

## DIA Leverages IBM Cloud and Confidential Computing to Help Secure its Decentralized Financial Information Platform

IBM Cloud confidential computing capabilities are designed to protect mission-critical decentralized finance (DeFi) data and applications in a cloud environment

ARMONK, N.Y. and ZUG, Switzerland, Jan. 26, 2021 /[PRNewswire](#)/ -- IBM (NYSE: [IBM](#)) and [DIA](#) announced today that DIA migrated its platform to [IBM Cloud](#) and is leveraging [IBM Cloud Hyper Protect Services](#) to manage how financial data is sourced, stored, processed and published. IBM Cloud Hyper Protect Services is a hybrid cloud offering designed to deliver sophisticated encryption capabilities to help secure highly sensitive data, which is especially important in the age of hybrid cloud. The migration of DIA's platform to a cloud environment backed by IBM Cloud [confidential computing](#) capabilities is designed to protect data and applications from potential malicious inside and external attacks.

DIA is located in Crypto Valley in Zug, Switzerland and is an open-source financial information platform that incentivizes the sourcing and validation of data and provides the data via traditional APIs as well as oracles. Oracles are the third-party trust mechanisms that allow smart contracts to receive data from sources outside of the blockchain.

### **Data security is key for success of the fast-growing decentralized finance space**

DeFi is an emerging area of digital finance that leverages blockchain-based smart contracts to execute and validate transactions, rather than relying on centralized financial institutions. As the industry grows, transparent data sources and oracles become critical to its reliability and success. Data sources that can be compromised and provide little transparency can lead malicious actors to manipulate attacks on DeFi platforms. To help mitigate this risk, DIA is leveraging the IBM Cloud – the industry's most secure and open public cloud for business.

### **IBM Cloud Hyper Protect Services help enable protection and privacy of data infrastructure**

Using IBM Cloud Hyper Protect Services, DIA can help provide technical assurance to its clients and users that their workloads are secured by protecting backend infrastructure against attacks on hardware, servers, applications and data layers. By taking advantage of 'Keep Your Own Key' (KYOK)<sup>1</sup> and confidential computing capabilities delivered via hybrid cloud capabilities from IBM, DIA can protect data with complete authority for their data and workloads.

IBM Cloud Hyper Protect Services provide confidential computing capabilities designed to enable data integrity and confidentiality for current and future workloads within hybrid cloud environments by employing isolation and encryption in security-rich enclaves to run cloud software.

This concept allows the platform's users to retain sole access to their crypto keys – meaning not even IBM can access them - and helps mitigate the risk of malicious actors viewing or modifying the confidential data. Built on IBM LinuxONE, by using IBM Cloud Hyper Protect Services, DIA has access to the highest level of security offered commercially by any cloud provider in the industry for cryptographic modules.<sup>2</sup>

"IBM Cloud Hyper Protect Services, confidential computing capabilities and IBM LinuxONE enable us to help implement a high security standard in the oracle landscape," says *Samuel Brack Co-Founder and CTO at DIA*. "Being able to assure that no third party can view or manipulate our off-chain computing operations effectively protects DIA and its users from potential malicious inside and outside attacks."

"As reliance on data grows, especially in the era of hybrid cloud, the need for cutting-edge security to protect digital assets becomes even more critical," said Hillery Hunter, IBM Fellow, VP & CTO, IBM Cloud. "On its mission to source and validate financial data, DIA's move toward a confidential computing environment bolsters security for all existing participants within its ecosystem. Now, DIA can work with clients in highly regulated industries and address their higher demand for confidentiality as they access their open source financial information platform."

DIA continues to explore opportunities to increase security, scalability and compliance of data delivery for both institutional and DeFi actors to help grow the ecosystem and to further increase trust in the still nascent DeFi industry.

## **About DIA**

[DIA](#) (Decentralised Information Asset) is an open-source, financial information platform that utilises crypto economic incentives to source and validate data. Market actors can supply, share and use financial and digital asset data.

About IBM Cloud: <https://www.ibm.com/cloud>

<sup>1</sup> Encryption keys and cryptographic operations are protected with highest level certified HSM - with Hyper Protect Crypto services: FIPS 140-2 Level 4.

<sup>2</sup> Based on IBM Hyper Protect Crypto Service, the only public-cloud enabled FIPS 140-2 Level 4-certified Hardware Security Module (HSM). FIPS 140-2 Security Level 4 provides the highest level of security defined in this standard. At this security level, the physical security mechanisms provide a comprehensive envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.

Contact:

Kate Gazzillo

[kate.gazzillo@ibm.com](mailto:kate.gazzillo@ibm.com)

SOURCE IBM

---