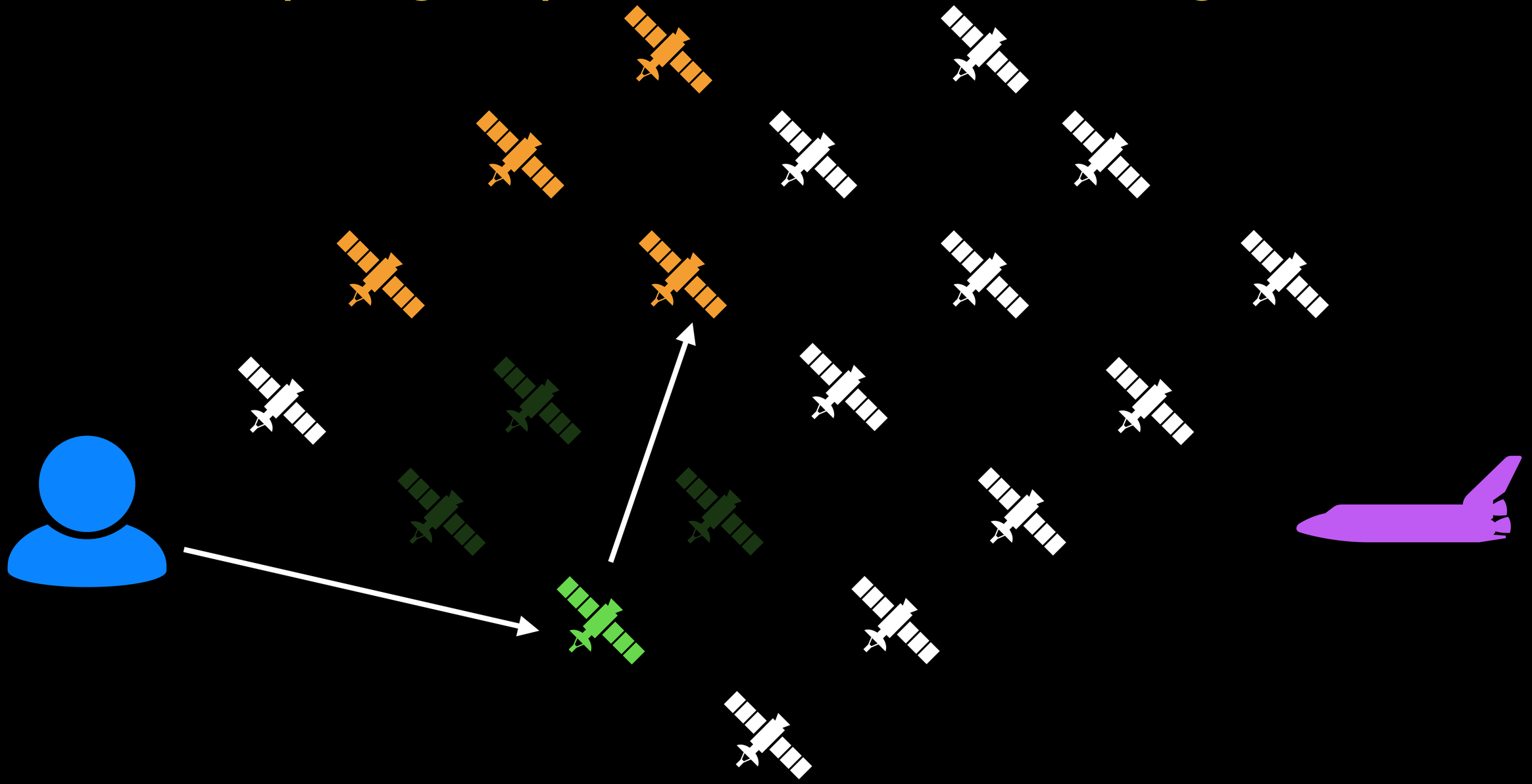
Composing Endpoint Identifiers and FE Programs



