ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т F.751.8 (07/2023)

СЕРИЯ F: Нетелефонные службы электросвязи

Мультимедийные службы

Техническая основа для обеспечения соответствия технологии распределенного реестра (DLT) регуляторным нормам

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ F

Нетелефонные службы электросвязи

ТЕЛЕГРАФНАЯ СЛУЖБА	F.1-F.109
Эксплуатационные методы для международной службы передачи телеграмм общего пользования	F.1-F.19
Сеть гентекс	F.20-F.29
Коммутация сообщений	F.30-F.39
Международная служба обмена сообщениями	F.40-F.58
Международная служба телекс	F.59-F.89
Статистика и публикации по международным телеграфным службам	F.90-F.99
Службы связи с работой по расписанию и с арендованными каналами	F.100-F.104
Фототелеграфная служба	F.105-F.109
ПОДВИЖНАЯ СЛУЖБА	F.110-F.159
Подвижные службы и многоадресные спутниковые службы	F.110-F.159
ТЕЛЕМАТИЧЕСКИЕ СЛУЖБЫ	F.160-F.399
Факсимильная служба общего пользования	F.160-F.199
Служба телетекс	F.200-F.299
Служба видеотекс	F.300-F.349
Общие положения для телематических служб	F.350-F.399
СЛУЖБЫ ОБРАБОТКИ СООБЩЕНИЙ	F.400-F.499
СПРАВОЧНЫЕ СЛУЖБЫ	F.500-F.549
ДОКУМЕНТАЛЬНАЯ СВЯЗЬ	F.550-F.599
Документальная связь	F.550-F.579
Программируемые интерфейсы связи	F.580-F.599
СЛУЖБЫ ПЕРЕДАЧИ ДАННЫХ	F.600-F.699
МУЛЬТИМЕДИЙНЫЕ СЛУЖБЫ	**F.700-F.799**
СЛУЖБЫ ЦСИС	F.800-F.849
УНИВЕРСАЛЬНАЯ ПЕРСОНАЛЬНАЯ ЭЛЕКТРОСВЯЗЬ	F.850-F.899
ДОСТУПНОСТЬ И ЧЕЛОВЕЧЕСКИЕ ФАКТОРЫ	F.900-F.999

Для получения более подробной информации просьба обращаться к Перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т F.751.8

Техническая основа для обеспечения соответствия технологии распределенного реестра (DLT) регуляторным нормам

Резюме

В Рекомендации МСЭ-Т F.751.8 определена техническая основа для обеспечения соответствия технологии распределенного реестра (DLT) регуляторным нормам, включая проблемы регулирования и технические возможности их решения. В настоящей Рекомендации проектирование технической основы DLT тесно связано со свойствами этих технологий, включая децентрализацию, неизменяемость и открытость. Настоящая Рекомендация может использоваться в качестве руководства поставщиками услуг DLT и разработчиками систем DLT в случаях, когда к системам DLT применяются регуляторные нормы.

Хронологическая справка *

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор
1.0	МСЭ-Т F.751.8	10.07.2023 г.	16-я	11.1002/1000/15174

Ключевые слова

Блокчейн, технология распределенного реестра; регулирование.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL https://handle.itu.int/ после которого укажите уникальный идентификатор Рекомендации.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т F.751.8

Техническая основа для обеспечения соответствия технологии распределенного реестра (DLT) регуляторным нормам

1 Сфера применения

В настоящей Рекомендации определена техническая основа для обеспечения соответствия технологии распределенного реестра (DLT) регуляторным нормам. Сфера применения настоящей Рекомендации включает:

– проблемы регулирования, связанные с DLT;

– технические возможности DLT для соблюдения регуляторных норм.

Целевыми пользователями настоящей Рекомендации являются поставщики услуг DLT и разработчики систем DLT. Регуляторные органы, занимающиеся DLT, не являются ее целевыми пользователями. Цель настоящей Рекомендации состоит не в том, чтобы предоставить регуляторные решения, касающиеся DLT, регуляторным органам, а скорее в том, чтобы предложить технические решения проблем, связанных с регуляторными нормами в отношении DLT.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T F.751.0] Рекомендация МСЭ-Т F.751.0 (2020 г.), *Требования к системам распределенного реестра*.

[ITU-T X.1401] Рекомендация МСЭ-Т X.1401 (2019 г.), *Угрозы безопасности технологии распределенного реестра*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 консенсус (consensus) [b-ITU-T X.1400]: Соглашение о том, что набор транзакций является действительным.

