

Recommendation

ITU-T X.1412 (04/2023)

SERIES X: Data networks, open system communications and security

Secure applications and services (2) – Distributed ledger technology (DLT) security

Security requirements for smart contract management based on the distributed ledger technology

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (1)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (2)	X.1300-X.1499
Emergency communications	X.1300-X.1309
Ubiquitous sensor network security	X.1310-X.1319
Smart grid security	X.1330-X.1339
Certified mail	X.1340-X.1349
Internet of things (IoT) security	X.1350-X.1369
Intelligent transportation system (ITS) security	X.1370-X.1399
Distributed ledger technology (DLT) security	X.1400-X.1429
Application Security (2)	X.1450-X.1459
Web security (2)	X.1470-X.1489
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
IMT-2020 SECURITY	X.1800-X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1412

Security requirements for smart contract management based on the distributed ledger technology

Summary

Recommendation ITU-T X.1412 analyses security threats and challenges and provides security requirements for smart contract management in distributed ledger technology (DLT) systems. As smart contracts are widely used in DLT systems, they are faced with a lot of security threats and challenges.

As such this Recommendation can be used by smart contract designers, developers, and managers to manage smart contracts, including design and development, compilation and deployment, invocation and execution, maintenance and management in DLT systems. This Recommendation does not deal with the security issues of wallets or distributed applications related to smart contracts.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1412	2023-04-29	17	11.1002/1000/15545

Keywords

Blockchain, distributed ledger technology, security requirements, smart contract.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2023

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation	2
4 Abbreviations and acronyms	2
5 Conventions	2
6 Security threats of smart contract management.....	2
7 Security framework of smart contract management	4
8 Security requirements for smart contract management.....	4
8.1 Security requirements in the design and development phase	4
8.2 Security requirements in the compilation and deployment phase.....	6
8.3 Security requirements in the invocation and execution phase.....	7
8.4 Security requirements in the maintenance and management phase	8
Appendix I – Smart contract weakness classification	9
Bibliography	15

Recommendation ITU-T X.1412

Security requirements for smart contract management based on the distributed ledger technology

1 Scope

This Recommendation analyses the security threats and challenges of the smart contract in distributed ledger technology (DLT) systems and specifies the security requirements for smart contract management.

This Recommendation can be referred to in smart contract lifecycle management as a starting point for security. This Recommendation does not deal with the security issues of wallets or distributed applications related to smart contracts.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1401] Recommendation ITU-T X.1401 (2019), *Security threats of distributed ledger technology*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 block [b-ITU-T X.1400]: Individual data unit of a blockchain (see clause 3.1.2), composed of a collection of transactions and a block header.

3.1.2 blockchain [b-ITU-T X.1400]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.3 blockchain system [b-ITU-T X.1400]: A system that implements a blockchain.

3.1.4 consensus [b-ITU-T X.1400]: Agreement that a set of transactions is valid.

3.1.5 consensus mechanism [b-ITU-T X.1400]: Rules and procedures by which consensus is reached.

3.1.6 distributed ledger [b-ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.7 distributed ledger technology (DLT) [b-ITU-T X.1400]: Technology that enables the operation and use of distributed ledgers.

3.1.8 DLT system [b-ITU-T X.1400]: A system that implements a distributed ledger.

3.1.9 on-chain [b-ITU-T X.1400]: Located, performed, or run inside a blockchain system.

3.1.10 off-chain [b-ITU-T X.1400]: Related to a blockchain system, but located, performed, or run outside that blockchain system.

3.1.11 personally identifiable information (PII) [b-ITU-T X.1252]: Any information:

- a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains;
- b) from which identification or contact information of an individual person can be derived; or
- c) that is or can be linked to a natural person directly or indirectly.

3.1.12 public DLT system [b-ITU-T X.1400]: A distributed ledger technology (DLT) system which is accessible to the public for use.

3.1.13 private DLT system [b-ITU-T X.1400]: A distributed ledger technology (DLT) system which is accessible for use only to a limited group of DLT users.

3.1.14 sensitive data [b-ITU-T X.1040]: Data with potentially harmful effects in the event of disclosure or misuse.

3.1.15 smart contract [b-ITU-T X.1400]: A program written on a distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated and triggered by specific conditions.

3.1.16 transaction [b-ITU-T X.1400]: Whole of the exchange of information between nodes. A transaction is uniquely identified by a transaction identifier.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPU	Central Processing Unit
DLT	Distributed Ledger Technology
DoS	Denial of Service
EVM	Ethereum Virtual Machine
PII	Personally Identifiable Information
SCSC	Smart Contract Security Challenge

5 Conventions

This Recommendation applies the following verbal forms for the expression of provisions:

- a) **"Shall"** indicates a requirement,
- b) **"Should"** indicates a recommendation,
- c) **"May"** indicates a permission,
- d) **"Can"** indicates a possibility and a capability.

6 Security threats of smart contract management

[ITU-T X.1401] categorizes the security threats to smart contracts into the following four types: timestamp dependence attack, mishandled exceptions attack, integer overflow attack, and predictable random number attack. Given below is a view of the attack method.