Digital Asset: Digitally stored content or online account owned by an individual.

Encode: Process of putting a sequence of characters into a specialized format for efficient transmission or storage

Decode: Takes encoded, raw, unreadable files and converts them back into human readable format.

ASCII: American Standard Code for Information Interchange

Hexadecimal: More concise and human readable representation of binary

Base64: Encoding scheme meant to represent data as numbers in a string format

Why do we need POE (Proof of Existence)

Before trying to use this for ourselves, here's a few quick ideas over why you might even want to to do this in the first place.
Helps you demonstrate data ownership without revealing actual data.
This is useful for things like copyrighted material or patents.
Checks for the integrity of your digital asset. Any proof of existence will recognize your document FOREVER.
Even the slightest difference will be recognized allowing you to be sure your asset hasn't changed.
Provides document Time stamping. You can use this to prove certain information existed at a certain time.
This can be useful in cases where you want to prove who was the original owner of the document.
Certifies the existence of the document without the need for a central authority.
Similar to many blockchain concepts this decentralized proof can't be erased or modified by anyone

POE Algorithms

There are a different of algorithms to demonstrate Proof of Existence. The two we have chosen to focus on here are SHA256 and MD5.
They both serve the same purpose. They're a way to hash a digital asset so it can be embedded in a transaction in the blockchain. This allows people to verify that a document existed at a certain point in time.

SHA256

This is an algorithm we've seen already in several different parts of the Bitcoin network. It's used in mining as part of the proof of work algorithm.
It's also used to create secured bitcoin addresses.
SHA256 stands for Secure Hash Algorithm. It is a one-way hashing function that takes in any piece of data and produces a unique hash.
This is the algorithm POEX uses to secure their digital documents.

MD5

Next, the MD5 algorithm is a hash function that takes in a String input and

produces a 128-bit hash value. This value is usually shown as a 32-character hexadecimal number that humans can read.

Goals of POE Algorithms

While each method does things a bit differently, the important thing to remember is their purpose.

They hash digital assets to hide the actual content. Once the hashed data is embedded in a transaction in the blockchain, the existence of that transaction in the blockchain proves that the document existed at the time the transaction got included into a block.

Proof of Existence: The concept that publicly proving and authenticating any digital asset on the blockchain by verifying its hash.

Created by Mohamed Abdel Nasser