International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.751.3

(03/2022)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Multimedia services

Requirements for change management in distributed ledger technology (DLT)-based decentralized applications

Recommendation ITU-T F.751.3

ITU-T F-SERIES RECOMMENDATIONS

NON-TELEPHONE TELECOMMUNICATION SERVICES

TELEGRAPH SERVICE	
Operating methods for the international public telegram service	F.1–F.19
The gentex network	F.20–F.29
Message switching	F.30–F.39
The international telemessage service	F.40–F.58
The international telex service	F.59–F.89
Statistics and publications on international telegraph services	F.90–F.99
Scheduled and leased communication services	F.100–F.104
Phototelegraph service	F.105–F.109
MOBILE SERVICE	
Mobile services and multidestination satellite services	F.110–F.159
TELEMATIC SERVICES	
Public facsimile service	F.160–F.199
Teletex service	F.200–F.299
Videotex service	F.300–F.349
General provisions for telematic services	F.350–F.399
MESSAGE HANDLING SERVICES	F.400–F.499
DIRECTORY SERVICES	F.500–F.549
DOCUMENT COMMUNICATION	
Document communication	F.550–F.579
Programming communication interfaces	F.580–F.599
DATA TRANSMISSION SERVICES	F.600–F.699
MULTIMEDIA SERVICES	**F.700–F.799**
ISDN SERVICES	F.800–F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850–F.899
ACCESSIBILITY AND HUMAN FACTORS	F.900–F.999

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

Recommendation ITU-T F.751.3

Requirements for change management in distributed ledger technology (DLT)-based decentralized applications

Summary

The development of applications using distributed ledger technology (DLT) enables the creation of new business models in various sectors of the economy and it has the potential to tackle, on a large scale, important challenges for our society, due to its ability to increase trust in the relationship between stakeholders. Technical immutability is key to building trust between stakeholders. On the other hand, real life introduces practical needs to update applications with smart contracts. This document defines some recommendations to tackle changes in applications using smart contracts.

The discussion of whether DLT networks provide different levels of technical immutability is out of the scope of this Recommendation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T F.751.3	2022-03-16	16	11.1002/1000/14965

Keywords

Blockchain, change management, distributed ledger technologies.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/.

Table of Contents

Recommendation ITU-T F.751.3

Requirements for change management in distributed ledger technology (DLT)-based decentralized applications

1 Scope

This Recommendation is intended to propose requirements for change management in distributed ledger technology (DLT)-based decentralized applications considering the need for changes in the real-world environment (e.g., changes in user requirements or the need to adapt to new regulation) where the application is running or an error correction is in the code. Although a change management framework may be useful for the decentralized application as a whole, this Recommendation is focused on changes that impact deployed smart contracts. Also, the change management described aims to approach unanticipated changes, including data, data structure and business logic. This document does not include lifecycle management activities of DLT-based applications. So, it is not discussing topics like auditing, bug bunties, tests, etc.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 application governance: A subset of the stakeholders that act to ensure that the decentralized application code does exactly what it should.

3.2.2 current smart contracts: Smart contracts that contain lines of code or data that motivated a change in an application that uses smart contracts.

3.2.3 change script: A script that specifies a change in an application that uses smart contracts, e.g., deploy new contracts and change data of current smart contracts.

3.2.4 future smart contracts: Smart contracts deployed or impacted in some way during the execution of a change in an application that uses smart contracts.

3.2.5 stakeholder: Someone with an interest or concern in the decentralized application.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DeFi Decentralized Finance

DLT Distributed Ledger Technology

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Background

The development of applications using DLT enables the creation of new business models in various sectors of the economy and it has the potential to tackle, on a large scale, important challenges for our society, due to its ability to increase trust in the relationship between stakeholders. Provided that there are no successful attacks or collusion between nodes, a DLT network, decentralized and synchronized by a consensus algorithm, will grant an immutable software execution environment. It is guaranteed to the stakeholders that the execution of the on-chain code will always correspond to what was specified in the smart contract code. As Kevin Werbach [b-Wer] discusses in his article, immutability is key to build trust between stakeholders, which rules out the need to involve centralized authorities, yet it does also increase relationship issues among these stakeholders with no easy conflict resolution mechanism.

