Question 14/17 – Distributed ledger technology (DLT) security

(Continuation of Question 14/17)

1 Motivation

Distributed Ledger Technologies (DLT), the most prominent implementation of which is Blockchain, are a new type of secure ledgers that is shared, replicated, and synchronized in a distributed. Data in distributed ledgers is controlled by multiple parties.

As a specific distributed database technology, DLT are inherently resistant to modification of the data - once recorded, the data in a block cannot be altered retroactively. This prominent feature of DLT is well known after the success of its early digital cryptocurrency applications known as Bitcoin.

DLT has become one of disruptive technologies with great potential to change our economy, culture, and society. DLT enables innovative financial/non-financial decentralized applications that eliminate the need for third party intermediaries. DLT will introduce new data management infrastructure that will accelerate a services revolution in industries (for example, banking and finance, government, healthcare, and super logistics) based on telecommunications.

Distributed ledger technologies will have a profound impact for telecom users and industries including telecom service providers.

There is a need for identifying the roles and responsibilities of telecom users, operators, and service providers with regards to security aspects in the DLT environment.

Standardization of the best comprehensive security solutions is vital for DLT that has many use cases for every sector including telecom industry. Due to some specific characteristics of the DLT, providing security becomes an especially challenging task that deserves study.

Recommendations under responsibility of this Question as of 7 January 2022: X.1400, X.1401, X.1402, X.1403, X.1404, X.1405, X.1406, X.1407 and X.1408.

Texts under development as of 7 January 2022: X.sa-dsm, X.sc-dlt, X.srscm-dlt, X.ss-dlt, and TR.qs-dlt.

2 Question

Study items to be considered include, but are not limited to:

a) How should security aspects (e.g., architecture and subsystems) be identified and defined based on the foundations (terms and definitions, concepts and taxonomy, use cases) in a DLT environment?

b) How should threats and vulnerabilities in applications and services based on DLT be handled?

c) What are the security requirements for mitigating the threats in a DLT environment?

d) What are security technologies to support applications and services based on DLT?

e) How should secure interconnectivity between entities in a DLT environment be kept and maintained?

f) What security techniques, mechanisms and protocols are needed for applications and services based on DLT?

g) What are globally agreeable security solutions for applications and services based on DLT, which are based on telecommunication/ICT networks?

h) What are best practices or guidelines of security for applications and services based on DLT?

i) What PII (Personally Identifiable Information) protection and information security management are needed for applications and services based on DLT?

j) How can DLT be used to support security?

k) How can the DLT security be assessed, evaluated, and assured?

l) With what stakeholders should SG17 collaborate?

3 Tasks

Tasks include, but are not limited to:

a) Perform a gap analysis on ongoing security relevant work in other organizations for distributed ledger technologies.

b) Study further to define security aspects of applications and services based on DLT, which are based on telecommunication/ICT networks.

c) Study foundations such as terms and definitions, concepts, and taxonomy, and use cases that are related to security and PII protection in DLT networks.

d) Study and identify security issues and threats in applications and services based on DLT.

e) Study and develop security mechanisms, protocols and technologies for applications and services based on DLT.

f) Study and develop secure interconnectivity mechanisms for applications and services based on DLT.

g) Study and identify PII protection issues and threats in applications and services based on DLT.

h) Study and develop information management system for entities providing applications and services based on DLT.

i) Study and develop guidance on DLT usage to support security.

j) Study and develop guidance for assessment, evaluation, and assurance on DLT security.

k) Produce a set of Recommendations to provide comprehensive security solutions for DLT based applications and services.

An up-to-date status of work under this Question is contained in the SG 17 work programme at https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=17&sg=17.

4 Relationships

WSIS Action Lines:

– C5

Sustainable Development Goals:

– 8 (Decent Work and Economic Growth)

– 9 (Industry, Innovation and Infrastructure)

– 11 (Sustainable Cities and Communities)

Recommendations:

– X-series and others related to security

Questions:

– ITU-T Qs 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17 and 15/17

Study Groups:

– ITU-T SGs 5, 11, 13, 16 and 20

Standardization bodies:

– ISO TC 307; ISO/IEC JTC 1/SC 27

Other bodies:

– GSMA; W3C; IEEE; UNECE (UN Economic Commission for Europe); FIGI; ATIS; CCSA; TIA; TTA; TTC