Международный союз электросвязи

МСЭ-Т X.1407

(01/2022)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги (2) – Безопасность технологии распределенного реестра (DLT)

Требования безопасности для услуг цифрового доказательства целостности данных на основе технологии распределенного реестра

Рекомендация МСЭ-Т X.1407

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды (1)	X.1140–X.1149
Безопасность приложений (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность умных электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1350–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределенного реестра (DLT)	**X.1400–X.1429**
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
Киберзащита	X.1590–X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800–X.1819

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

Рекомендация МСЭ-Т X.1407

Требования безопасности для услуг цифрового доказательства целостности данных на основе технологии распределенного реестра

Резюме

В Рекомендации МСЭ-Т X.1407 определяются угрозы и требования безопасности для цифрового доказательства целостности данных на основе технологии распределенного реестра (DLT).

Исходное защищенное свидетельство хранится вне блокчейна. Хеш-значения данных хранятся в блокчейне. В Рекомендации МСЭ-Т X.1407 проводится анализ угроз безопасности для услуг цифрового доказательства целостности данных на основе DLT, а именно в отношении регистрации свидетельств и их происхождения. В этой Рекомендации также приведены требования, соблюдение которых позволит устранить угрозы безопасности.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1407	07.01.2022 г.	17-я	11.1002/1000/14800

Ключевые слова

Цифровое доказательство целостности данных, технологии распределенного реестра, угрозы и требования безопасности.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например, http://handle.itu.int/11.1002/1000/11830-en.

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/авторскими правами на программное обеспечение, 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 соответствующим базам данных МСЭ-Т, доступным на веб-сайте МСЭ-Т по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1407

Требования безопасности для услуг цифрового доказательства целостности данных на основе технологии распределенного реестра

1 Сфера применения

В настоящей Рекомендации определяются угрозы и требования безопасности для услуг цифрового доказательства целостности объектов на основе технологии распределенного реестра (DLT). Платформа цифрового доказательства целостности данных на основе DLT обеспечивает предоставление услуг по распространению, запросу и отслеживанию цифровых свидетельств целостности объектов с использованием технологий распределенного реестра.

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 источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

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

[ITU-T X.1402] Recommendation ITU-T X.1402 (2020), *Security framework for distributed ledger technology.*

[ITU-T X.1404] Recommendation ITU-T X.1404 (2020), *Security assurance for distributed ledger technology.*

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в разделе 1.4 [b-ISO 23257] и других документах.

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

3.1.2 технологии распределенного реестра (distributed ledger technologies (DLT)) [b-ISO 22739]: Технологии, позволяющие работать с распределенными реестрами и использовать их.

3.1.3 технологическая платформа распределенного реестра (distributed ledger technology platform) [b-ISO 22739]: Набор объектов для обработки, хранения и передачи данных, которые совместно обеспечивают возможности системы DLT в каждом узле DLT.

3.1.4 целостность (integrity) [b-ISO 13491-2]: Показатель того, что данные не были изменены или разрушены несанкционированным способом.

3.1.5 реестр (ledger) [b-ITU-T X.1400]: Хранилище информации, в котором хранятся окончательные и полные (неизменяемые) записи транзакций.

3.1.6 смарт-контракт (smart contract) [b-ISO 22739]: Компьютерная программа, хранящаяся в системе DLT, в которой результат любого выполнения программы записывается в распределенный реестр.

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

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Аббревиатуры

В настоящей Рекомендации используются следующие сокращения и акронимы.

DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
DLT	Distributed Ledger Technology	Технология распределенного реестра
PBFT	Practical Byzantine Fault Tolerance	Алгоритм "практическая византийская отказоустойчивость"
PoS	Proof of Stake	Доказательство доли владения
PoW	Proof of Work	Доказательство выполнения работы

5 Соглашения

В настоящей Рекомендации применяются следующие глагольные формы для формулировки положений:

a) "должен" – обозначает требование;

b) "следует" – обозначает рекомендацию;

c) "разрешается" – обозначает разрешение;

d) "может" – обозначает возможность и способность.

6 Обзор

В случае если данные распределены по разным системам, процесс доказательства целостности этих данных представляет собой сложную задачу. Кроме того, процесс проверки целостности может потребовать поиска во многих базах данных, системах или вручную в бумажных копиях. Эту ситуацию усложняет отсутствие полной истории транзакций; в результате это может привести к задержкам, дополнительным расходам и трудозатратам, а также к принятию ошибочных решений. DLT – это защищенный от несанкционированного доступа децентрализованный реестр, который создает уровень доверия, необходимый для обмена ценностями без посредников. Он опирается на децентрализованные базы данных, которые обеспечивают целостность записей обо всех транзакциях, возможность совместной работы с ними, прозрачность, а также возможность проверки и аудита. Таким образом отслеживаемые и защищенные от несанкционированного доступа функции DLT позволяют создать решение для цифрового доказательства целостности, так чтобы создание или изменение обманным путем исходных данных было невозможно без того, чтобы эти изменения были обнаружены.