Technology alone cannot make sure that the code of the smart contract will really reflect what should be executed. For instance, an error in the code may lead its execution to mismatch the requirements that originated it. A change in the agreement of the stakeholders can also occur, for whatever reason, which may render it impossible to adapt the smart contract to the new reality.

Application governance is what ensures that the decentralized application code does exactly what it should. The act of deploying one or more smart contracts is associated with an application governance decision. Any change in a smart contract is also a change in the original decision on how to code the smart contract and must therefore represent a new decision of the same group.

Since the applications depend on the network to execute, the correct execution of the smart contracts also depends on the network governance. In some cases, especially when the permissioned networks are created to serve a specific purpose, the network's governance members can be the same members of the application governance, but this is merely a coincidence and does not necessarily occur all the time.

Actions and decisions of the governance quite often occur off-chain. The stakeholders that possess authority jointly agree on a scope that must be built and they quite often hire or delegate to an executor the development and the deployment of the smart contract. In practical terms, this delegation is rooted in the application governance's trust towards the executor.

Considering a more mature setting, application governance can occur through an automatized change management process in the DLT network itself. There are many ways to involve the members of the application governance and there are plenty of examples in both permissioned and permission-less DLT networks in how to manage group decisions. Some examples are smart contracts that require multiple signatures (multisig) to execute a transaction, voting mechanisms and governance token distribution (as common in some decentralized finance (DeFi) platforms).

This idea of having an on-chain change management process allows minimizing trust in the change executor and sharing decision-making responsibilities. In this kind of setting, less involved stakeholders could trust that the changes in the smart contract keep the original high-level decisions that led to the development of the smart contract.

Note that a change management solution does not necessarily imply a native support in the DLT platform, since it can also be implemented using smart contracts. In addition, a change management solution does not harm the technical immutability of DLT. It involves a set of trackable procedures applied in a specific period of time to change a DLT-based decentralized application.

The use of a change management framework in DLT-based decentralized applications may cause relevant impact in the overall solution. For example, the framework may demand an additional amount of computational resources to run the smart contract code, may increase complexity of smart contract code or even avoid the use of existing smart contract standards. In order to decide when to use a change management framework in a specific project, it is necessary to consider the cost and benefits involved.

7 Technical requirements for change management in DLT-based decentralized applications

This Recommendation proposes three high-level requirements for an application change process as follows. All of them should be met through on-chain development, to guarantee the predictability and trust of the process.

These requirements were grouped by three layers. The picture below presents the name and main goal of each layer. The bottom layer is very technical, related to software engineer requirements to solve the technical issue. The layers above address the relationship with the stakeholders and the application governance. All layers are detailed in the following clauses.

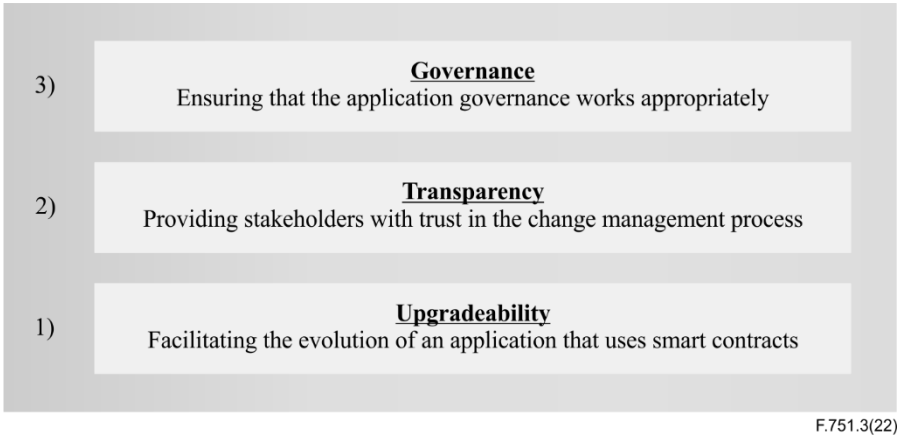

Figure 1 – The layers of requirements for change management in decentralized applications

7.1 Facilitating the evolution of an application that uses smart contracts

This requirement comprises correction of code error, the update of some business requirements, or the change of the state variables of the contracts.