3.1.2 механизм консенсуса (consensus mechanism) [b-ITU-T X.1400]: Правила и процедуры, с помощью которых достигается консенсус.

3.1.3 распределенный реестр (distributed ledger) [b-ITU-T X.1400]: Тип реестра, который используется совместно, копируется и синхронизируется распределенным и децентрализованным образом.

3.1.4 секретность (privacy) [b-ITU-T J.160]: Способ обеспечения того, что информация не раскрывается кому-либо, кроме сторон, для которых она предназначается. Для обеспечения конфиденциальности информация как правило шифруется. Также называется "конфиденциальностью".

3.1.5 угроза (threat) [b-ISO/IEC 27000]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствует.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AML	Anti-Money-laundering		Борьба с отмыванием денег
DLT	Distributed Ledger Technology		Технология распределенного реестра
FATF	Financial Action Task Force on money laundering	ФАТФ	Группа разработки финансовых мер по борьбе с отмыванием денег
IoT	Internet of Things		Интернет вещей
KYC	Know Your Customer		"Знай своего клиента"
PKI	Public Key Infrastructure		Инфраструктура открытых ключей
TEE	Trusted Execution Environment		Доверенная среда выполнения

5 Соглашения по терминологии

В настоящей Рекомендации используются следующие соглашения:

– ключевые слова "**требуется**, **чтобы**" и "**должен**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

– ключевое слово "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии этому документу данное требование не является обязательным;

– ключевые слова "**может факультативно**" и "**может**" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Эти термины не означают, что вариант реализации поставщика должен обеспечивать выполнение соответствующей функции, активируемой по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может факультативно предоставить данную функцию и по-прежнему заявлять о соответствии спецификации.

6 Обзор

Технология распределенного реестра (DLT) позволяет большим группам узлов в сети распределенного реестра приходить к соглашению и записывать информацию без центрального органа. Быстрое развитие DLT создает проблемы с точки зрения регуляторных норм, в том числе регуляторных норм, касающихся охраны секретности/конфиденциальности, защиты данных, реагирования на сетевые атаки, криптовалюты и т. д. DLT применяется в различных областях, таких как криптовалюта, управление цепочками поставок и IoT. Таким образом, необходимо обобщить регуляторные требования на основе анализа функций и свойств DLT и определить техническую основу для одновременного соблюдения принципа открытости и регуляторных норм. Выполненная предварительная работа представлена в [b-DLT 4.1] и получила дальнейшее развитие в технических спецификациях, приведенных ниже.

7 Проблемы регулирования

7.1 Утечка конфиденциальной информации

Утечка конфиденциальной информации может произойти непосредственно внутри блокчейна в результате комбинирования внешних данных с данными внутри или вне блокчейна. Транзакции и открытые ключи могут быть напрямую доступны внутри блокчейна, особенно в случае систем общедоступного распределенного реестра. Внешние данные могут позволить соотнести открытые ключи с лицами или компаниями и тем самым идентифицировать транзакции.

В общедоступных распределенных реестрах контроль доступа отсутствует, и все данные, хранящиеся непосредственно внутри блокчейна, доступны любому. Хранение (незашифрованных) конфиденциальных данных в общедоступном распределенном реестре считается утечкой конфиденциальных данных.

7.2 Неизменяемость записей и отсутствие функции для удаления транзакций/ содержащейся информации

Согласно регуляторным нормам, требуется удаление персональных данных в зависимости от приложения DLT и типа данных. Это требование содержится в законах и подзаконных актах, что противоречит принципу неизменяемости систем DLT.

ПРИМЕЧАНИЕ. – Примером требования об удалении данных является право на забвение в Статье 17 Общего регламента ЕС по защите данных (Документ [b-GDPR]).

Кроме того, во исполнение законодательства и других нормативно-правовых актов о защите данных, может потребоваться внесение исправлений в транзакции. Это возможно только с помощью вилок, которые ставят под угрозу надежность систем распределенного реестра.

7.3 Угрозы безопасности

Угрозы безопасности для компонентов DLT описаны в [ITU-T X.1401] в пунктах 5.1 (угрозы протоколам), 5.2 (угрозы сетям) и 5.3 (угрозы данным).

7.4 Потеря токенов, цифровой валюты и других активов

В результате реализации угроз данным часто происходит потеря токенов, цифровой валюты и других активов. Однако эти потери также могут быть вызваны сознательным обманом с использованием поддельных монет, мошеннических систем распределенного реестра или с помощью лиц, стоящих за адресами учетных записей. Фишинговые атаки также могут заставить людей совершать транзакции, которые они иначе не совершали бы.