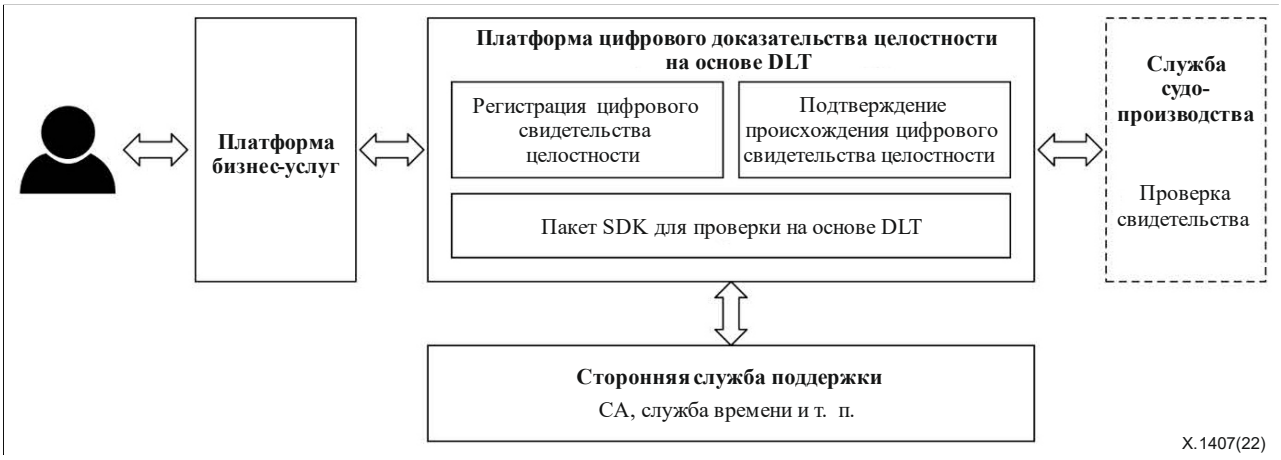

Рисунок 1 – Иллюстрация процесса цифрового доказательства целостности на основе DLT

В базовые сценарии на платформах цифрового доказательства целостности на основе DLT входят регистрация свидетельств и проверка их происхождения. Пользователь платформы бизнес-услуг инициирует обращение к службе цифрового доказательства и регистрирует свидетельство в DLT, сохраняя хеш-код полученной цифровой подписи с помощью контракта на регистрацию IP-свидетельств. Процесс проверки целостности свидетельства зависит от проверки его хеш-кода и сравнения этого хеш-кода со значениями, хранящимися в DLT. Более того, чтобы гарантировать законное использование цифрового свидетельства и защитить права пользователей, предоставляется услуга запроса и проверки цифровых свидетельств для судебной экспертизы в случае судебного разбирательства в онлайновом формате.

Хотя отслеживаемые и защищенные от несанкционированного доступа функции DLT позволяют лучше контролировать и использовать целостность записей, внедрение DLT создает некоторые угрозы безопасности. Они могут быть нацелены на пользователей, цифровые свидетельства или процессы их регистрации и подтверждения происхождения. Следовательно, необходимо и полезно суммировать угрозы безопасности различных категорий с помощью анализа действий, связанных с цифровой проверкой целостности на основе DLT. По итогам анализа этих угроз определяется набор требований безопасности.

7 Заинтересованные стороны и процессы цифрового доказательства целостности на основе DLT

7.1 Заинтересованные стороны

7.1.1 Внутренние заинтересованные стороны

К внутренним заинтересованным сторонам следует относить:

a) пользователя;

b) платформу бизнес-услуг;

c) платформу цифрового доказательства целостности на основе DLT.

7.1.2 Внешние заинтересованные стороны

К внешним заинтересованным сторонам относятся:

a) сторонние вспомогательные услуги, включая организации, обеспечивающие выдачу сертификатов CA, службу времени и прочие услуги;

b) регуляторные органы, включая национальные судебные органы и другие организации, связанные с судопроизводством.

7.2 Процессы цифрового доказательства целостности на основе DLT

7.2.1 Регистрация цифрового свидетельства целостности

Регистрация цифровых свидетельств целостности в DLT включает следующие основные процессы.

a) Пользователь взаимодействует с платформой бизнес-услуг, и ему может потребоваться защита аутентичности деловой информации; бизнес-платформа отправляет извлеченные характеристики исходной информации на платформу цифрового доказательства целостности на основе DLT.

b) Платформа цифрового доказательства целостности на основе DLT генерирует электронное свидетельство с указанием извлеченных характеристик, отметкой времени и другой необходимой информацией.

c) Платформа цифрового доказательства целостности на основе DLT генерирует уникальный хеш-код электронного свидетельства с помощью криптографических хеш-функций (таких как SHA256).

d) Платформа бизнес-услуг генерирует цифровую подпись для хеш-кода с помощью секретного ключа владельца.

e) Платформа бизнес-услуг передает запись свидетельства по адресу смарт-контракта в распределенных реестрах.

f) Платформа цифрового доказательства целостности на основе DLT проверяет, готова ли цифровая подпись и информация, и выполняет смарт-контракт, создавая соответствующую запись в реестре.

g) Информация о регистрации свидетельства упаковывается в новый блок транзакций, после чего этот новый блок передается в сеть.

