2.3.4.2.1 Data-At-Rest

Return to State of Data Taxonomy

Overview

Return to Top

Data-at-Rest refers to all data in computer storage. It excludes data while it is moving across or within a network and it excludes data that is temporarily residing in computer memory. Data-at-Rest refers to data that is actively being accessed within the computer storage, data that is archived (i.e., backups), or reference data that change rarely or never.

Here are some specific, traditional examples of Data-at-Rest:

- Data in a DIDO (i.e., Blockchain, Distributed Ledger Technology (DLT), Directed Acyclic Graph (DAG), etc.)
- Data on Servers
- Corporate data stored on the hard drives of local computers including Desktops, Notebooks, and Mobile Devices
- Data on an external backup medium including Archival Nodes
- Data stored on Storage Area Network (SAN) devices
- Data on offsite Cloud Storage service providers (i.e., Google, Dropbox, Apple, Microsoft, etc.)

Businesses, government agencies, and other institutions are concerned about the ever-present threat posed by hackers to data at rest. In order to keep data at rest from being accessed, stolen, or altered by unauthorized people, security measures such as data encryption and hierarchical password protection are commonly used. For some types of data, specific security measures are mandated by law.

DIDO Specifics

Return to Top

Within DIDOs, the **Data-At-Rest** refers to data actually residing on the Nodes in the Blockchain, Distributed Ledger Technology (DLT), Directed Acyclic Graph (DAG), InterPlanetary File System (IPFS), etc. However, not all **Nodes** have the same data. For example, a Pruned Node has less data than an Archival Node. An Archival Node has more data than a Lightweight Node (Wallet). Regardless of the specific data or the quantity of data, once it is distributed onto the **nodes** it is classified as storage.

Within Ethereum, data at rest is labeled Storage within Solidity and represents two 32 byte values. One represents the Key for the Storage, while the other represents the data value associated with the **key**. As a general rule, the **key** value is an address within the Node Network.

Within a DIDO, **Data-At-Rest** is generally physically available to anyone having access to the **Node**. Depending on the Network Access Control, the risk can vary. In a Private Network there is obviously less risk than there is a Public Network, however, this depends on the Securability of every Node in the Node Network.

It is best to assume there is

- No **Physical Security** - Unless the DIDO is completely locked down with a few well physically fortified **Nodes**, there is no **Physical Security**. If they are locked down, how distributed is the system?
- No **Platform Security** - DIDOs are all about the data and if anyone gains access to the machines there is no **Platform** security other than the encryption of the data. No matter what is done on the **platform**, the data can be accessed by other platforms that may be compromised.
- No **Application Security** - DIDOs are all about the data and if anyone gains access to the machines there is no **Application** security other than the encryption of the data. No matter what is within the **application**, the data can be accessed by other platforms that may be compromised.
- No **Culture Security** - Unless a DIDO is **Permissioned** and **Private** network, there is no way to rely on cultural security.

Cryptocurrencies, when viewed as a surrogate for DIDOs in general, have had a fair share of suspicion from governments including: India, China, the US, and Europe[1)].

> *Until a few years ago, Bitcoin was touted as the underground currency that even the world's leading intelligence agencies won't be able to track — but that may not really be the case. Examples from as far back as 2015, when the creator of the Bitcoin market called the 'Silk Road' was sentenced to life in prison for facilitating the sale of $1 billion in illegal drugs, show otherwise. Investigators can still follow the money. Even the most private of cryptocurrencies like Monero, DASH, and Verge are traceable to a certain degree. This is because of the very nature of blockchain. Every single transaction is recorded and kept on a ledger — and that ledger is accessible to everyone.*

As evidence of the non-anonymous nature of Cryptocurrencies, the United States just filed a Civil Action suite to return $150M in embezzled funds from Sony by tracking money to Bitcoin[2)].

> *The United States took action in federal court today to protect and ultimately return more than $154 million in funds that were allegedly stolen from a subsidiary of Tokyo-based Sony Group Corporation and then seized by law enforcement during the FBI's investigation of the theft. The United States filed a civil forfeiture complaint in the Southern District of California to protect Sony's interest in the property, which an employee allegedly embezzled in May 2021 and converted to more than 3,879 Bitcoins valued today at more than $180 million. Those funds were seized by law enforcement on December 1, 2021, based on the FBI's investigation. According to the government's complaint, Rei Ishii, an employee of Sony Life Insurance Company Ltd. ("Sony Life") in Tokyo, allegedly diverted the $154 million when the company attempted to transfer funds between its financial accounts. Ishii allegedly did this by falsifying transaction instructions, which caused the funds to be transferred to an account that Ishii controlled at a bank in La Jolla, California. Ishii then quickly converted the funds to Bitcoin cryptocurrency, the complaint said.*

1)

Madana Prathap, Business Insider India, 24 December 2021, Accessed: 5 January 2021, https://www.businessinsider.in/investment/news/bitcoin-does-not-make-payments-anonymous-just-really-hard-to-trace/articleshow/85068905.cms

2)

United States Department of Justice, U.S. Attorney's Office, Southern District of California, United States Files Civil Action to Return $150 Million in Embezzled Funds to Sony; FBI Tracks Money to Bitcoin, 20 December 2021, Accessed: 5 January 2022, https://www.justice.gov/usao-sdca/pr/united-states-files-civil-action-return-150-million-embezzled-funds-sony-fbi-tracks