SPACECHAIN

SpaceChain Handset Solution

What is the SpaceChain Handset?

SPACECHAIN

A highly secure device designed to connect to a fully protected, globally covered network

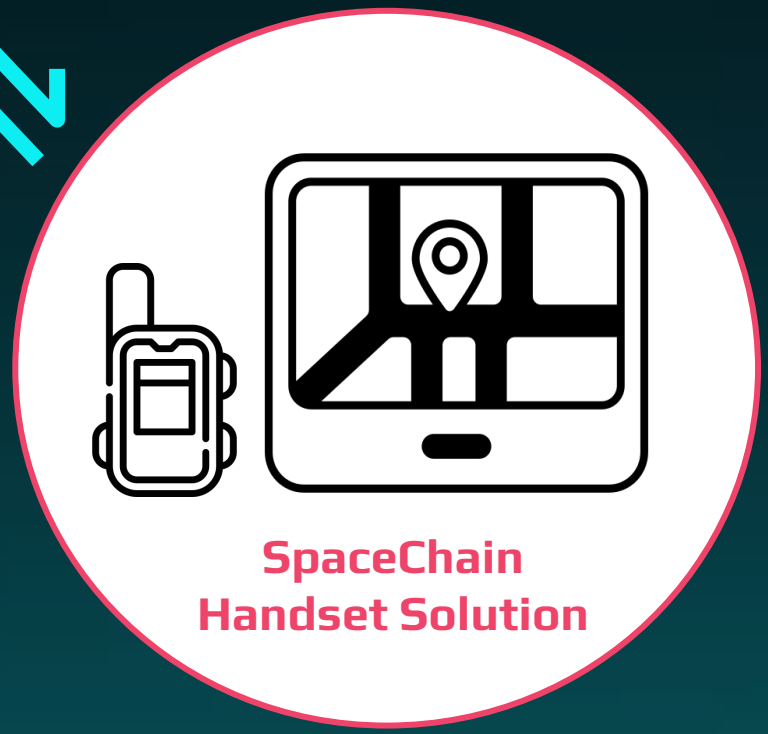
Key features

100% global coverage on an encrypted network

Financial-grade security protection

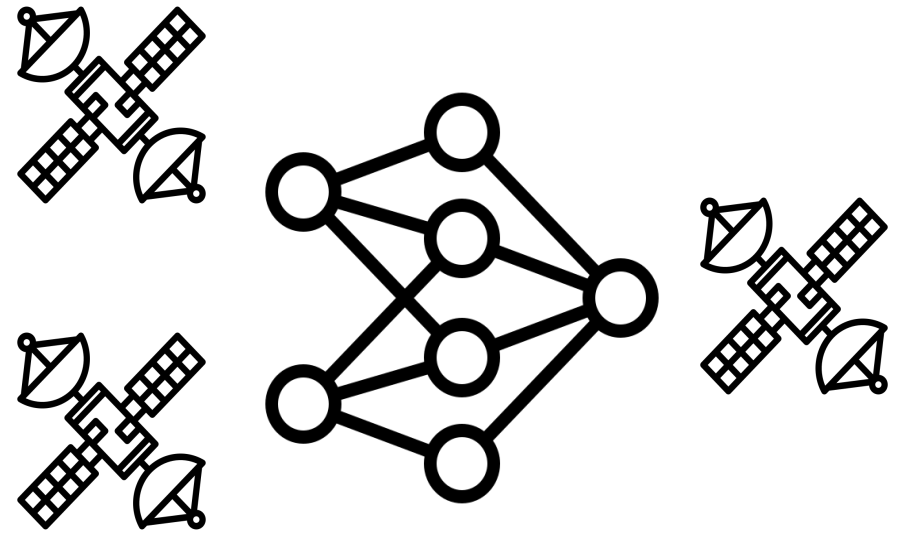
In-orbit key generation for enhanced security

System framework



Key generation in SPACE

The SpaceChain KMS LEO satellite system provides secure key management by using multiple satellites to create a reliable root of trust. These satellites deliver device certificates directly to handsets, ensuring security.



KMS Satellite LEO Constellation

RELIABLE

Multiple satellites work together to ensure no single point of failure.

SECURE

The root of trust is built in orbit, providing a strong foundation for device security.

EFFICIENT

Handsets are certified and receive security certificates directly from the satellite network.