7.2.2 Происхождение цифрового свидетельства целостности

Проверка происхождения цифрового свидетельства целостности включает следующие основные процессы.

a) Пользователь запрашивает цифровое свидетельство целостности, хранящееся в распределенных реестрах.

b) В случае судебного разбирательства в онлайновом формате платформа судопроизводства проводит судебную экспертизу цифровых свидетельств на основе записей в распределенных реестрах.

8 Угрозы безопасности при цифровом доказательстве целостности на основе DLT

В этом разделе анализируются угрозы безопасности для заинтересованных сторон, то есть пользователя, платформы цифрового доказательства целостности на основе DLT и процессов, участвующих в цифровом доказательстве целостности на основе DLT, а именно регистрации и проверки происхождения цифровых свидетельств целостности. Угрозы для компонентов протокола, сети и данных в приложениях на основе DLT подробно рассматриваются в [ITU-T X.1401].

8.1 Угрозы безопасности, связанные с пользователем

8.1.1 Подделка идентичности пользователя

Зарегистрированные пользователи подают незаконные запросы, используя фальшивую личную информацию, чтобы получить не положенное им разрешение.

8.1.2 Утечка секретного ключа

Угрозы утечки секретного ключа в реестре чаще всего заключаются в атаках на клиентское программное обеспечение или физических атаках (например, демонстрация распечатанного секретного ключа другим лицам). Утечка секретного ключа позволяет другим пользователям получить доступ к платформе доказательства на основе DLT, что ставит под угрозу ее безопасность. Угроза утечки секретного ключа подробно рассматривается в пункте 6.3.2 [ITU-T X.1401].

8.1.3 Потеря секретного ключа

Угрозы потери секретного ключа чаще всего заключаются в атаках злонамеренных программ, физических атаках (например, потеря секретного ключа, распечатанного на бумаге) и т. п. Такое поведение может привести к раскрытию конфиденциальности пользователей, что позволяет злонамеренным пользователям получить доступ к платформе доказательства на основе DLT и нарушить ее безопасность. Угроза потери секретного ключа подробно рассматривается в пункте 6.3.3 [ITU-T X.1401].

8.1.4 Нарушение конфиденциальности

Доказательная информация владельца может включать в себя конфиденциальную личную информацию, такую как имя и идентификационные данные, и в процессе регистрации свидетельства может возникнуть проблема утечки конфиденциальной информации пользователя. Угроза нарушения конфиденциальности подробно рассматривается в пункте 6.3.1 [ITU-T X.1401].

8.2 Угрозы безопасности, связанные с регистрацией свидетельств

8.2.1 Мошеннические действия со свидетельствами

В соответствии с алгоритмом извлечения признаков цифрового доказательства злоумышленники могут создавать различные признаки документа, содержание которого подобно содержанию исходного документа. Таким образом злоумышленники могут записать в распределенные реестры незаконную информацию.

8.2.2 Фальсификация свидетельств

Злонамеренные пользователи могут подделать свидетельство подлинности исходного документа или нарушить его целостность и доступность, что приведет к записи в распределенные реестры подложного свидетельства. Атаки с использованием асимметричного алгоритма шифрования могут привести к применению небезопасных методов передачи и хранения данных. Атака с использованием асимметричного алгоритма шифрования подробно описана в пункте 6.1.5 [ITU-T X.1401].

8.2.3 Атака с воздействием на отметки времени

Атаки могут изменять отметки времени платформы доказательства на основе DLT, в результате чего эта платформа не сможет точно отслеживать последовательность событий регистрации свидетельств, что лишит ее возможности обеспечить эффективную основу для судебной экспертизы происхождения свидетельств.

8.2.4 Атака 51%

Если злоумышленники овладевают более чем 51% вычислительной мощности, они могут построить новый блокчейн. Новый блокчейн может аннулировать свидетельства в основном блокчейне. Кроме того, атака 51% может привести к успешной регистрации нарушителя. Атака 51% подробно описана в пункте 6.1.1 [ITU-T X.1401].

