Proof of Evolution

Proof of evolution (PoE) is a model of verifying that a node within the Fabric processed a Nuance as requested. The verification work serves as a useful way to provide security to the Fabric.Businesses that already have their own blockchain running will be able to seamlessly integrate into the wider blockchain network, while still using their own private blockchains and consensus algorithms.

Nodes within the Fabric are not fully replicated state machines. Each node can have its own set of capabilities to perform work on behalf of a Nuance. Thought has devised a method to determine if a node has indeed performed the processing of Nuance on behalf of another node, i.e. POE.

Using a fully homomorphic and quantum computing proof encryption scheme, where E is the encryption function and D is the decryption function, for a given Nuance with data d, the Nuance is defined as a sequential set of functions F that each are a capability on a foreign node or behavior within the Nuance whose input is d or the output of the previous function in the set. It can then be said that if F is the arbitrary set of functions { A, B, C } and B is a capability on a foreign node within the Fabric, when processed by a foreign node, the Nuance with data d, will be processed in the following manner:

$A(d) = O1 \rightarrow B(O1) = O2 \rightarrow C(O2) = T$

where T is the transformed data of the Nuance, using a fully homomorphic encryption scheme, it can be said that if d is encrypted, the data of the Nuance is E(d) with transformed data T.

To verify that the foreign node is honest about its processing, it will be asked to hand back a mathematical proof P such that $P \equiv F$. The original sending node and all other Fabric members can use this proof to check that $P(d) \equiv D(T)$. The proof is distributed amongst nodes in a random order fashion with each node processing an encrypted portion of the proof and no node is aware of which node owns which piece of the proof. In addition, if the hashes of d and D(T) are the same, then it can be shown that no transformations were applied to the Nuances’ data.

Revision #2

Created Mon, Dec 11, 2023 2:53 AM by Aaron Malone

Updated Wed, Feb 21, 2024 8:36 PM by Andrew