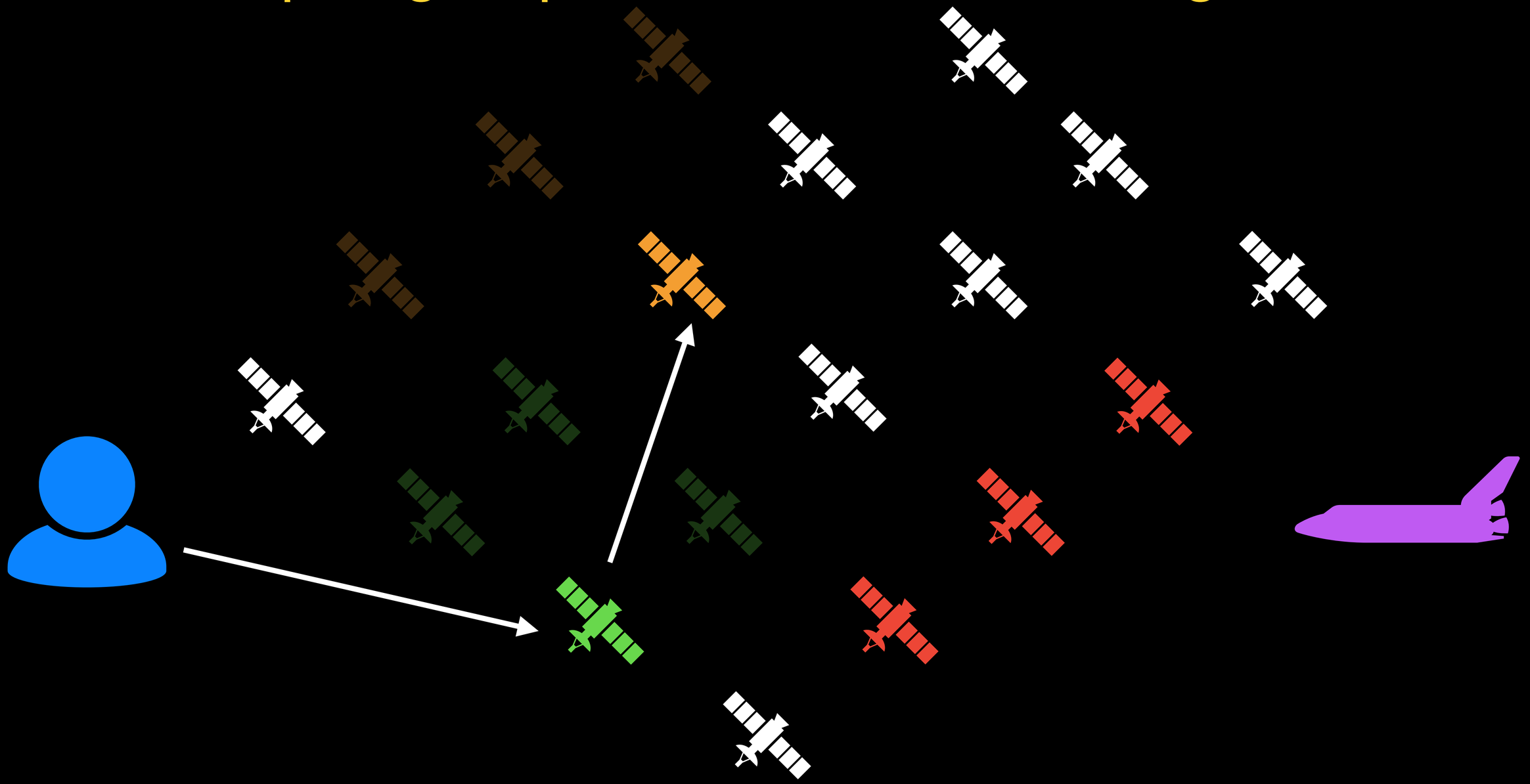
Composing Endpoint Identifiers and FE Programs