Satellites → Root of Trust → Certification → Handset

100% SAFE NETWORK with global coverage

Our solution provides reliable 24/7 global coverage with secure, encrypted communication, backed by a rugged, military-grade design for durability in demanding environments.

Dedicated Encrypted Satellite Network

SPACECHAIN

24/7 Global Coverage

Stay connected anytime, anywhere.

"Experience Global Connectivity & Unmatched Security."

Secure Communication

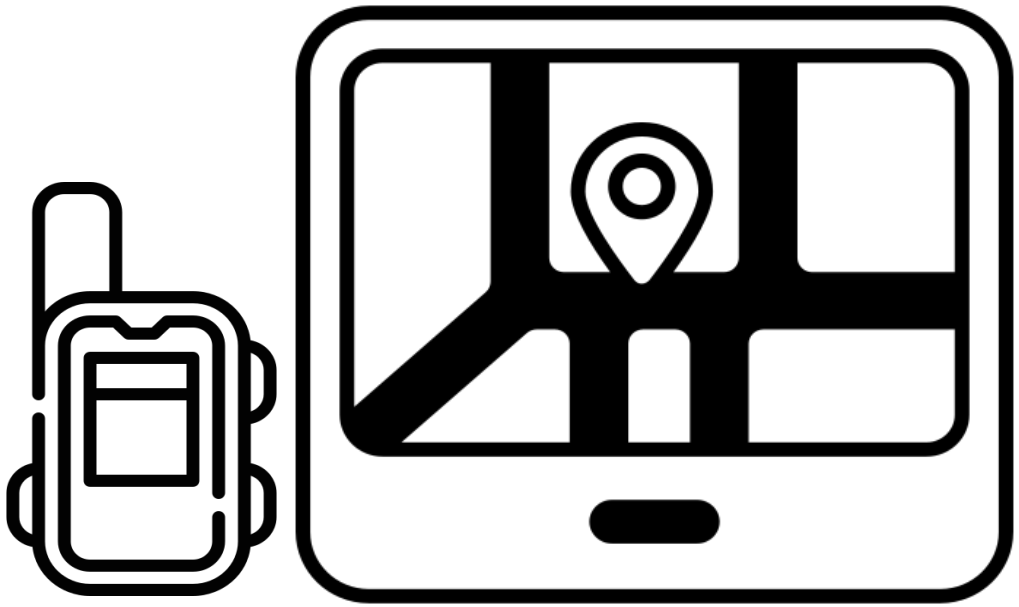
Custom encrypted protocol + dedicated satellite link.

Military-Grade Reliability

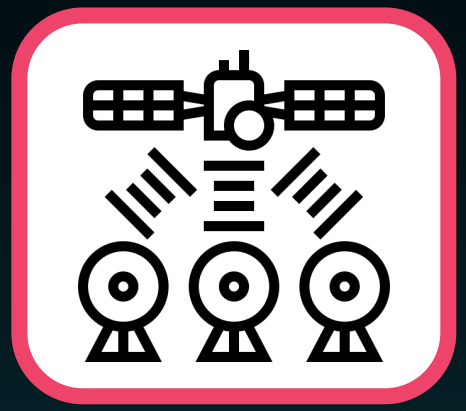
Built for durability and ruggedness.

Device with FULL PROTECTION

Combining satellite networks with financial-grade security chip technology, SpaceChain's device ensures global coverage and highly secure, isolated communication.



SpaceChain Handset Solution

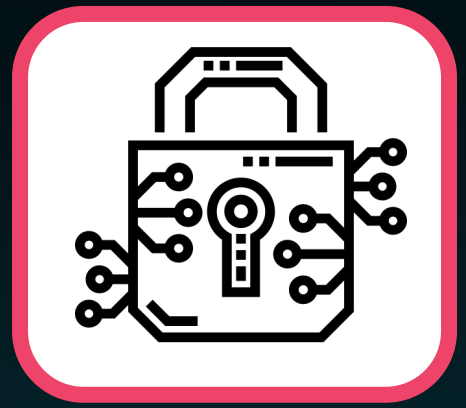


Encrypted Global Satellite Network

All key-related communications are handled over a dedicated, encrypted satellite network. This global network isolates data and protects against external attacks.

Financial-Grade Security Chip

The device integrates a professional security chip that securely stores key data and performs encryption within an isolated environment, ensuring safe operations away from the device's software and hardware.