8.2.5 Атака подкупом

Злоумышленники, располагающие достаточными ресурсами, могут подкупать владельцев узлов с правом голоса и действовать в ущерб правам и интересам сети доказательства на основе распределенного реестра. Так, злоумышленники могут записать в сеть доказательства на основе распределенного реестра неправомерную информацию о свидетельствах. Атака подкупом подробно описана в пункте 6.1.1 [ITU-T X.1401].

8.2.6 Атака с удержанием блока

На платформе доказательства на основе DLT, базирующейся на алгоритме консенсуса PoW (доказательства выполнения работы), злоумышленник может сохранить добытый им блок и тайно добывать следующий, если располагает достаточными мощностями. Выпуская несколько блоков, пока другие майнеры генерируют один, злоумышленник может заставить других майнеров растрачивать энергию впустую. Мишенью атаки является оператор платформы, который получает нулевые подтверждения. Это может сделать недействительным доказательство основного блокчейна. Это также может привести к успешной регистрации нарушителя. Атака с удержанием блока подробно описана в пункте 6.1.1 [ITU-T X.1401].

8.2.7 Атака с переключением блокчейна

Злоумышленник может переключаться между разными блокчейнами, используя сложные алгоритмы настройки блокчейна. Это может привести к несправедливому вознаграждению злоумышленников в ущерб другим пользователям. Это также может привести к значительному увеличению эффективной вычислительной мощности майнингового пула и к успешной регистрации нарушителя. Атака с переключением блокчейна подробно описана в пункте 6.1.1 [ITU-T X.1401].

8.2.8 Распределенная атака типа отказ в обслуживании

На платформе доказательства на основе DLT злоумышленник может заблокировать сеть с помощью распределенных атак типа отказ в обслуживании (DDoS), при этом наиболее распространенными методами являются атака Сибиллы и атака затмения. Это может привести к успешной регистрации свидетельства злоумышленника. Атака Сибиллы подробно описана в пункте 6.2.3, а атака затмения – в пункте 6.2.1 [ITU-T X.1401].

8.2.9 Атака с перехватом BGP

Злоумышленник может воспользоваться протоколом захваченного пограничного шлюза (border gateway protocol – BGP) и разделить сетевые узлы распределенных реестров на две или более групп. В результате DLT разбивается на два или несколько параллельных блокчейнов. Тогда регистрация свидетельств и регистрация свидетельств злоумышленника будут выполняться в параллельных ветвях. После прекращения атаки распределенный реестр воссоединяется с самым длинным основным блокчейном, другие ветви отбрасываются, и все записи свидетельств в этих ветвях становятся недействительными, что может привести к успешной регистрации свидетельства злоумышленника.

8.3 Угрозы безопасности, связанные с происхождением свидетельств

8.3.1 Атака с записью информации злоумышленника

Никакие данные транзакций в DLT не подлежат удалению. После того как информация записана в DLT, ее невозможно уничтожить. Злоумышленники могут записывать в распределенные реестры свою информацию путем запуска атак на основе смарт-контрактов, например атак с использованием неправильно обработанных исключений, как подробно описано в пункте 6.1.2 [ITU-T X.1401]. Платформа генерирует новые блоки, что приводит к атаке с использованием спам-блоков, а это влияет на производительность платформы доказательства на основе DLT.

8.3.2 Раскрытие информации о свидетельствах

Следует использовать специальный алгоритм шифрования и хранения информации о происхождении свидетельств. Важно обеспечить безопасность алгоритма шифрования. Атаки с использованием асимметричного алгоритма шифрования могут привести к небезопасному состоянию платформы доказательства на основе DLT. Атака с использованием асимметричного алгоритма шифрования подробно описана в пункте 6.1.5 [ITU-T X.1401].

9 Требования безопасности цифрового доказательства целостности на основе DLT

В этом разделе описаны требования безопасности цифрового доказательства целостности на основе DLT, которые базируются на анализе угроз безопасности, перечисленных в разделе 7. Кроме того, в этом разделе описываются требования безопасности, относящиеся к заинтересованным сторонам, то есть к пользователям, платформе цифрового доказательства целостности и к процессам, задействованным в предоставлении услуг цифрового доказательства целостности на основе DLT, а именно к регистрации цифровых свидетельств и проверке происхождения цифровых свидетельств. Требования безопасности в отношении данных, сети, консенсуса и применения подробно описаны в пунктах 8.1–8.4 [ITU-T X.1402].

9.1 Требования безопасности в отношении пользователей

9.1.1 Защита идентичности пользователей

Для платформы цифрового доказательства целостности на основе DLT устанавливаются следующие требования безопасности, связанные с предотвращением мошенничества с идентификационной информацией.

a) Платформа цифрового доказательства целостности на основе DLT должна определять операционные полномочия различных пользователей. Платформа должна позволять пользователям подписывать информацию с помощью секретного ключа и отправлять ее в DLT. DLT должна восстанавливать открытый ключ на основе подписи, идентифицировать пользователей с помощью открытого ключа и аутентифицировать операции пользователей.

b) Когда пользователь регистрируется на платформе, платформа сначала проверяет его идентификационную информацию, а затем может присвоить каждому пользователю метку.

c) Платформа цифрового доказательства целостности на основе DLT должна записывать все операции каждого пользователя в распределенные реестры.

d) При регистрации каждого свидетельства платформа цифрового доказательства целостности на основе DLT должна требовать выполнения функций аутентификации личности, включая управление доступом, пароль, цифровую подпись, биометрическое распознавание и т. д.