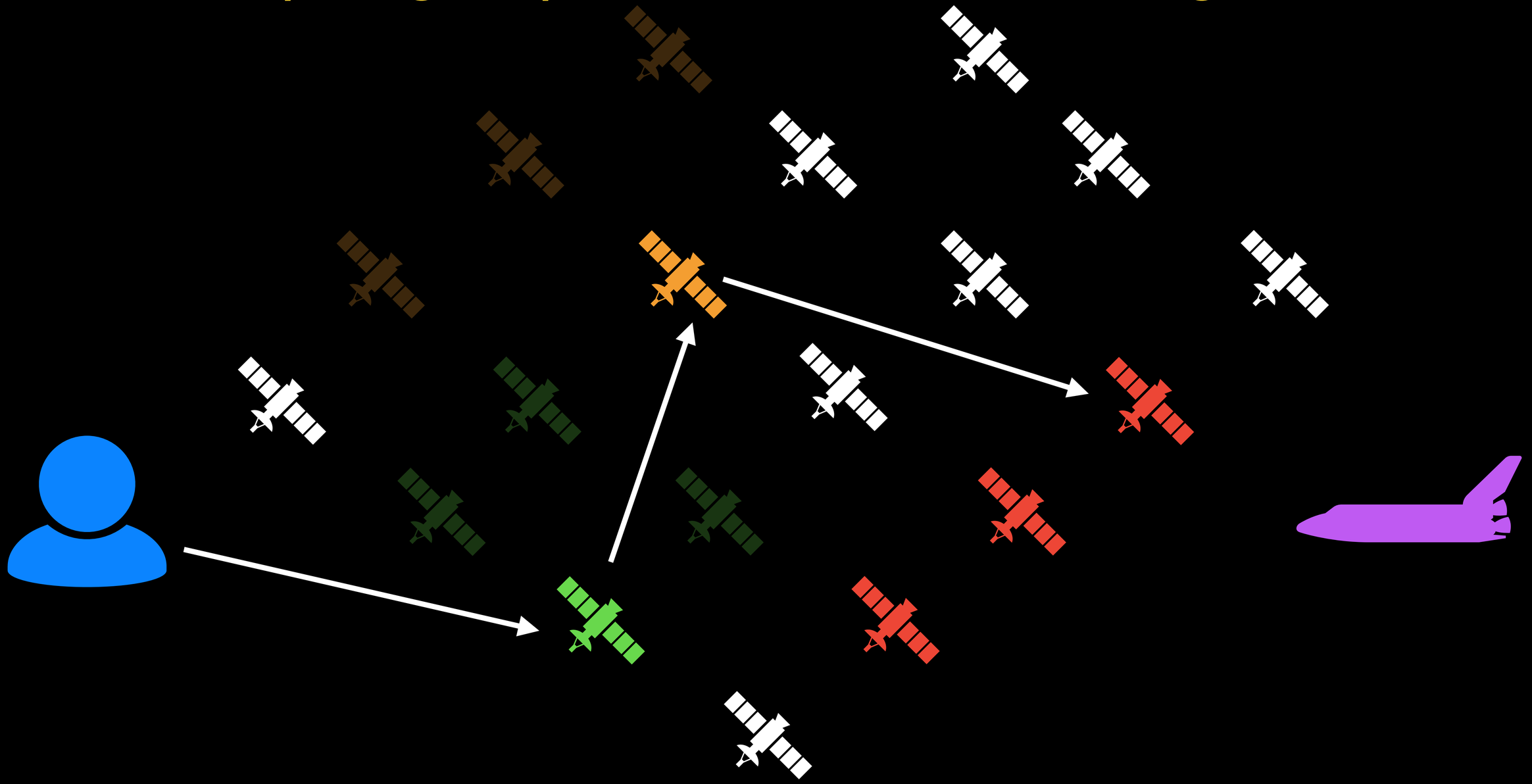
Composing Endpoint Identifiers and FE Programs



