Solution Brief

# IBM Hyper Protect Digital Assets Platform

—

Protect your digital assets on a ***hyper*** secure, tamper-proof Linux-based platform

*Financial Institutions, Exchanges, Fintechs, Crypto Custody providers*

IBM Systems / 8 December 2020/

# Digital assets are cryptographically secured with a public and private key pair

The public key is like a mailbox (everyone can see it, and anyone can send digital assets to it) while the private key is like the key to that mailbox (only the owner can open it and access what's inside).

**If you hold the private key, you own the digital assets at the corresponding public key address.**

"Wallets" store your private keys, public keys, and public addresses. They also let you make transactions.

Digital Asset Market is exploding — according to a 2019 Research and Market report, the tokenization market size is estimated to grow from USD 983 million to USD 2.6 billion by 2023, at a CAGR of 22.1% during the forecast period.

However, custody of crypto assets presents a high barrier to entry into the crypto market for institutional players, primarily due to issues around managing wallets and the private keys that control them. Private keys can be lost, stolen or hacked, resulting in the loss of digital assets controlled by those key.

Big financial institutions in particular need to carefully plan for cybersecurity at all levels by considering the opportunity of differentiation through advanced cybersecurity practices.

Whether your data is stored in an always-available **hot wallet** or it is a digital asset sitting in **frozen storage**, security is a top priority. Large-data breaches and hacks can result in costly fines, devaluation of brand reputation, and huge revenue loss, leading organizations to ask a critical security question:

**How can we ensure that our digital assets are fully protected from both external and internal threats?**

# The challenge: Securing your wallet

## Cryptocurrency

Cryptocurrency exchanges are increasingly popular today, allowing for the conversion of currency managed by a central bank into a cryptocurrency and vice versa. However, crypto-wallets can be stolen, or the owner of the cryptocurrency exchange can pass away without sharing the master encryption key for the cryptocurrency asset repository.

Similar problems can occur even if you do not own any cryptocurrencies. Apps for stores or restaurants may have their own rechargeable wallets either in your local currency value or their own points value translated from the local currency.

If something happens to their system that stores your money/points and loses them, there is almost nothing your central bank and/or local bank can do to help, as this falls outside of their system (once you have purchased the points, it is considered a completed transaction by the bank).

# The challenge: Securing your wallet

## Application-based money transfers

More and more banks are permitting people to transfer money to other banks, using their own franchised money transfer applications, without needing to know routing/account numbers for a wire transfer.

You can think of this as a 'digital asset', where the valued asset is stored in digital format and can be moved from one owner to another easily and quickly without having to involve the 'traditional' central agency.

Digital assets are not just currency but also anything digital that represents ownership of physical assets that can be owned legally, including property titles, deeds, and even intellectual property.

Bad incidents (including cyber-attacks) that happen to a system that stores these digital assets can be catastrophic if there is no other way to restore proof-of-ownership and/or the property itself.

# The IBM solution

Uniquely **trusted building blocks** for digital asset custodians, exchanges, issuance providers, and permissioned blockchains build differentiated solutions with holistic Hyper security to protect private keys, applications, and data.

Engineered for trusted computing, the platform leverages IBM® Hyper Protect Virtual Servers – an appliance solution that is designed to protect your mission-critical workloads and sensitive data from both internal and external threats. This offering provides developers with security throughout the entire development lifecycle.

- Client application images are built, signed and deployed securely with a trusted Secure Image Build process.
- Infrastructure providers will not have access to application processes and application data but can still manage images and deployments through APIs.
- Developers and auditors can validate the source used to build images at any time. A build manifest is automatically generated through the Secure Image Build process.

**Build**
applications with security

**Deploy**
workloads with trust

**Manage**
applications with simplicity

# The IBM solution

## Trusted CI/CD

Application images are securely signed, built and deployed with the Secure Image Build process. This means that no backdoor or malware can be introduced during the build and deploy process, ensuring application integrity. As a result, solution developers and auditors can confirm the application image's integrity, knowing that the securely built image contains only what is intended.

## Restricted Access

Implementing least privilege access is a common security practice – this means no one has the access to resources or data unless they absolutely need it. In this solution, infrastructure providers and cloud admins do not have access to the application data and memory. They can still manage the application through permissioned APIs, but access to the data itself is not possible.

## Image Provenance

Full transparency of the application build source is made available via a Manifest – making it easier for developers to validate that the image deployed contains the code that they intended to deploy. Auditors can use the Manifest to compare a components list against actual components that are deployed.

No cloud / system admin access

Developers can build and validate their own images

Docker images inherit security without any code changes

# The solution value

## Security

The IBM deployment environment is specially engineered for trusted computing. IBM Hyper Protect Virtual Servers are FIPS 197-compliant protected memory enclaves (up to 16TB each) that exploit the most secure commercially available hardware security modules (HSM) for encryption, hardware bound signing, and custom-built, immutable compliance workflows. Restricting administrators to white-listed REST APIs with no direct operating system or memory access and a tamper-proof secure boot ensures that the entire environment is protected from malicious insiders and outsiders. EAL 5+ rated virtual server isolation allows problematic code to be quarantined.

## Scale

– *Confidential computing that scales*

  We make our clients' innovative solutions insider-proof at enterprise scale on an easy-to-integrate, open cloud platform.

– *Future-proof with extreme security without ISV lock-in*

  Deploy open-source and ISV solutions with Secure Image Build to protected memory enclaves (up to 16TB each) and exploit FIPS 140-2 Level 4 HSM, the highest commercially available

## Hybrid Cloud Flexibility

The underlying technology of Hyper Protect Services provides secure cloud services for both on-premises and cloud deployment of mission-critical workloads. This means you can build once and have the flexibility to deploy anywhere, giving you the same trusted security, availability, and reliability you expect from IBM. Based on your individual needs per workload (resources, time, cost, etc.), you can choose to develop cloud-native both in the private cloud, public cloud, or a combination of the two.

You can read more about the highest security provided by IBM LinuxONE in the IBM Redbook® Maximizing Security with LinuxONE.

# Learn more

For more information, visit
Hyper Protect Virtual Servers.

Get more information about how to maintain and use the product.

Visit IBM Knowledge Center

Financing Available: IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. For more information, visit: ibm.com/financing.

IT Infrastructure, New Orchard Road Armonk, NY 10504.
Produced in the United States of America, November 2020.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.