7.5 Финансовые и иные преступления

Системы распределенного реестра могут использоваться для совершения финансовых преступлений, таких как отмывание денег, или для содействия в совершении других преступлений, таких как атаки программ-вымогателей и т. д. Транзакции могут иметь незаконное содержимое, которое соответствует правилам протокола, но противоречит различным нормативно-правовым актам.

8 Технические возможности обеспечить соответствие регуляторным нормам

8.1 Техническая основа

Проектирование технической основы DLT для соответствия регуляторным нормам тесно связано со свойствами DLT, включая децентрализацию, автономность, неизменяемость, открытость, прозрачность и анонимность. Технические возможности DLT соответствовать регуляторным нормам определяются следующим образом: на уровне приложений, с точки зрения возможностей в отношении секретности/конфиденциальности, удаления данных, безопасности данных, а также возможностей на базовом уровне. В контролируемом распределенном реестре решающее значение имеет подотчетность, и рекомендуется, чтобы поставщики услуг DLT определили базовое юридическое лицо по организационным вопросам, чтобы уменьшить неопределенность в плане регуляторных мер.

8.2 Возможности на уровне приложений

– Рекомендуется, чтобы в системы DLT, используемые для передачи цифровых активов, был включен модуль, который обеспечивает соблюдение правил ФАТФ и/или конкретных национальных норм.

– Рекомендуется, чтобы в системах контролируемого распределенного реестра поддерживались функция "знай своего клиента" (KYC) и функция борьбы с отмыванием денег (AML) с использованием таких методов, как подписи на основе инфраструктуры открытых ключей (PKI).

– Поставщики услуг и разработчики систем DLT могут факультативно использовать такие методы, как ограничение прав совершения транзакций и блокировка учетных записей, для вмешательства в транзакции, созданные вредоносными и аномальными узлами.

– Поставщики услуг и разработчики систем DLT могут факультативно предоставить ссылку на официально признанную PKI. Это может факультативно использоваться для отождествления транзакций с юридическим лицом.

8.3 Возможности в отношении секретности/конфиденциальности

– Рекомендуется, чтобы в системе DLT не публиковалась конфиденциальная информация или персональные данные, в том числе информация об учетной записи, персональные данные/информация, позволяющая установить личность, данные транзакций, информация о цифровых активах и иная конфиденциальная информация, если для ее публикации нет основания.

– Не рекомендуется хранить данные, содержащие этот тип информации, в системе общедоступного распределенного реестра. Если этот тип информации требует верификации системой DLT, то в системе DLT рекомендуется хранить только зафиксированные или иным образом подтвержденные данные.

– Если невозможно избежать хранения данных в системе DLT, то для защиты конфиденциальных данных (коммерческих или личных) от раскрытия рекомендуется использовать криптографические методы, такие как доказательства с нулевым разглашением, запутывание учетных записей или методы, основанные на аппаратной изоляции (например, TEE).

– Рекомендуется должным образом обеспечивать защиту конфиденциальных данных, хранящихся вне блокчейна, с помощью некоторых подходящих криптографических методов.

– Рекомендуется, чтобы системы DLT, в которых хранится конфиденциальная информация, предлагали соответствующий контроль доступа, чтобы гарантировать возможность только авторизованного доступа. Рекомендуется ограничить доступ авторизованными лицами и/или ситуациями, когда доступ авторизован.

– Для хранения вне блокчейна рекомендуется использовать подходящие методы контроля доступа.

– Для защиты информации внутри блокчейна могут факультативно использоваться шифрование, доказательства с нулевым разглашением и криптографические хеш-функции. Однако проблемой неизменяемого хранилища в блокчейне является то, что способы скомпрометированного доступа невозможно заблокировать. Рекомендуется провести анализ рисков и/или анализ влияния технологии на защиту данных в отношении хранения конфиденциальных/личных данных в блокчейне.

8.4 Возможности удаления данных

Ключевым свойством систем распределенного реестра является высокий уровень неизменяемости. В связи с этим полное устранение свойства неизменяемости часто устраняет саму причину, по которой в первую очередь происходит выбор системы распределенного реестра.

Когда неизменяемость нежелательна для всех атрибутов транзакции, рекомендуется хранить данные вне блокчейна и только производить их валидацию, например путем сохранения доказательства для валидации данных вне блокчейна. Для этой цели в блокчейне могут факультативно использоваться такие технологии, как доказательства с нулевым разглашением, зафиксированные данные или хеш-значение. Требуется принять соответствующие меры, чтобы сделать невозможным получение какой бы то ни было лишней информации из данных, хранящихся в блокчейне.

