

# Protect Digital Wallets And Cryptocurrency Transaction Data

## Background

A leading global payment platform born in the heart of Silicon Valley, this company has grown its business model from simple financial services to various business, consumer, and peer-to-peer offerings. Recently, the platform added crypto finance features to purchase, sell, and hold popular cryptocurrencies and digital assets. Blockchain elements were built into the platform using a propriety digital asset security microservice.

*“We tried to protect our microservice using secure enclaves but discovered how hard it is. Anjuna enabled the protection of our digital asset security microservice quickly and easily—without requiring any changes to our application. Customers trust knowing their digital wallets are kept isolated and secure on AWS.”*

- CTO, Cryptocurrency Platform



## Challenges:

A cryptocurrency platform needs to protect customer digital wallet keys held in a proprietary blockchain microservice.

## Key Result:

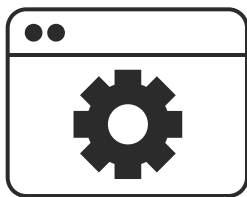
Anjuna Confidential Computing software secures cryptographic keys, transactions, and digital assets in the cloud without significant investments in staff and resources.

## Challenges

The payment platform needed to secure its proprietary multi-party computing (MPC) key management microservice to eliminate unauthorized access to its customers' digital wallets in the cloud. The microservice itself is not secure by default because it stores the cryptographic keys in memory as plaintext. Knowing the keys are vulnerable and susceptible to attack, the platform attempted to leverage the cloud provider's secure enclave technology to secure their microservice but soon discovered it was too complex to do-it-yourself (DIY) and the effort required re-architecting the SaaS application.

## Environment

The company uses AWS for its platform. In conjunction with its commitment to open-source, multi-cloud, and hybrid support, the company sought the flexibility and scalability of AWS Nitro Enclave technology to support its cryptocurrencies and digital assets services. The company also sought to expand to a multi-cloud environment to deliver high availability of its services to customers with the highest level of security.



**CRYPTOCURRENCY  
PLATFORM**



**BLOCKCHAIN KEY  
MANAGEMENT MICROSERVICE**



**AWS WITH NITRO ENCLAVES**

## Solution

After realizing it was too difficult to deploy Confidential Computing on their own, the company turned to Anjuna Security. Anjuna® Confidential Computing software quickly enables the secure enclave technology available on AWS with no recoding required. With the click of a button, Anjuna ensures that insiders, third-party cloud admins, and bad actors have no access to the private data of cryptocurrency transactions and digital assets.



## Results

Anjuna Confidential Computing software hardened the proprietary MPC key management microservice ensuring digital currency transactions on AWS are always encrypted in memory. Now, platform customers trust their digital wallets are fully secure and can leverage the platform with total confidence. Anjuna facilitated simple and rapid use of AWS Nitro Enclave technology to deliver advanced data protection across the entire cloud environment.

## About Anjuna

Anjuna Security makes the public cloud secure for business. Software from Anjuna Security effortlessly enables enterprises to safely run even their most sensitive workloads in the public cloud. Unlike complex perimeter security solutions easily breached by insiders and malicious code, Anjuna leverages the strongest hardware-based secure computing technologies available to make the public cloud the safest computing resource available anywhere.

[anjuna.io](https://anjuna.io) | [info@anjuna.io](mailto:info@anjuna.io) | 650-501-0240