

# FreeBit Co., Ltd.: Bringing blockchain technology and Thales Luna HSMs together to forge an innovative digital key infrastructure

## Summary

The demand for digital keys as an integral part of a highly convenient network society is growing. At the forefront of the spread of digital keys are the automotive, housing and hotel industries. FreeBit Co., Ltd., (hereinafter referred to as "FreeBit"), a company engaged in the provisioning of Internet-related services, has jointly developed a blockchain-based infrastructure for digital keys together with Alps Alpine Co., Ltd., leading manufacturers of car electronics. In addition, FreeBit jointly developed The Log, a blockchain-based solution to help prevent tampering with tracing logs and other forms of system operating information, and the company has begun using this solution on an in-house basis.

In blockchain systems, the management of private keys is the key to security. FreeBit built a scheme for managing private keys that is compliant with the highest level of FIPS 140-2<sup>1</sup> at Security Level 3 validation, and successfully created an innovative blockchain-based infrastructure combining security, versatility and scalability.

## Selection points

As shown by such trending keywords as CASE<sup>\*2</sup> and MaaS<sup>\*3</sup>, the automotive industry is facing a period of major change. FreeBit has been expanding its business on a multi-layered basis with respect

to everything from infrastructure services that include the provisioning of support for Internet Service Providers (ISPs) and Mobile Virtual Network Operators (MVNOs), to cloud services for corporate clients, and mobile communication services that provision solution services for the education, pharmaceutical and housing sectors. When it comes to the automotive industry, however, FreeBit has entered into a comprehensive tie-in arrangement with Alps Alpine Co., Ltd., and is engaged in joint development work in accordance with the concept of CaaS<sup>\*4</sup> for the realization of a seamless car life in the era of CASE and MaaS.

Announced in January 2019, the first digital key system is a simple, low-cost option that covers key management processes for the issuance of car keys and the transference of rights. Announced in July 2019 as the second digital key system to be released, The Log is designed to prevent tampering with system operating information in all types of Internet and IoT infrastructure. The Log is being gradually introduced to cloud services as well. Plans are also underway to adopt The Log for digital keys being jointly developed together with Alps Alpine Co., Ltd.



" Using Luna HSMs, we were able to create a highly connected and versatile blockchain infrastructure. We will seek to expand the applicability of this infrastructure into all sorts of different fields, such as platforms for storing important data other than logs. Blockchain constitutes an exceptional technology that is vital in the IoT era, and we believe that the areas in which it can be applied by combining it with Luna HSMs can be broadened even further."

— Tomohiro Tamanoi, Senior Executive Manager

1. The Federal Information Processing Standard (FIPS) 140-2 is a benchmark for verifying the effectiveness of cryptographic hardware. If the product in question is FIPS 140-2-validated, this status indicates that the product has been tested and formally verified by the U.S. and Canadian governments.

2. CASE: An acronym for connected, autonomous, shared, and electric.

3. MaaS: Mobility as a Service.

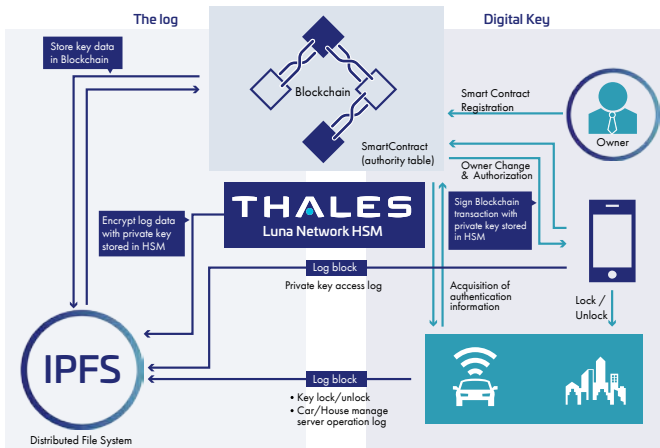
4. CaaS: Car as a Service.