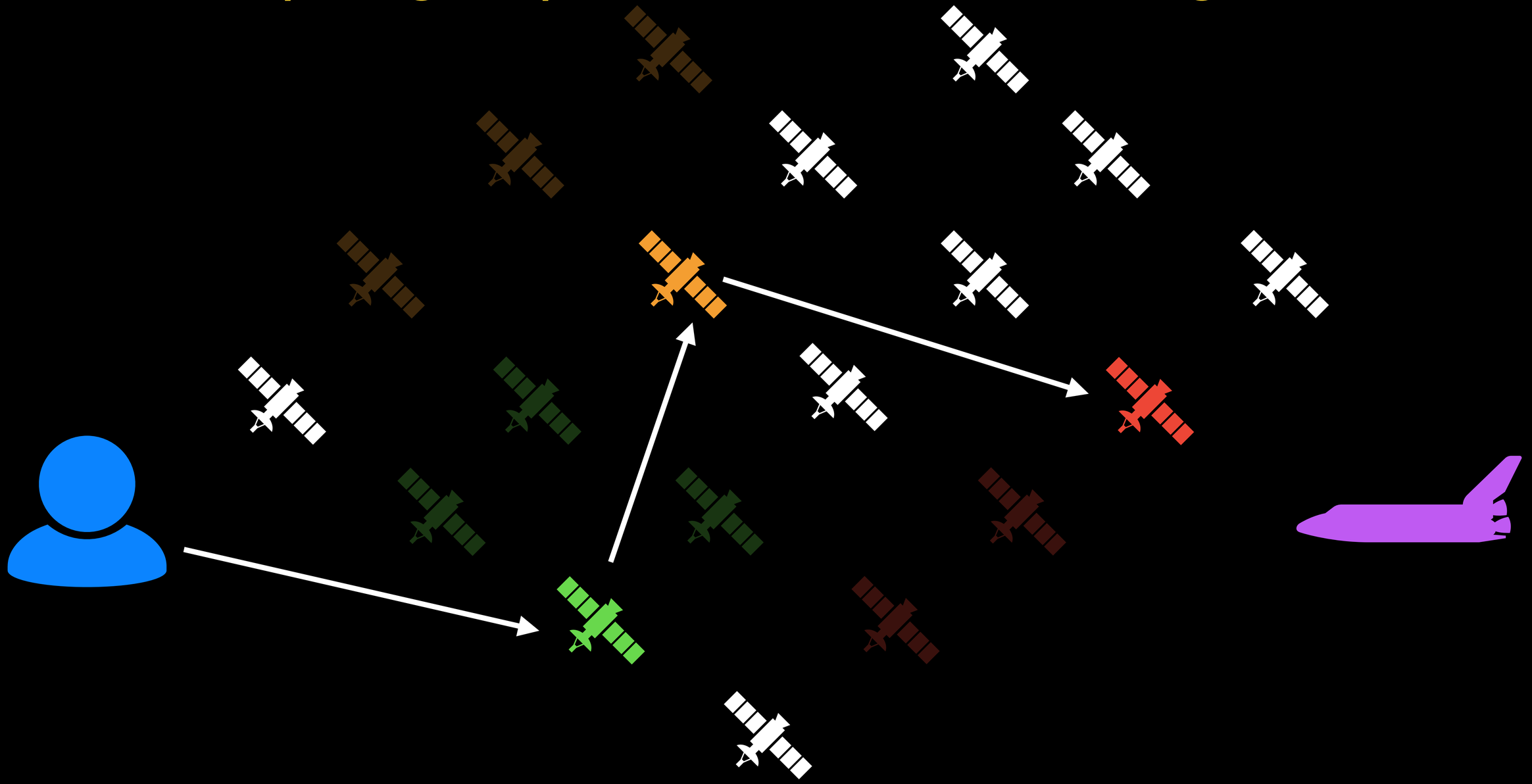
Composing Endpoint Identifiers and FE Programs



