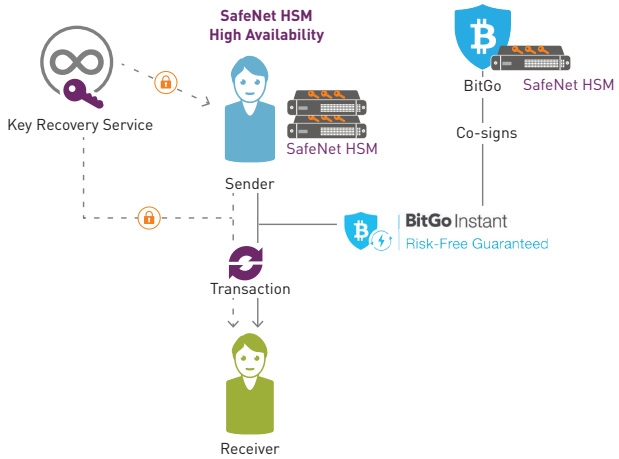
SOLUTION BRIEF

Securing Digital Currency with BitGo Multi-Signature and SafeNet HSMs

With the invention of Bitcoin and blockchains, cryptocurrencies and digital assets are rapidly coming to mainstream finance. Security of systems processing digital assets is paramount, and today's financial institutions expect all the robustness and security of traditional systems also applied to digital assets. Without strong data protection, an enterprise would simply not be able to take advantage of the many benefits offered by BitGo's digital currency - including the ability to easily and quickly process high-volume cryptocurrency transactions and payments.

Gemalto and BitGo have partnered to provide BitGo's solution the highest level of security by safely storing all user cryptographic keys inside SafeNet Hardware Security Modules (HSMs). As a result, BitGo's enterprise customers can now make digital currencies such as Bitcoin usable for business in a regulated economy, ensuring their assets are always secure.



Gemalto / BitGo Solution Capabilities:

- Secure cryptocurrency transactions within the FIPS 140-2 validated HSM confines
- Instant, secure transactions between participants
- Extend HSM functionality with the BitGo code custom logic running on the HSM
- Additional security with multi-signature technology
- Meet SLAs with a high scalability HSM
- Full back up and recovery of keys and wallets

BitGo Multi-Signature Technology

BitGo is the world leader of digital asset multi-signature technology. BitGo's powerful platform provides unparalleled security through on-premises signing, a co-signing engine with policy enforcement and multi-user approvals, along with simple integration and instant scalability for the world's largest transaction processors.

BitGo wallets consist of 3 keys: one held by BitGo; one held by the user for signing; and one held by the user for recovery and backup. Two signatures are required on every transaction on a BitGo wallet.

With BitGo software on the SafeNet HSM, BitGo and Gemalto have created the world's first industry-grade servers for processing cryptocurrency signing and key derivation. BitGo relies exclusively on Gemalto to store all of it's encryption keys, and this implementation is extended to BitGo customers using blockchain in their own on-premises solutions. As a result, digital assets can be securely stored in environments requiring the highest level of security.

SafeNet HSMs from Gemalto

SafeNet HSMs are dedicated cryptographic processors specifically designed for protection of the lifecycle of cryptographic keys that secure transactions, identities and applications and act as a root of trust for the cryptographic infrastructures of the most security conscious organizations in the world.

SafeNet HSM hardware appliances protect end-user private keys used to co-sign Bitcoin transactions. This is an essential component to maintaining the trusted integrity of the blockchain. BitGo selected FIPS 140-2 Level 3 validated SafeNet HSMs as they offer a unique level of flexibility for application developers to create their own firmware and execute it within the secure confines of the HSM. Known as Functionality Modules (FMs), the toolkits provide a comprehensive facility to develop and deploy custom firmware.

High Assurance for BitGo Bitcoin Digital Currency Customers

Contact us to determine how BitGo Instant technology, together with SafeNet HSMs can provide you the with enhanced security and assurance for your BitGo digital currency transactions or help ensure the integrity of the custom blockchain.

About Gemalto Enterprise Security

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments, and data – from the edge to the core. Gemalto's portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Benefits of Joint Solution:

- Strong, secure hardware root of trust for your private signing keys
- Speed for your high volume transactions
- Customizable solution
- Protection against double spending
- Continuity and certainty to meet your business needs
- Recoverable keys and unlike other blockchain solutions
- Only Multi-Signature / HSM key storage solution available today
- Combined solution providing the highest levels of security for blockchain digital currency transactions

About BitGo

BitGo's mission is to make digital currencies usable for businesses in a regulated economy. BitGo's technology solves the most difficult security, compliance and architectural problems associated with blockchains, enabling businesses to integrate digital currencies into their existing financial systems. Processing more than $1B monthly, BitGo customers include the largest cryptocurrency exchanges and application providers in the world. Headquartered in Palo Alto, the company was founded in 2013 by veterans in online security and financial technology.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free