Log Integrity Verification Algorithm

Andrew Sutton Reza Samavi

May 18, 2017

Data: Event header graph: hg_i, event body graph: bg_i, signature graph: sg_i
Result: Boolean verification value: v_i

$Triples \leftarrow (\text{extractTriples}(hg_i) \cup \text{extractTriples}(bg_i) \cup \text{extractTriples}(sg_i))$;

$H \leftarrow \prod_{j=1}^{|Triples|} h(t_j \in Triples) mod(p)$;

$URI \leftarrow$ Query block graphs for H (Listing 1) ;

if $URI \neq \emptyset$ **then**

  $v_i \leftarrow \text{verifySignature}(sg_i, hg_i, bg_i)$;

else

  $v_i \leftarrow$ false ;

end

return v_i

Algorithm 1: Verification algorithm

```
1  SELECT ?g WHERE {
2    GRAPH ?g { ?s blo:scriptPubkeyBitcoinTransactionOutput
       @integrityProofDigest } }
```

Listing 1: SPARQL query for finding block payload