PRIVACY PRESERVING BLOCKCHAINS

Phillip H. Griffin
Griffin Information Security, United States

Abstract *– This paper describes blockchains constructed using the SignedData Cryptographic Message Syntax (CMS) data type. SignedData serves as a container for the block header and data content components of the blockchain blocks. The described blockchain and each of its blocks can be distributed, allowing each block to be managed in a different security zone and to reside at a different physical location on the internet of things (IoT). SignedData blockchains can be embedded in the records of other storage system types, such as blockchain, distributed ledger, and database systems. An extended hash pointer that links the series of SignedData blocks together, is applied to create sidechains that can be added to or deleted from any block to address privacy concerns such as right-to-be-forgotten, and to link SigncryptedData and other object types to a SignedData block. A tokenization manifest is presented that supports 'off-chain', field level data confidentiality of block content. When these techniques are combined with digital signatures, confidentiality, data integrity, and origin authenticity can be provided to entire blocks, transactions, or transaction fields within a block.*

Keywords – ASN.1, Blockchain, SigncryptedData, SignedData, Tokenization