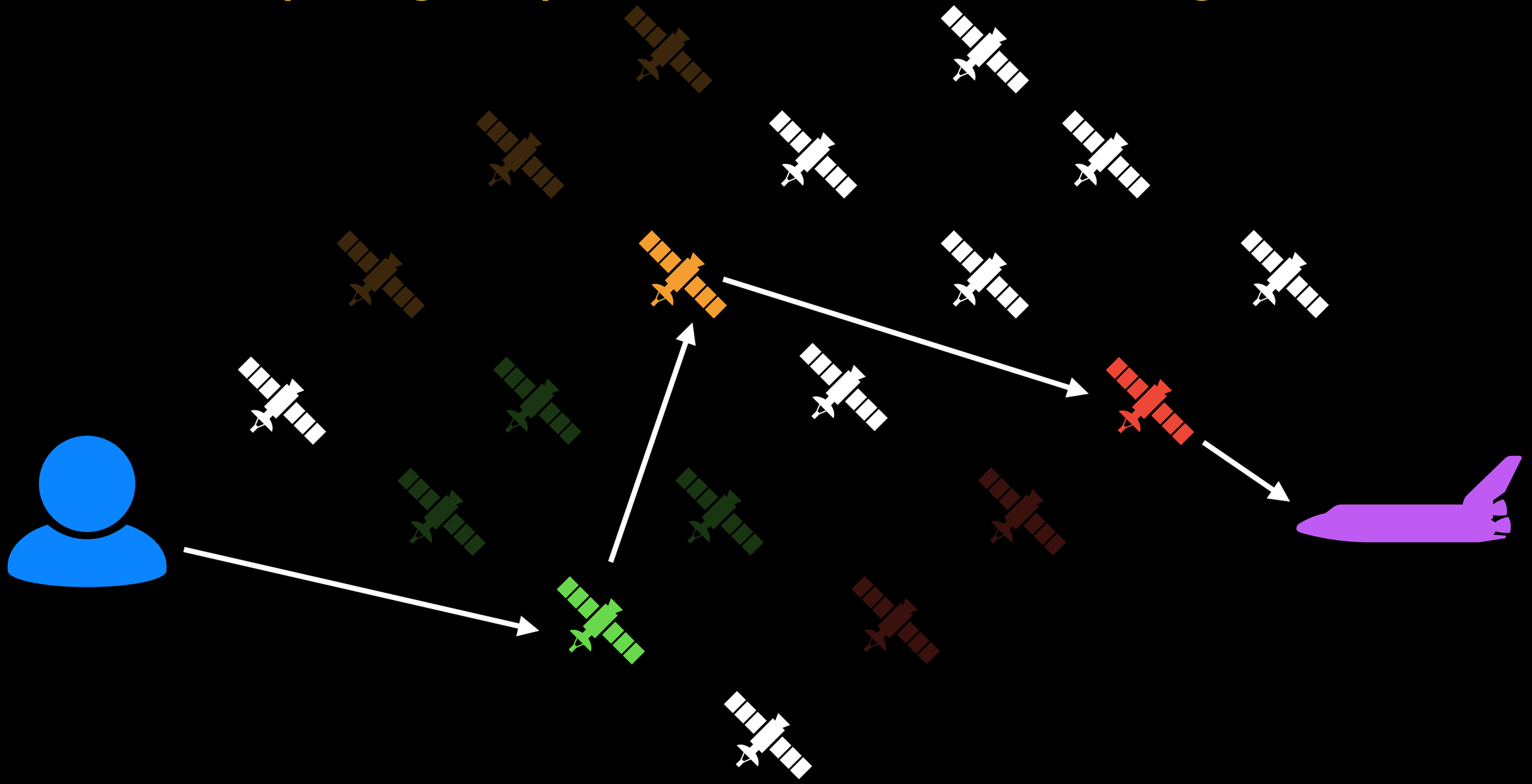
Composing Endpoint Identifiers and FE Programs