Integrated Hardware Protection

Equipped with defenses against physical and side-channel attacks, the security chip is designed to withstand various hardware threats, enhancing the overall safety and durability of the device.

With all these features, we can build the most secure key distribution system in the world.

SO, WHAT ARE THE BENEFITS FOR US?

Scenario 1

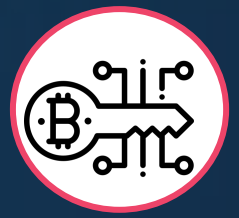
Personal identity authentication & digital asset management terminal

Key features

A secure solution for digital identity and asset management

Biometric Authentication

Fingerprints, facial recognition, iris scans



Digital Asset Management

Secure management of cryptocurrency private keys

Organizational Identity

Web3 community identity proof and authority verification

Cyber Authentication

- Decentralized identity verification (DID)
- NFT, BNS, and ENS account ownership
- DApp interactions

Benefits of the terminal

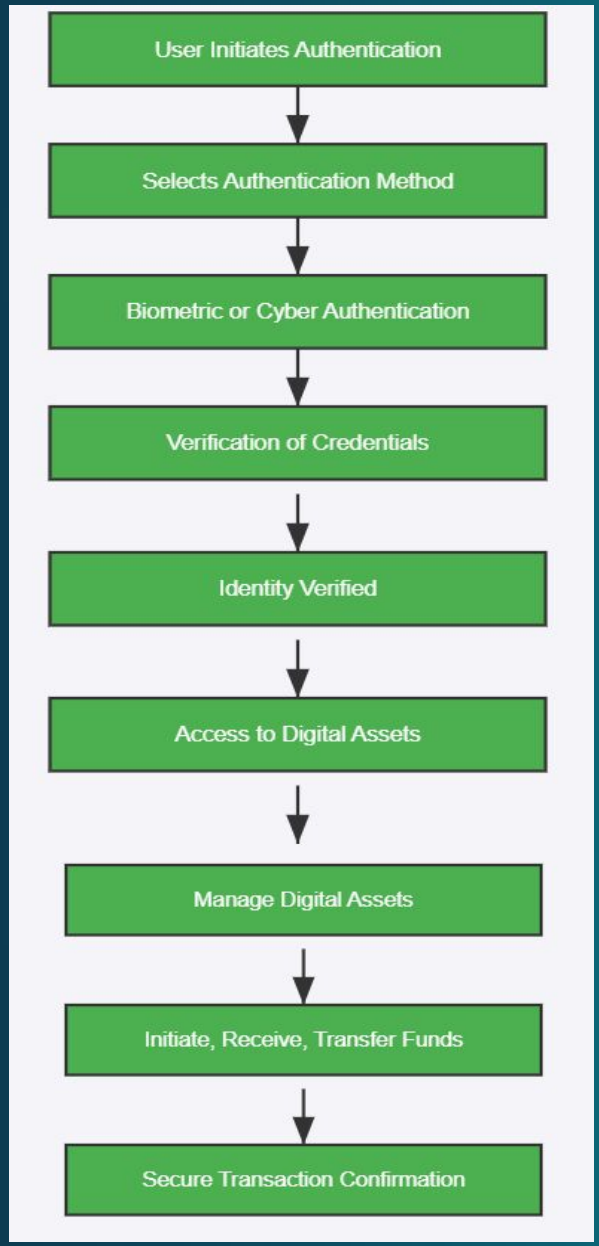
All-in-One Solution

- Secures user authentication with a secure element.
- Enables login through zero-knowledge proofs or SpaceChain KMS.
- Allows users to verify their Web3 identity and asset ownership without revealing personal information.

Personal Digital Asset Management

- Full protection for cryptocurrency keys.
- Manage assets anytime, anywhere via satellite network.
- Securely initiate, receive, and transfer funds while verifying identities.