В некоторых случаях верификации данных вне блокчейна может быть недостаточно, и требуется постоянство данных. Тем не менее постоянство данных может требоваться только в течение определенного периода времени или при выполнении некоторых условий. Примерами таких сценариев являются данные транзакций, которые необходимо сохранять только до тех пор, пока не выполнена следующая транзакция, а также записи, которые необходимо сохранять в течение определенного периода времени (например, 10 лет). В этих случаях факультативно может быть создан

распределенный реестр, который автоматически удаляет эти данные, когда выполнена следующая транзакция или когда истекает определенный период времени. Можно факультативно использовать такие методы, как отсечение [b-Nakamoto] и хеш-хамелеон [b-Camenisch].

При использовании таких технологий:

– должно быть четко определено, какие части реестра должны оставаться неизменяемыми;

– должно быть четко определено, при каких условиях могут быть изменены другие части;

– протокол распределенного реестра должен определять, как эти данные удаляются;

– протокол распределенного реестра должен гарантировать, что данные, удаление или изменение которых не требуется, остаются защищенными от изменения;

– должно быть обеспечено, чтобы архивные копии реестра хранились только в соответствии с действующими регуляторными нормами.

Целью удаления данных является ответ на нормативные требования местного законодательства, рекомендации или иные требования. Рекомендуется ограничить функциональную возможность удаления определенной частью данных, чтобы сохранялось доверие к неизменяемости остальных данных.

8.5 Возможности в отношении безопасности данных

– Поставщикам услуг и разработчикам систем DLT рекомендуется обеспечивать, чтобы проектирование систем DLT с использованием криптографии и других технологий соответствовало требованиям безопасности и оказания услуг DLT, включая надежность, полноту и неизменяемость, в частности за счет использования соответствующих криптографических алгоритмов и механизмов консенсуса.

– Поставщикам услуг и разработчикам систем DLT рекомендуется обеспечивать согласованность данных в блокчейне.

8.6 Возможности на базовом уровне

– Поставщикам услуг и разработчикам систем DLT рекомендуется принять соответствующие меры для обеспечения целостности, конфиденциальности, доступности и использования сетей DLT, а также для соблюдения ими норм.

– Разработчикам систем DLT рекомендуется противодействовать сетевым угрозам с помощью соответствующей структуры безопасности.

– Поставщики услуг и разработчики систем DLT могут факультативно использовать такие методы, как увеличение вычислительной мощности или ресурсов для предотвращения атак на механизм консенсуса.

– Поставщикам услуг и разработчикам систем DLT рекомендуется поддерживать безопасность смарт-контрактов в системах DLT с помощью формальной верификации или других методов обнаружения уязвимостей.

– Разработчики систем DLT могут факультативно проектировать отказоустойчивость систем DLT в случае появления вредоносных узлов. Систему DLT рекомендуется восстанавливать, когда набор обычных узлов работает со сбоями или становится вредоносным.

Библиография

[b-ITU-T J.160] Рекомендация МСЭ-Т J.160 (2005 г.), *Архитектура структуры для предоставления критических во времени услуг по сетям кабельного телевидения с использованием кабельных модемов*.

[b-ITU-T X.1400] Рекомендация МСЭ-Т X.1400 (2020 г.), *Термины и определения, относящиеся к технологии распределенного реестра*.

[b-Camenisch] Camenisch J., Derler D., Kernn S., Pöhls H. C., Samelin K., and Slamanig D. (2017), *Chameleon-hashes with ephemeral trapdoors and Applications to Invisible Sanitizable Signatures*, Public-Key Cryptography, Berlin, Springer, pp. 152-182. https://doi.org/10.1007/978-3-662-54388-7_6

[b-DIN SPEC 4997] DIN SPEC 4997 (2020), *Privacy by blockchain design: A standardised model for processing personal data using blockchain technology*.

[b-DLT 4.1] ITU-T HSTP.DLT-RF (2019), *Distributed ledger technologies: Regulatory framework*.

[b-GDPR] European Union General Data Protection Regulation law, Article 17, *Right to erasure ('right to be forgotten')*. https://gdpr.eu/article-17-right-to-be-forgotten/

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

[b-Nakamoto] Nakamoto S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	**Нетелефонные службы электросвязи**
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2023 г.