9.1.2 Защита секретного ключа

Для платформы доказательства на основе DLT устанавливаются следующие требования безопасности, связанные с защитой закрытых ключей.

a) Платформа цифрового доказательства целостности на основе DLT должна предотвращать утечку секретных ключей – оператор платформы доказательства на основе DLT должен предотвратить проникновение вредоносного кода в системы своих клиентов.

b) Платформа цифрового доказательства целостности на основе DLT должна предотвращать потерю секретных ключей – пользователи платформы доказательства на основе DLT должны хранить секретные ключи в безопасном месте и не оставлять их на легкодоступных нефизических и физических носителях (например, на бумаге) без каких-либо механизмов защиты (в число потенциальных контрмер входит использование личных идентификационных номеров, паролей, отпечатков пальцев, другой биометрической информации и т. д.).

9.1.3 Защита конфиденциальности

В рамках звеньев операций по обработке информации (сбор, хранение, использование, распространение, передача, публичное раскрытие и т. д.) платформы цифрового доказательства целостности на основе DLT должны приниматься соответствующие меры защиты, чтобы предотвратить незаконный сбор информации о владельцах, злоупотребление ею и ее утечку, а также для максимальной защиты законных прав и интересов владельцев.

9.2 Требования безопасности в отношении регистрации свидетельств

9.2.1 Предотвращение мошенничества со свидетельствами

Для платформы доказательства на основе DLT устанавливаются следующие требования безопасности, связанные с предотвращением мошенничества с цифровыми свидетельствами.

a) Для предотвращения возможности подделки цифровых свидетельств платформа доказательства на основе DLT должна обеспечивать согласование алгоритмов с гарантией уровня безопасности (LoSA) и надежный механизм консенсуса (CMS) [ITU-T X.1404], такой как практическая византийская отказоустойчивость (PBFT).

b) Платформа доказательства на основе DLT должна контролировать эффективную вычислительную мощность сети, обнаруживать аномальные изменения и предотвращать атаки с переключением блокчейна.

c) Платформа доказательства на основе DLT должна повышать сложность алгоритмов вычисления собственных значений, гарантируя при этом, что эффективность работы системы будет находиться в разумных пределах.

9.2.2 Предотвращение фальсификации свидетельств

Для платформы доказательства на основе DLT устанавливаются следующие требования безопасности, связанные с предотвращением фальсификации цифровых свидетельств.

a) Платформа доказательства на основе DLT должна использовать аппаратное шифрование.

b) Платформа доказательства на основе DLT должна использовать алгоритмы шифрования, гарантирующие безопасную передачу информации свидетельств. Связанные с платформой сторонние службы должны использовать алгоритмы шифрования, гарантирующие безопасное хранение информации свидетельств. Платформа и связанные с ней сторонние службы должны выбирать подходящие алгоритмы шифрования, обеспечивающие компромисс между безопасностью и стоимостью вычислений, а также длиной ключа – можно увеличить длину ключей, чтобы компенсировать риски, вызванные повышением вычислительной мощности.

9.2.3 Защита регистрации свидетельств

Для платформы доказательства на основе DLT устанавливаются следующие требования безопасности, относящиеся к управлению безопасностью регистрации.

a) Платформа цифрового доказательства целостности на основе DLT должна быть синхронизирована с доверенной сторонней службой времени.

b) Платформа цифрового доказательства целостности на основе DLT должна подавать предупредительные сигналы об атаках, уязвимостях, вредоносном коде, анализе угроз и утечке данных, а также предоставлять другую оперативную информацию об угрозах и выявлять проблемы, относящиеся к платформе, с помощью сканирования уязвимостей и автоматического тестирования безопасности.

c) Платформа цифрового доказательства целостности на основе DLT должна обеспечивать аутентификацию идентичности и управление доступом для снижения риска атак, таких как злонамеренная подмена и дистанционная атака.

d) Для мобильных приложений платформа цифрового доказательства целостности на основе DLT должна обеспечивать методы защиты безопасности, такие как усложнение и запутывание исходного кода, в целях предотвращения обратного анализа, декомпиляции и внедрения вредоносного кода.