Here's how it works



SPACECHAIN

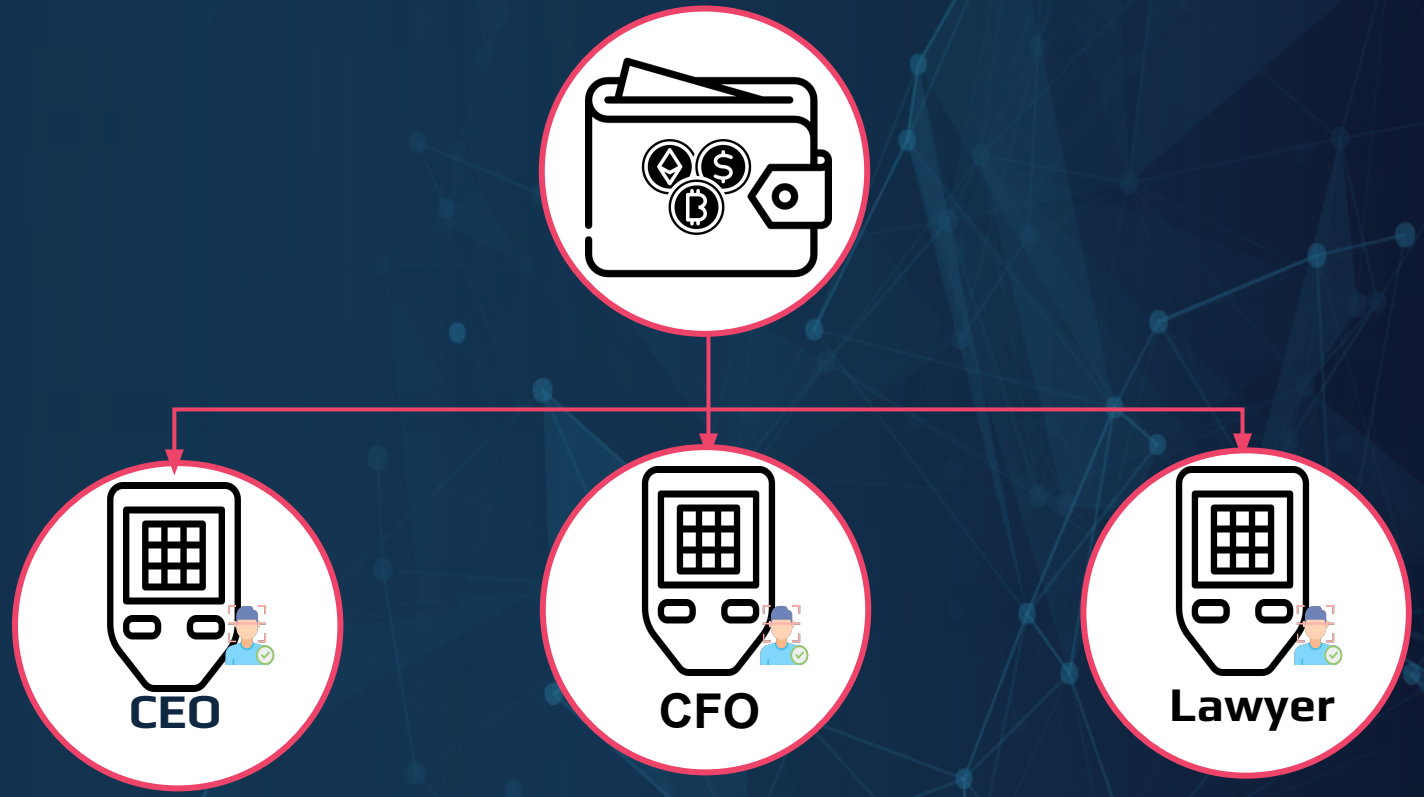
Scenario 2

Digital asset multi-party co-managed account

Simplifying digital asset management for teams

What is a Multi-Party Management Account?

- A secure way for teams to manage digital assets together.
- Each manager has specific permissions based on their role.



Key features

Real-Time Monitoring

- Managers can check account status and approve transactions anytime, anywhere, using their mobile devices.

Strong Security

- Managers' identities are linked to their devices through advanced biometric methods like iris scans and fingerprints.
- Utilizes SpaceChain KMS satellites for secure signature authentication, ensuring all actions are traceable.

Robust security & flexible management

Hardware-Level Protection

- Even if a device is lost or damaged, account security remains intact thanks to secure elements protecting sensitive data.

Smart Contracts for Authority Control

- Each manager’s permissions are defined by smart contracts, ensuring reliability and flexibility.
- These contracts are programmable and verifiable, making management straightforward and secure.

Ideal Use Cases

- Perfect for key company accounts, high-value transactions in exchanges and casinos, and management of crypto and ETF assets.