Composing Endpoint Identifiers and FE Programs

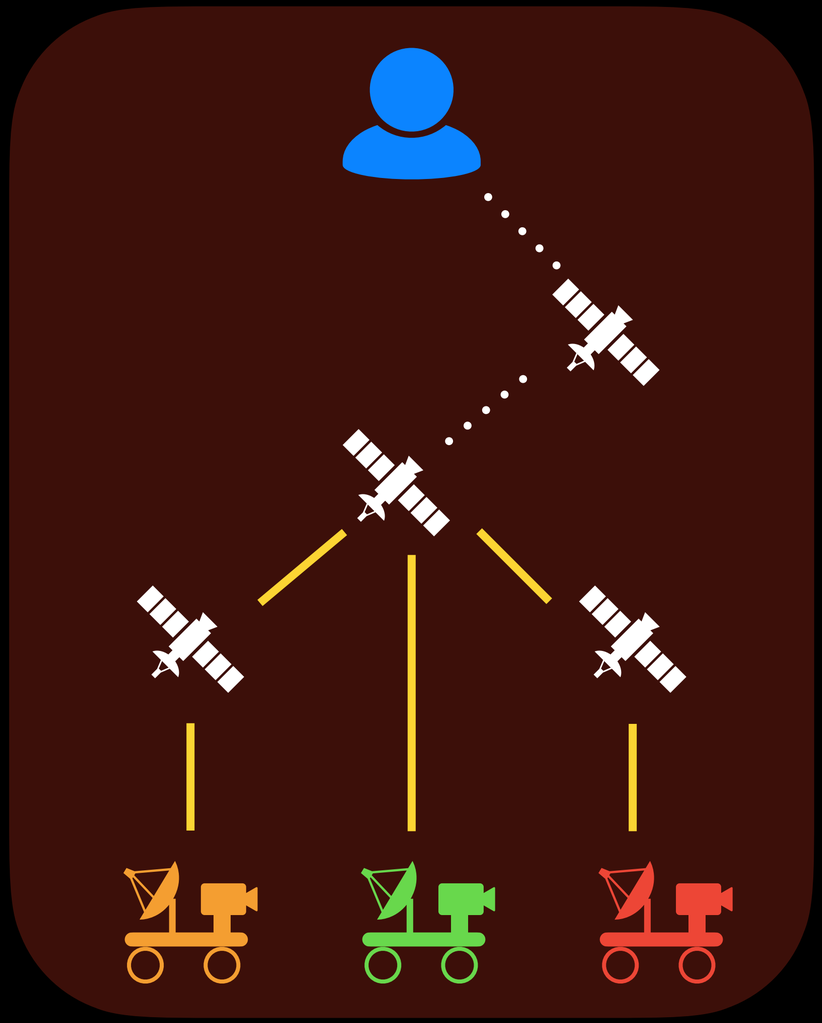


Composing Endpoint Identifiers and FE Programs



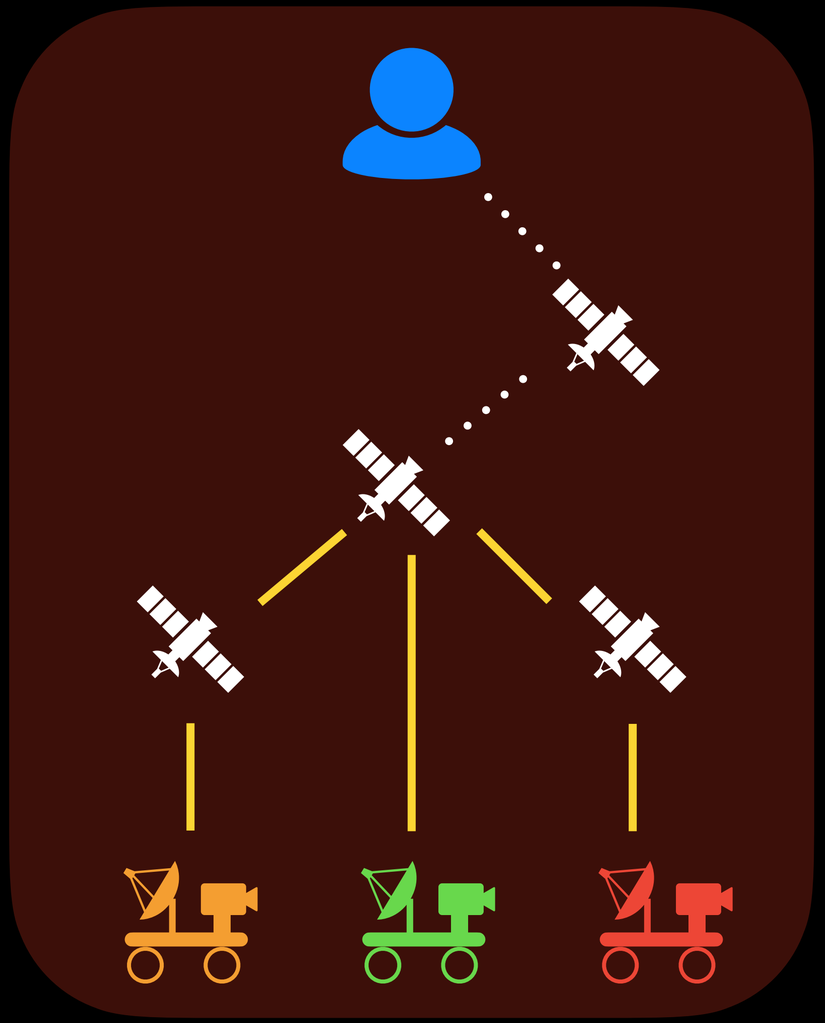
Challenges

Multicast Routing

