INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

FOCUS GROUP ON APPLICATION OF DISTRIBUTED LEDGER TECHNOLOGY

DLT-I-048

Question(s): WG1 Bern, 5-7 February 2018

INPUT DOCUMENT

Source: Corporation for National Research Initiatives (CNRI)

Title: Definition of "block" as a "Digital Entity"

Purpose: Discussion

Contact: Patrice Ann Lyons
CNRI
United States of America

Tel: +1-703-620-8990
E-mail: palyons@bellatlantic.net

Keywords: FG DLT; distributed ledger technology;

Abstract: This Contribution proposes that a "block" be defined as a "digital entity" as specified in Recommendation ITU-T X.1255 for purposes of the Base Document on definition of terms and definitions for DLT

Proposal

There is no apparent reason to deviate from the definition of **Digital Entity** as specified in Recommendation ITU-T X.1255 (9/2013). It is important to adopt neutral terminology in order to avoid confusion in practice. In addition to "block," there have been many different words, such as "container," "cryptolope," "package" or more generally "digital object," that have been used over the last two decades to identify the concept of a logical entity or data structure that may embody digital information subject to various rights or interests, or in which there is value, that, when processed, may manifest this information incorporated in this form of expression.

A block is intrinsically a sequence of bits, or a set of sequences of bits, that is a machine-independent data structure consisting of one or more elements in digital form capable of being parsed by different information systems, and having as an essential element a unique identifier. A **block** may be connected with one or more other blocks in a specific way to form what is sometimes referred to informally as a **blockchain**. Thus, a block and/or a blockchain meet the definition of a Digital Entity for purposes of X.1255. A blockchain may also be referred to as a composite Digital Entity, namely a Digital Entity that consists of multiple Digital Entities.

A Digital Entity may be mutable or immutable. A block may be immutable, but a blockchain (or "**Distributed Ledger"**) is intrinsically mutable.

What is unique to a specific Distributed Ledger, which in itself may be deemed a blockchain, is the particular way in which the blocks are connected, including the processes by which new blocks are added along with the choice of connection points and technical method of chaining. There are literally an infinite number of choices to select from, including the use of encryption in various ways, and, at the other extreme, those that treat the composite Digital Entity as a set or collection of possibly unrelated Digital Entities.

A blockchain must be identified in order to know to what existing Digital Entity a new block is being added. Further, each block in the blockchain must be separately identified to interpret and validate it, including obtaining the relevant provenance information and perhaps *date-time-stamp*

associated with its inclusion in the blockchain. Considerations for power usage and latency would suggest that efficient alternate means of enabling trust be considered and/or specified. These alternatives will ultimately depend on the use of trusted identifier resolution systems with built-in security that enable one to identify, locate and validate a particular block or blockchain with high confidence, or to do the same for any other Digital Entity created by a different set of rules.

A background reading list in support of this proposal is given in **Annex A** to this Contribution.

ANNEX A

Baseline distributed ledger technology terms and definitions:

Some Background Reading on Proposal

Kahn, Robert E., “The organization of computer resources into a packet radio network,” Advanced Research Projects Agency, National Computer Conference, at 175, https://www.computer.org/csdl/proceedings/afips/1975/5083/00/50830177.pdf

Kahn, Robert E., Vinton G. Cerf, "An Open Architecture For a Digital Library System and a Plan For Its Development," The Digital Library Project Volume I: The World of Knowbots, (DRAFT) March 1988, http://hdl.handle.net/4263537/2091

Kahn, Robert E., Robert Wilensky, "A Framework for Distributed Digital Object Services," *International Journal on Digital Libraries*, (2006) 6(2): 115-123, https://www.doi.org/topics/2006_05_02_Kahn_Framework.pdf (First published by the authors May 13, 1995, "A Framework for Distributed Digital Object Services", http://hdl.handle.net/4263537/5001).

Managing Access to Digital Information, Cross-Industry Working Team, May 1997, http://www.xiwt.org/documents/ManagAccess-1.pdf.

Kahn, Robert E., Patrice A. Lyons, “Representing Value as Digital Objects," *Journal on Telecommunications & High Technology Law*, Vol. 5, Issue 1, 189 (2006) http://www.jthtl.org/content/articles/V5I1/JTHTLv5i1_KahnLyons.PDF.

A patent application based in part on the ideas expressed in this article was filed by CNRI, and later abandoned when the claims were rejected by the United States Patent & Trademark Office as covered by the now expired, CNRI Patent No. 6,135,646, System for Uniquely and Persistently Identifying, Managing, and Tracking Digital Objects). The application, titled Authenticating and using digital objects, specified that the technology may be applied in managing, inter alia, the issuance and authentication of financial instruments (US 20030233570 A1, http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220030233570%22.PGNR.&OS=DN/20030233570&RS=DN/20030233570)

_____