Scenario 3 Private encrypted communication

Secure and private communication for everyone

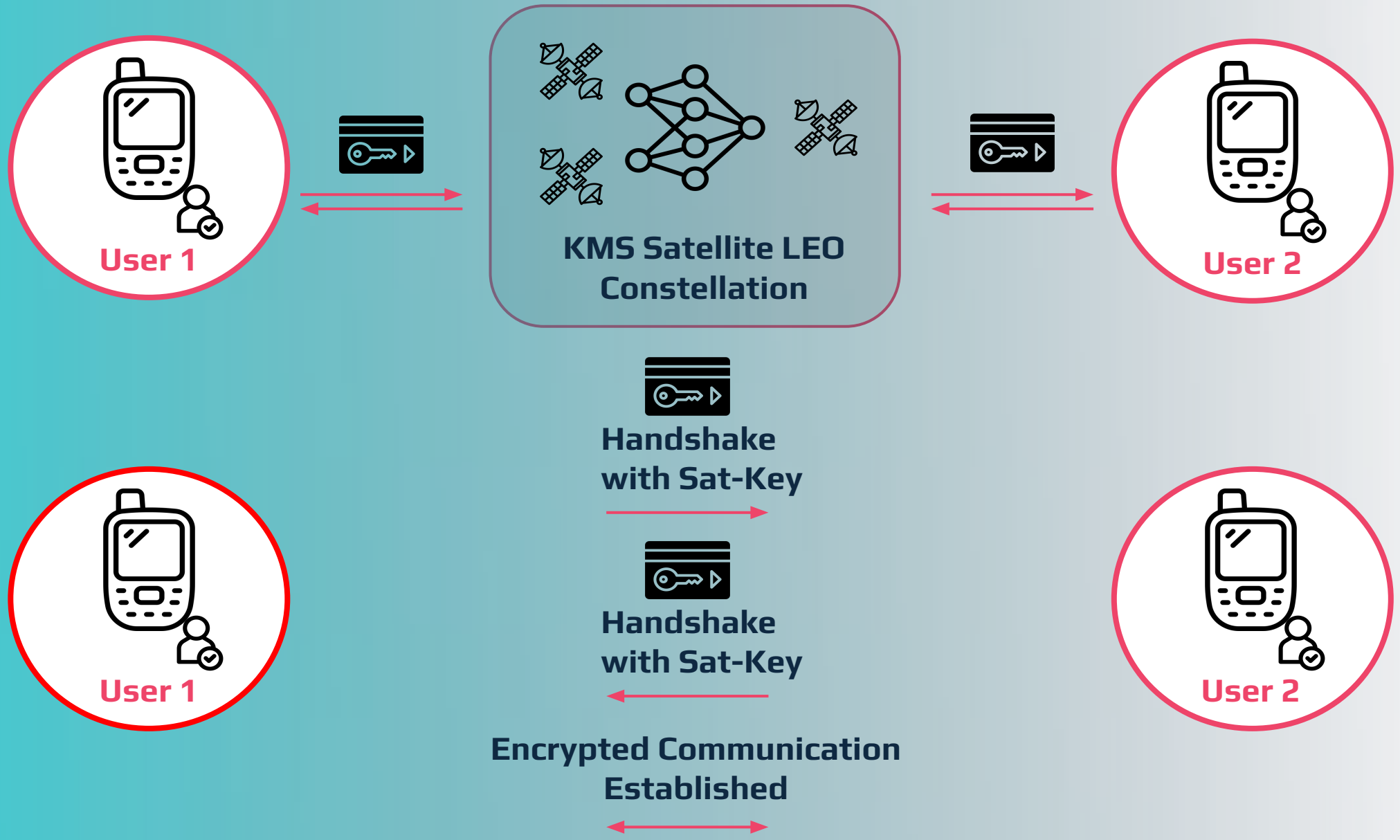
What is Private Encrypted Communication?

- A safe way for users to communicate without fear of interception.
- Ensures that only verified users can send and receive messages.

How It Works

- **User Authentication:**
  → Users verify their identities using the SpaceChain KMS system.
  → They receive certified identity authentication certificates for added security.

- **Encrypted Messaging:**
  → Users exchange these certificates to set up a secure communication channel.


