Hey there! The AWS workspace will be undergoing maintenance and will be unavailable on Tuesday, Jan 11th, 2021 from 3:00pm to 4:00pm Pacific Daylight Time (UTC-7:00). We apologize for any inconvenience this may cause.

Mentor Help

Ask a mentor on our Q&A platform

POE Algorithms

There are a different of algorithms to demonstrate Proof of Existence. The two focus on here are SHA256 and MD5.

They both serve the same purpose. They're a way to hash a digital asset so it ca transaction in the blockchain. This allows people to verify that a document exis time.

SHA256

This is an algorithm we've seen already in several different parts of the Bitcoin 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 tha 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 proc value. This value is usually shown as a 32-character hexadecimal number that h

Goals of POE Algorithms

While each method does things a bit differently, the important thing to remem

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

Wrap Up

To recap, in this section we covered:

- **Proof of Existence:** The concept that publicly proving and authenticating blockchain by verifying its hash.
- We saw a demo using the POEX online document notarization service.
- Lastly, we discussed different algorithms commonly used for proof of exis and MD5.