To fulfil this requirement, a change management framework:

a) is required to preserve the access to the data originally used by the current smart contracts to the future smart contracts, as a way to minimize data migration;

b) in the context of a change, is required to make it feasible to alter data used by the current smart contracts in a way that is not possible without a change;

c) in the context of a change, is required to make it feasible to alter the data structure used by the current smart contracts in a way that is not possible without a change;

d) is recommended to expose an immutable way of finding the current version of the smart contracts (sometimes called "proxy contract");

e) is recommended to enable the possibility of preserving some parts of the code from the current smart contracts as non-upgradeable;

f) is recommended to preserve the quality of the smart contracts codes throughout time, even after various evolutions[1];

g) in the context of a change, is recommended to enable the application owners to make available a choice for application users to opt between staying managed by the current smart contracts, migrating to the future smart contracts or even finishing the relationship with the smart contracts (if the user can choose, it is known as "you-are-free-to-opt-out" principle).

Note that according to the intrinsic characteristics of a DLT network, data stored in transactions for the network are not to be altered. It is only possible to alter the current state of the data stored in the variables of the smart contracts. Thus, the development of this item requirement is not able to solve the issue of the right to be forgotten present in privacy laws.

7.2 Providing stakeholders with trust in the change management process

Besides meeting the first requirement, a framework that meets this requirement grants for all stakeholders the trust that the process of change management is respected. The stakeholders include the ones that do not take part in the change process themselves, but that are interested in it.

A change management framework that conforms to this requirement:

a) is recommended to establish that changes go through a life cycle, which typically includes proposal, approval, execution and conclusion or cancelling;

b) is recommended to associate the change with off-chain information that spells out its motivation and the rationale adopted for the solution;

c) is recommended to guarantee that every change is executed through an automatized change script;

d) is recommended to make a change proposal (including change script) available for analysis of the application governance before the change approval;

e) is required to prevent the execution of changes that do not go through the change process approval[2];

f) is required to provide transparency regarding which changes were proposed and what happened to these propositions;

g) is recommended to work out a system to monitor the changes in progress;

h) is recommended to enable the introduction of a time gap between the proposal and the approval or between the approval and the execution of the change, which would allow the users to take some time to decide what to do regarding the imminent application change as well as allow the development team to create an additional safety mechanism.

---

1 This is more difficult to achieve in some cases, for example, when the upgrade mechanism is implemented as an independent layer of smart contracts. There are some solutions that include specific restrictions in the current and future smart contract code due to the way that the underlying DLT is implemented (for example, how data is stored, the difference of constructor and methods, etc) [b-Pal].

2 One possible way to achieve this is including the entire changing script on-chain before the change approval. Another approach is making the hash of the changing script on-chain before the change approval, in a common practice called commit and reveal [b-Pal].

Ideally, one should start discussing the change proposition in an off-chain way, to facilitate the debate and the evaluation of the impacts. Only when the members agree on what must be proposed should a change be proposed by using the process. To associate the change with the off-chain information (as described in item 'b'), it is possible, for instance, to register in the DLT the hash that documents the motivation, discussion and evaluation of the impact of the change and, possibly, the rationale adopted for the solution. A way to make the monitoring of the changes possible is (as described in item 'f') to emit an event for each modification of change state.

7.3 Ensuring that the application governance works appropriately

This requirement aims to make sure that the correct set of stakeholders participate in the application governance and that they agree on the conformity of the smart contract. A development that meets the three requirements of this Recommendation must then have the concept of governance structure automatized, and it must be capable of deciding on changes to share the responsibility for the change.

A change management framework that conforms to this requirement:

a) is recommended to include a mechanism to aid the group's decision-making process;

b) is recommended to provide a mechanism for the creation of subgroups and delegation of votes to decide on specific changes;

c) is recommended to support the classification of changes in different levels of formality regarding deployment, which will depend on how high the change impact will be and how urgent it needs to be implemented;

d) is recommended to support the inclusion or elimination of members of the application governance;

e) is recommended to enable the participation of the governance structure since the very first deployment of the smart contracts.

Bibliography

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-Pal] Paladino, S. (2020), *The State of Smart Contract Upgrades*, OpenZeppelin. <https://blog.openzeppelin.com/the-state-of-smart-contract-upgrades/, last visited on July 2021>

[b-Wer] Werbach, K. (2018), *The Siren Song: Algorithmic Governance By Blockchain*, in After the Digital Tornado: Networks, Algorithms, Humanity. Available at SSRN. <https://ssrn.com/abstract=3578610, last visited on July 2021>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	**Non-telephone telecommunication services**
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022