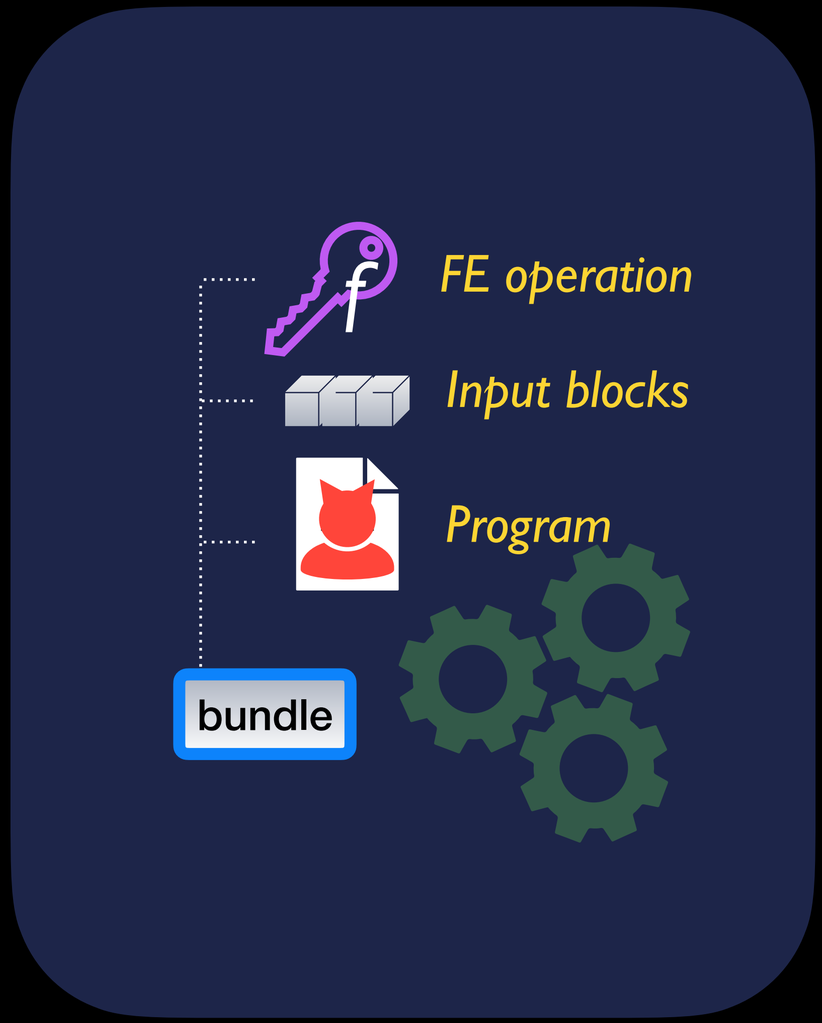


Challenges

Multicast Routing

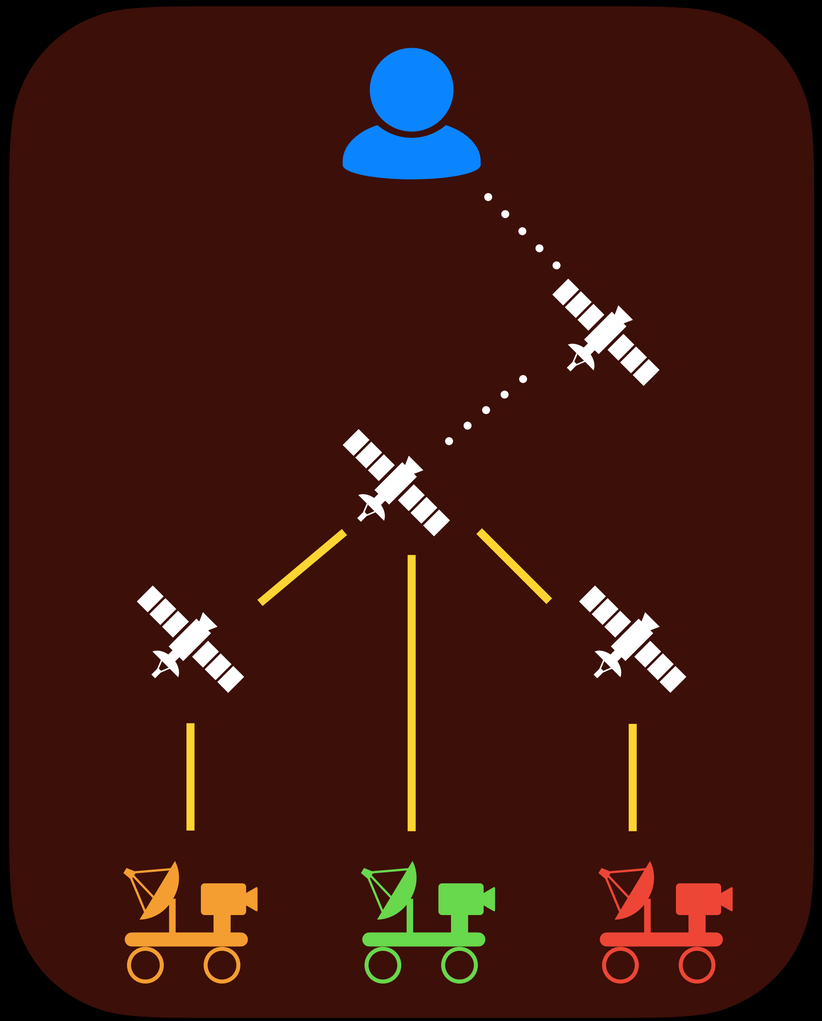


Safe Execution of Untrusted FE Programs

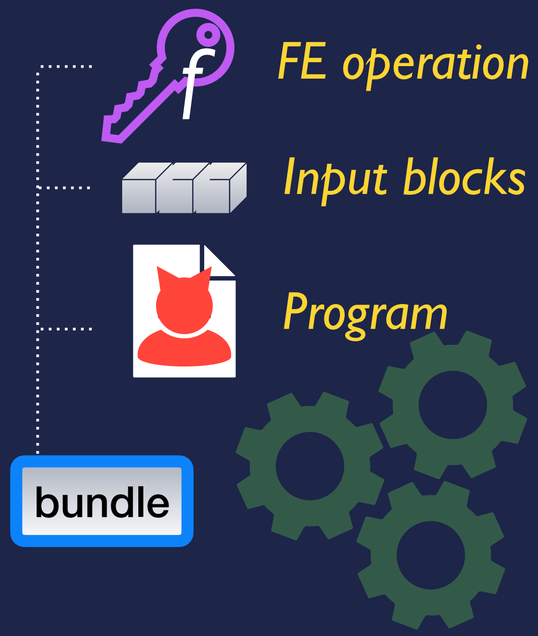