User 1
KMS Satellite LEO Constellation
User 2
Handshake with Sat-Key
Handshake with Sat-Key
User 1
User 2
Encrypted Communication Established

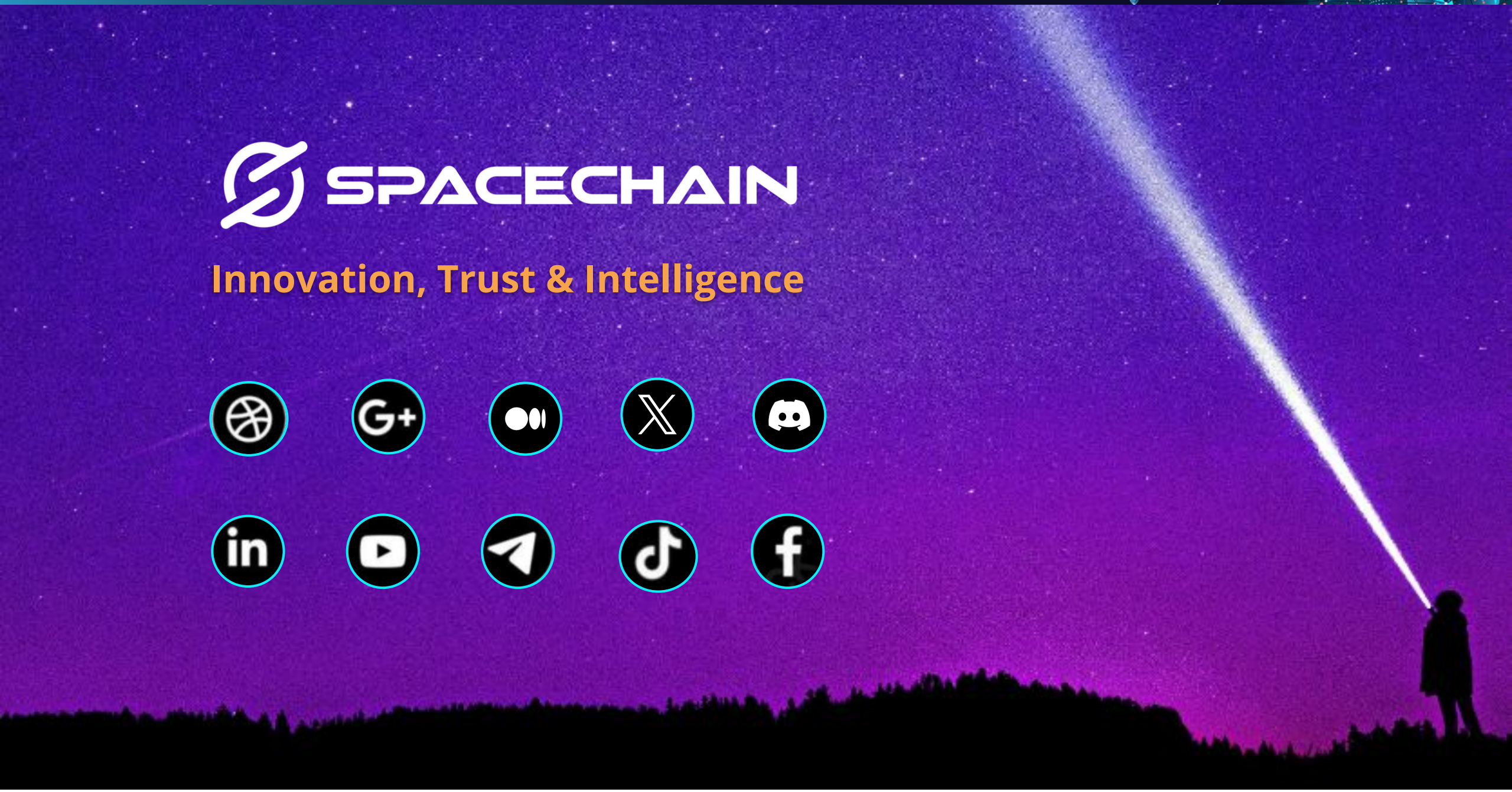
Benefits of encrypted communication

Why Choose Private Encrypted Communication?

- **Message Verification:** All messages can be easily checked and verified for authenticity.
- **Global Accessibility:** Communicate privately from anywhere in the world at any time.

Who Can Benefit?

- Ideal for businesses, professionals, and anyone who values their privacy in communication.


SPACECHAIN
Innovation, Trust & Intelligence