AN INTERNET OF BLOCK THINGS

Phillip H. Griffin
Griffin Information Security, United States

Abstract *– This paper defines extensible, distributed blocks of hash-linked data constructed using the Cryptographic Message Syntax (CMS) SignedData message. The described SignedData blockchain allows each block to reside in a different physical location on the Internet of Things (IoT). Each signed, time-stamped block content can combine data from multiple locations that are 'detached' from and remote to its block header. Two types of SignedData sidechains are described, ephemeral and fixed. Ephemeral sidechains can be added to any block at any time without affecting the integrity of the blockchain. They can also be removed without disruption, making them ideal for use in applications that must manage limited storage capacity or comply with right-to-be-forgotten privacy regulations. A simple blockchain example is presented using CMS SignedData for its block content and headers. This example is then extended to create doubly-linked blockchains and blockchain grids.*

Keywords – ASN.1, Blockchain, IoT, Sidechain, SignedData