e) Платформа может использовать технологию контрольных точек для записи заданного кода в клиентскую программу, так чтобы она принимала все эффективные транзакции до контрольной точки, тем самым предотвращая атаку 51%; контрольная точка должна: ввести улучшенный механизм консенсуса доказательства доли владения (PoS) с использованием ограничительных и штрафных мер, установить отметки времени транзакций, установить стороннюю службу надежной аутентификации узлов для аутентификации идентичности, а также не принимать нулевые подтверждения.

f) Платформа может выполнять фильтрацию портов для удаления аномального трафика, обеспечивать защиту безопасности облака и надежную защиту для разрешения конфликтов в системе доменных имен (DNS), чтобы обеспечить безопасную работу, а также должна регулировать размер блоков данных для предотвращения спам-атак.

g) Платформа цифрового доказательства целостности на основе DLT должна обеспечивать сбор свидетельств и отслеживание инцидентов безопасности, анализировать причины и представлять методы для сдерживания атак.

9.3 Требования безопасности в отношении происхождения свидетельств

9.3.1 Предотвращение записи вредоносной информации

Для обеспечения безопасности информации о происхождении свидетельств платформа цифрового доказательства целостности на основе DLT должна:

a) регулировать размер блоков данных, чтобы узлы не создавали спам-блоки;

b) гарантировать невозможность для неавторизованных и анонимных объектов находить или получать доступ к данным учетных записей и транзакций в узлах системы распределенного реестра;

c) использовать библиотеки, гарантирующие безопасность вычислений, такие как SafeMath;

d) выполнять проверку кода во избежание переполнения целочисленной переменной и неправильной обработки исключений для предотвращения атак в смарт-контрактах;

e) использовать генераторы непредсказуемых случайных чисел, чтобы злоумышленники не могли управлять результатами смарт-контрактов;

f) в процессе разработки программы сделать дизайн управления доступом как можно более строгим, чтобы предотвратить возможность изменения злоумышленниками принадлежности функций смарт-контрактов в целях получения наивысших операционных полномочий.

9.3.2 Защита информации свидетельств

Для обеспечения безопасности информации свидетельств платформа цифрового доказательства целостности на основе DLT должна:

a) использовать для хранения информации свидетельств вне блокчейна зашифрованные запоминающие устройства;

b) выбирать подходящие алгоритмы шифрования, обеспечивающие компромисс между безопасностью и стоимостью вычислений, а также длиной ключа – можно увеличить длину ключей, чтобы компенсировать риски, вызванные повышением вычислительной мощности;

c) использовать эффективный механизм управления доступом для обеспечения контролируемого доступа к информации свидетельств.

Дополнение I

Пример сценария использования электронных счетов-фактур на основе технологии распределенного реестра

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Согласно механизму консенсуса могут проверяться и утверждаться только счета-фактуры, составленные налоговыми органами; счета-фактуры, составленные любыми другими узлами, не могут быть подтверждены, что гарантирует подлинность счетов-фактур. В смарт-контрактах транзакции и выставление счетов-фактур производятся одновременно, и процесс оплаты и оформление счетов-фактур потребителями осуществляются без проблем. Обзор представлен на рисунке I.1. Дополнительные сведения см. в документе [b-IEEE 2142.1-2021] (Recommended practice for e-invoice business using blockchain technology).

Рисунок I.1 – Обзор сценария использования электронных счетов-фактур на основе DLT

Пример сценария использования электронных счетов-фактур на основе технологии распределенного реестра медицинскими учреждениями описывается следующим образом.

a) Медицинские учреждения регистрируют учетную запись в блокчейне, подключаются к системе выставления счетов-фактур на основе DLT и определяют условия выставления счетов-фактур в блокчейне.

b) Медицинское учреждение выдает рецепт.

c) Пользователь оплачивает медицинские расходы по рецепту.

d) После оплаты пользователь получает подробный перечень медицинских расходов.

e) Пользователь подает заявление на возмещение расходов.

f) Пользователь успешно получает электронный счет-фактуру через блокчейн.

g) Сканируя код на мобильном терминале, пользователи могут получать и просматривать электронные счета-фактуры в блокчейне.

h) Мобильный терминал может отправлять сообщения о возможности возмещения расходов, и пользователи передают информацию и получают возмещение расходов с помощью электронного счета-фактуры в блокчейне.

Процесс оформления счетов-фактур после оплаты может включать следующие этапы:

– этап A – транзакция;

– этап B – выставление счета-фактуры;

– этап C – возмещение расходов;

– этап D – оформление свидетельства об уплате налога (налоговая очистка).

Рисунок I.2 – Блок-схема сценария использования электронного счета-фактуры на основе DLT

На этапе транзакции, когда заказчик (покупатель) размещает заказ, поставщик услуг (продавец) создает заказ на платежной платформе, затем платежная платформа подтверждает заказ после получения подтверждения от заказчика и после обработки платежа создается квитанция. Квитанция может иметь форму блока платежа в цепочке платежей или записи в централизованной базе данных.