Blockchain technology was used to innovate digital keys and log management systems. It takes advantage of a robust security mechanism for preventing data from being rewritten by unauthorized persons, and provides the ability to efficiently cover the long lifecycle of both new and used cars with a public system. In a blockchain, authority is ultimately protected by a private key, and the system by which private keys are managed is indeed the critical point for the security level of the entire system. Upon weighing various cryptographic key management solutions, FreeBit determined that the adoption of dedicated hardware specially designed for the purpose of providing cryptographic key protection would ensure the highest levels of security. The Luna Network HSM was consequently introduced.

## Solutions

Freebit selected Luna Network HSM as its hardware root of trust due to its flexibility and strong security architecture, namely the FIPS 140-2 Level 3-validated hardware; operations by which private keys are never removed from the hardware; as well as support for elliptical curves and the various necessary cryptographic algorithms. Additionally, they were able to extend their return on investment by partitioning a single HSM into multiple virtual HSMs, while supporting functionality proprietary to FreeBit. Integration with Luna Network HSM was completed in a short period of time and included a wallet function, which was already being developed through the use of PKCS #11, a standard interface for cryptographic devices. Service cutover was performed as initially planned.







Build innovative digital key systems and off-chain log storage systems with security infrastructure combining blockchain and the Luna Network HSM.

## About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> [cpl.thalesgroup.com](http://cpl.thalesgroup.com) <    

**Americas** – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: [CPL.sales.AMS\\_TG@thalesgroup.com](mailto:CPL.sales.AMS_TG@thalesgroup.com)  
**Asia Pacific** – Unit 1106-1107, New Kowloon Plaza 38 Tai Kok Tsui Road, Kowloon Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: [CPL.sales.APAC\\_TG@thalesgroup.com](mailto:CPL.sales.APAC_TG@thalesgroup.com)  
**Europe, Middle East, Africa** – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: [CPL.sales.EMEA\\_TG@thalesgroup.com](mailto:CPL.sales.EMEA_TG@thalesgroup.com)

## Challenges

- Robust security in terms of private key management is required for any new blockchain-based digital key system
- It is not enough to simply store private keys; innovation, reliability, and performance are also important when it comes to the high-speed processing of encryption and digital signature services in an Ethereum environment

## Solutions

- Developed a strong mechanism for the management of private keys by combining blockchain with the Luna Network HSM
- Using infrastructure produced by combining blockchain with Luna Network HSM, FreeBit developed The Log, a solution designed to prevent tampering with system operating information
- They also built a new, high-security mechanism for the management of logs corresponding to off-chain parts that are vital to large-scale blockchain systems

## Advantages

- Established the highest level of security for the management of private keys to achieve an innovative digital key system
  - HSM for retaining cryptographic keys in hardware throughout their lifecycle
  - FIPS 140-2 Level 3 validated
- An easy to develop, versatile, and highly scalable technical infrastructure has been realized
  - High-speed linking with SmartContract and IPFS (InterPlanetary File System) servers in an Ethereum environment has been achieved in a manner that is compatible with industry-standard interfaces
  - Public key interface supports industry-standard PKCS #11
  - A high level of processing muscle delivers exceptional performance
- A single HSM can be partitioned, and the resulting partitions can be efficiently used in parallel in a production/development environment
  - Can be divided into up to 100 partitions-multiple services can be developed concurrently
- Building backup systems with a highly secure HA configuration
  - Using the Thales Luna Backup HSM, a dedicated backup hardware device, a backup system can be built without lowering the security level
  - The HA configuration is also prepared in advance to facilitate the building of a backup system without the hassle of setting it up
- Stable support in Japan
  - Materials for developers are fully available, in particular, source codes for encryption, SmartContract linking, and digital signatures have proven to be very useful
  - Thales is highly knowledgeable about blockchain technology