Challenges

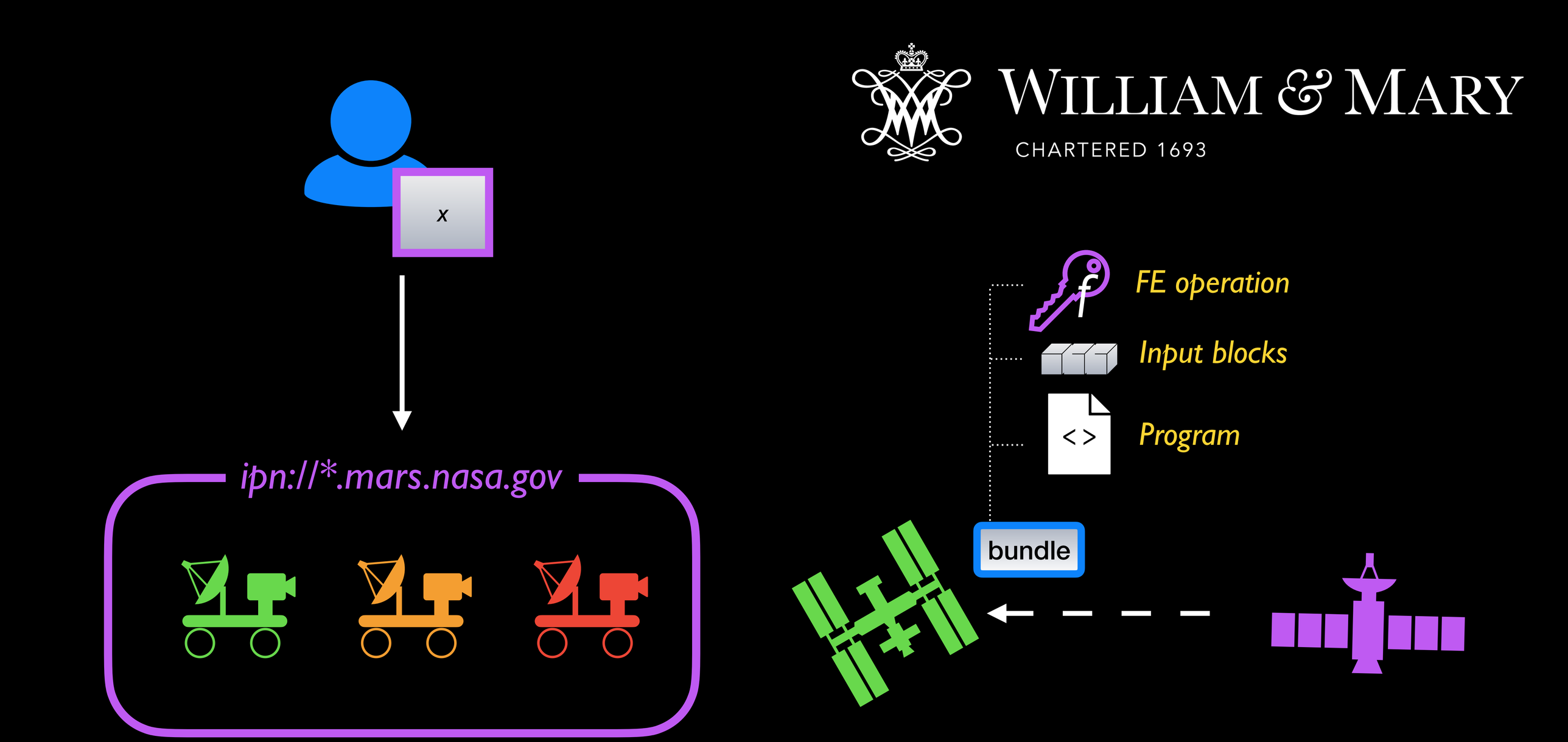
Multicast Routing



Safe Execution of Untrusted FE Programs



Key Management



WILLIAM & MARY
CHARTERED 1693

Stephen Herwig

https://www.cs.wm.edu/~smherwig