На этапе выставления счета-фактуры налоговое ведомство продавца выставляет счет-фактуру на основе заявления покупателя, поступившего, например, из электронного кошелька покупателя, и квитанция об оплате используется в качестве неизрасходованного входящего остатка транзакции (unspent transaction output – UTXO) для выставления счета-фактуры. В число участвующих узлов входят основные узлы консенсуса, закрепленные на базовом уровне реестра, а также узлы упрощенной проверки платежей (simplified payment verification – SPV), такие как узел продавца, узел персонального кошелька и т. п.

На этапе возмещения расходов предприятие, связанное с заказчиком (customer associating enterprise – CAE) в качестве узла SPV, проверяет счет-фактуру, когда покупатель инициирует процесс возмещения расходов, и в персональном кошельке происходит возмещение расходов по счету-фактуре в качестве UTXO.

В процессе налоговой очистки к процессу присоединяются конечные узлы налоговых ведомств и узел SPV CAE, а счет-фактура используется в качестве UTXO для возмещения НДС.

Система электронных счетов-фактур с использованием DLT имеет следующие преимущества.

1 Имеется гарантия того, что счет-фактура является подлинным документом и весь процесс получения счетов, выставления счетов, обращения, ввода и возмещения прослеживается.

2 Данные счета-фактуры защищены от подделки, и в процессе бухгалтерского учета совместно участвуют налоговый орган, сторона, выставляющая счета на оплату, сторона, ответственная за распространение информации, и сторона, возмещающая расходы.

3 Для электронных счетов-фактур на основе DLT не требуются знаки оплаты налога и специальное оборудование. Для традиционного счета на оплату в случае сетевых магазинов требуется несколько знаков оплаты налога для каждого магазина, а электронный счет-фактура на основе DLT автоматически обрабатывается системой ERP, и большое количество магазинов не влечет за собой дополнительных затрат.

4 При использовании традиционных счетов-фактур, если количество счетов-фактур, утвержденных налоговыми органами, не может удовлетворить потребности бизнеса из-за временного увеличения объема бизнеса, налогоплательщик может обратиться в налоговые органы за дополнительными счетами-фактурами. Счета же на основе DLT предоставляются по запросу, и дополнительной подачи заявлений не требуется.

5 Получение и приобретение налоговым органом традиционных счетов на бумаге требует времени и усилий, в то время как электронные счета на основе DLT обрабатываются без бумажных документов.

Дополнение II

Пример проверки документов об образовании на основе технологии распределенного реестра

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Проверка документов об образовании – трудоемкий процесс, который может занимать дни или недели. Работодателям требуется подтверждение квалификации, и они тратят значительное время на обращение в университеты для проверки целостности документов об образовании и для того, чтобы убедиться, что соискатели обладают безупречной квалификацией. Блокчейн обеспечивает прозрачность и упрощает предъявление аутентифицированных документов об образовании различным работодателям или любым другим сторонам.

Работодатели могут проверить целостность документа об образовании с помощью DLT. DLT – признанная безопасная технология хранения документов об уровне подготовки студентов, доступная различным учреждениям и университетам. Она обеспечивает непрерывный публичный учет, защищенный от изменений в учреждении или потери личных дел.

Этот процесс состоит из следующих компонентов.

Пользователи

– эмитент (университет)

– получатель (студенты)

– проверяющий (работодатели)

Системы

– университетские узлы

– платформа блокчейн

Данные

– хеш-коды документов об образовании

– электронный файл документа об образовании

Процесс проверки целостности документа об образовании основан на проверке его хеш-кода и сравнении с хеш-кодами, хранящимися в блокчейне, как показано на рисунке II.1. Выполняются следующие шаги.

– Университет выдает студенту новый электронный документ об образовании и загружает файл в DLT.

– DLT хеширует и сохраняет файл документа об образовании.

– Для демонстрации подтверждения целостности студент или работодатель загружает документ об образовании на платформу DLT.

– DLT вычисляет хеш-код документа, а затем сравнивает его с хеш-кодами, хранящимися в блокчейне.

– Если полученный хеш-код соответствует одному из хеш-кодов, хранящихся в блокчейне, то документ об образовании подлинный.

