

1.2 Purpose

[return to Introduction](#)

The goals of a [Reference Architecture \(RA\)](#) as expressed in this paper are derived from the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD/NII)¹⁾, which are:

- Provide a common language for the various [stakeholders](#)
- Provide consistent implementation of technology to solve problems
- Support [validation](#) and comparison of implementations
- Encourage adherence to common standards, specifications, and patterns

Achieving these goals will enhance the likelihood that DIDOs and networks will be engineered correctly. DIDOs are intended to cover the entirety of distributed computing, including improvements in data storage and computing that are now used to support DIDO processes, but were not considered in Nakamoto's paper²⁾ and the consequent highly successful launch of [Bitcoin cryptocurrency](#). Nakamoto's paper proposed a "[ledger](#)" for storing data and a collection of transactions, captured in a block. Blocks of transactions are verified and validated using a [Consensus Algorithm](#). Bitcoin relies on [Proof-of-Work \(PoW\)](#) consensus. This solution, although usable, has proven to be expensive, making widespread ubiquitous adoption difficult³⁾. Other implementations such as [Ethereum](#) were built upon the Bitcoin [blockchain](#) concept, which replaced the costly PoW with [Proof of Stake \(PoS\)](#). The DIDO RA is extensible to evolving and emerging blockchain technologies. For example, Boyen⁴⁾ notes that:

*Our blockchain-free proposal shifts onto the transactions themselves the task of affirming prior transactions. Verification no longer results in a chain of transactions blocks, but in a lean graph comprised only of transactions...*⁵⁾

The DIDO RA concerns distributed, [Peer-to-Peer \(P2P\)](#) computing including blockchains and cryptocurrencies, but also covers domains that have little or nothing to do with currencies. For example, DIDOs can be blockchains, [distributed ledgers](#), or graphs. Blockchains may use any consensus algorithm such as PoW or PoS. Cryptocurrencies are used as a placeholder for any of the other domains that can be supported using DIDO: supply chains, government records, scientific data, medical records, escrows, swaps, etc.

The explosion in cryptocurrencies is well known and documented. An example is presented extremely well in Figure 1 for the animation provided by Jeff Desjardins⁶⁾.

Note "ICO funds raised" went from zero in 2014 to about \$6.5 billion in November 2017.



Figure 1: The explosive growth of [Initial Coin Offering \(ICO\)](#) over four years

CoinDesk used data from CoinGeko, see Figure