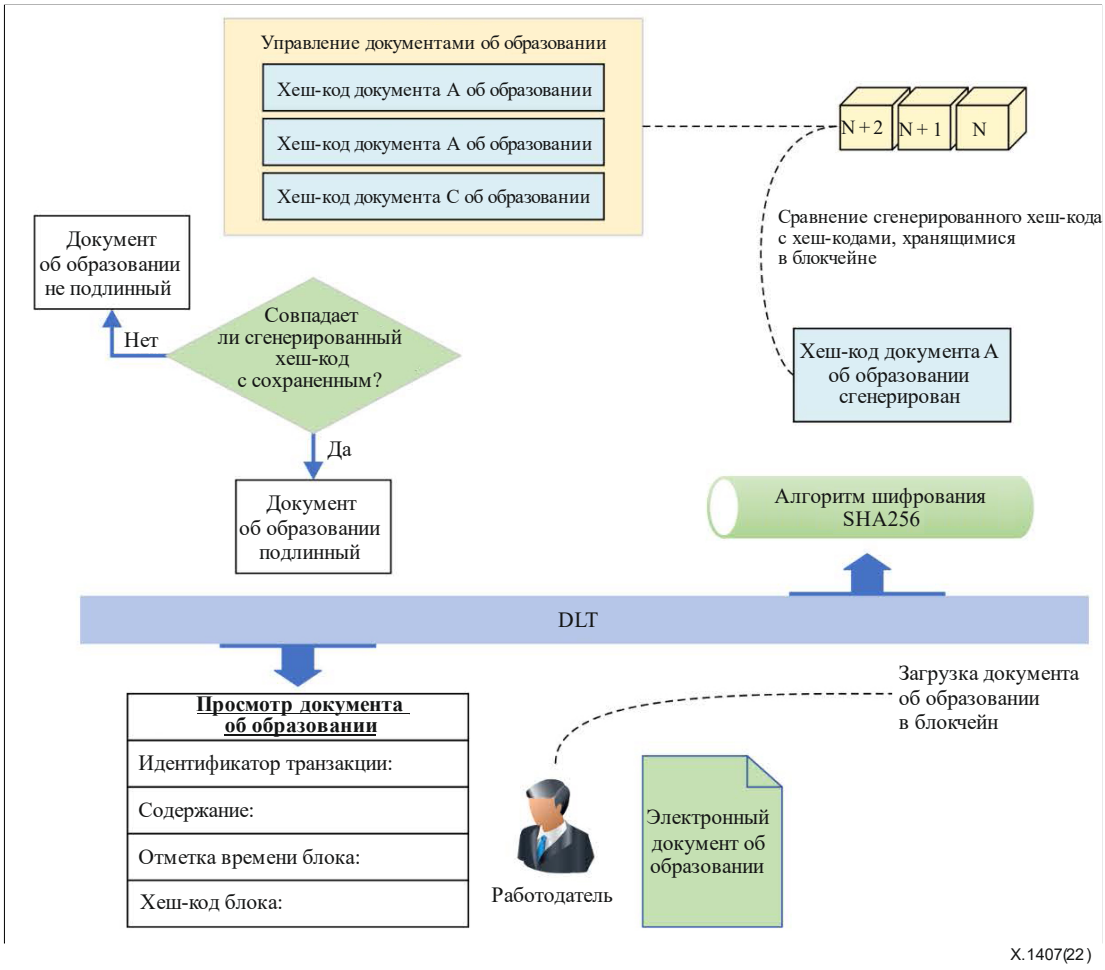

Рисунок II.1 – Обзор сценария проверки документа об образовании на основе DLT

Преимущества использования DLT для аутентификации документов об образовании:

– DLT решает текущие проблемы в процессе проверки и аутентификации;

– DLT позволяет сгруппировать все университеты на единой платформе;

– DLT побуждает работодателей сотрудничать с университетами на систематической основе;

– DLT помогает хранить и распространять достоверную и целостную информацию как единый источник истины;

– DLT экономит время, деньги и силы.

Библиография

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

[b-IEEE 2142.1-2021] IEEE 2142.1-2021, *IEEE Recommended practice for e-invoice business using blockchain technology.*
https://standards.ieee.org/ieee/2142.1/7590/

[b-ISO 5807] ISO 5807:1985, *Information processing – Documentation symbols and conventions for data, program and system flowcharts, program network charts and system resources charts*.
https://www.iso.org/standard/11955.html

[b-ISO 13491-2] ISO 13491-2:2017(en), *Financial services – Secure cryptographic devices (retail) – Part 2: Security compliance checklists for devices used in financial transactions.*
https://www.iso.org/obp/ui/#iso:std:iso:13491:-2:ed-4:v1:en

[b-ISO 22739] ISO 22739: 2020, *Blockchain and distributed ledger technologies – Vocabulary.*
https://www.iso.org/standard/73771.html

[b-ISO 23257] ISO 23257:2022, *Blockchain and distributed ledger technologies – Reference architecture.*

[b-ISO 56000] ISO 56000:2020, *Innovation management – Fundamentals and vocabulary*.
https://www.iso.org/standard/69315.html

[b-ISO/IEC 27000] ISO/IEC 27000:2018(en), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

[b-Kaur] Kaur, S., Chaturvedi, S., Sharma, A. Kar, J. (2021), *A Research Survey on Applications of Consensus Protocols in Blockchain*, Security and Communication Networks, Vol. 2021, Article ID 6693731, January, pp. 1-22.
https://doi.org/10.1155/2021/6693731

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, 2022 г.