International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1407

(01/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

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

Security requirements for digital integrity proofing service based on distributed ledger technology

Recommendation ITU-T X.1407

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	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
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	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1407

Security requirements for digital integrity proofing service based on distributed ledger technology

Summary

Recommendation X.1407 specifies the security threats and requirements in digital integrity proofing based on distributed ledger technology (DLT).

The original proof protected is stored in the off-chain. The hashed data values are stored in the on-chain. Recommendation ITU-T X.1407 analyses the security threats to the digital integrity proofing services based on DLT, namely, proof registration and proof provenance. This Recommendation also describes the security requirements that could address security threats.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1407	2022-01-07	17	11.1002/1000/14800

Keywords

Digital integrity proofing, distributed ledger technologies, security threats and requirements.

* 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

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 ... 2

5 Conventions ... 2

6 Overview ... 2

7 Stakeholders and processes for DLT-based digital integrity proofing ... 3

7.1 Stakeholders ... 3

7.2 Processes of DLT-based digital integrity proofing ... 3

8 Security threats for DLT-based digital integrity proofing ... 4

8.1 Security threats w.r.t user ... 4

8.2 Security threats w.r.t proof registration ... 4

8.3 Security threats w.r.t proof provenance ... 5

9 Security requirements for DLT-based digital integrity proofing ... 6

9.1 Security requirements for a user ... 6

9.2 Security requirements for proof registration ... 7

9.3 Security requirements for proof provenance ... 8

Appendix I – Use case of e-invoice based on distributed ledger technology ... 9

Appendix II – Use case for verification of academic certificates based on distributed ledger technology ... 12

Bibliography ... 14

Recommendation ITU-T X.1407

Security requirements for digital integrity proofing service based on distributed ledger technology

1 Scope

This Recommendation specifies the security threats and requirements for digital proofing of the integrity of an entity based on distributed ledger technology (DLT). The DLT-based digital integrity proofing platform provides services for distributing, querying, and tracking digital proof of the integrity of an entity using distributed ledger technologies.

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 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 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined in section 1.4 of [b-ISO 23257], and elsewhere:

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

3.1.2 distributed ledger technologies (DLTs) [b-ISO 22739]: Technology that enables the operation and use of distributed ledgers.

3.1.3 distributed ledger technology platform [b-ISO 22739]: Set of processing, storage and communication entities which together provide the capabilities of the DLT system on each DLT node.

3.1.4 integrity [b-ISO 13491-2]: Property that data has not been altered or destroyed in an unauthorized manner.

3.1.5 ledger [b-ITU-T X.1400]: Information store that keeps final and definitive (immutable) records of transactions.

3.1.6 smart contract [b-ISO 22739]: Computer program stored in a DLT system wherein the outcome of any execution of the program is recorded on the distributed ledger.

3.1.7 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident which can result in harm to a system or organization.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
PoS	Proof of Stake
PoW	Proof of Work
PBFT	Practical Byzantine Fault Tolerance

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 permission,

d) "Can" indicates a possibility and a capability.

6 Overview

The process of proving the integrity of certain data is a challenge in case the data is scattered across different systems. Also, the process of checking the integrity may require searching in many databases, systems, or manually in hard copies. This situation suffers from the absence of the complete history of the transaction; as a result, this could lead to delays, additional efforts and costs, and incorrect decision making. DLT is a tamper-proof, decentralized ledger that establishes a level of trust necessary for the exchange of value without the use of intermediaries. It relies on decentralized databases that provide integrity, collaborative, transparent, verifiable, and auditable records for all transactions. Thus, the traceable, tamper-proof features of DLT enables a solution for digital integrity proofing where the original data cannot be fraudulently created or compromised without a way to detect the changes.

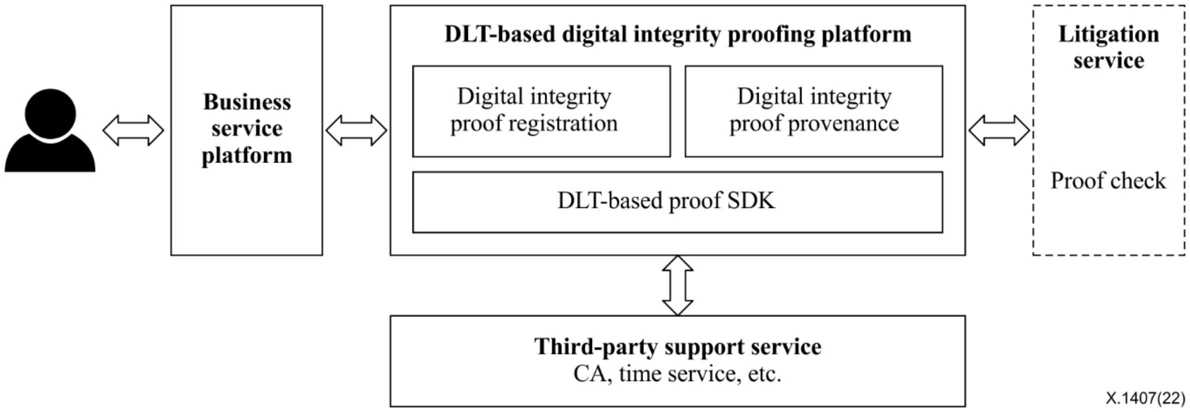

Business service platform
DLT-based digital integrity proofing platform
Digital integrity proof registration
Digital integrity proof provenance
DLT-based proof SDK
Litigation service
Proof check
Third-party support service
CA, time service, etc.
X.1407(22)

Figure 1 – Illustration of digital integrity proofing based on DLT

The basic scenarios on DLT-based digital integrity proof platforms involve proof registration and proof provenance. The user on the business service platform initiates a digital proof service call and registers the proof onto the DLT and stores the hash of the extracted digital signature through the IP proof registration contract. The process of checking the integrity of the proof depends on checking the hash value of the proof and comparing the hash with the hashes stored on the DLT. Moreover, to guarantee the legal use of a digital proof and protect the rights of the user, a digital proof querying and checking service is provided for forensics on online litigation.

Although the traceable, tamper-proof features of DLT enable better control and exploit the integrity of the records, there are security threats present in adopting DLT. Some threats are directed at users, some at digital proof, and others at proof registration and provenance processes. Therefore, it is necessary and useful to summarize security threats in different categories based on analyses of the activities involved in DLT-based digital integrity proof. Based on the analysis of these threats, a set of security requirements is identified.

7 Stakeholders and processes for DLT-based digital integrity proofing

7.1 Stakeholders

7.1.1 Internal stakeholders

Internal stakeholders should include:

a) User

b) Business service platform

c) DLT-based digital integrity proofing platform.

7.1.2 External stakeholders

External stakeholders include:

a) Third-party support services, including organizations that provide CA certificate issuance, time service and other services;

b) Regulatory agencies, including national judicial agencies, and other litigation-related organizations.

7.2 Processes of DLT-based digital integrity proofing

7.2.1 Digital integrity proof registration

The key processes of digital integrity proof registration on the DLT include:

a) The user interacts with the business service platform and may generate the needs to protect the authenticity of the business-related information, the business platform sends the extracted features of the original information to the DLT-based digital integrity proofing platform;

b) The DLT-based digital integrity proofing platform generates electronic evidence with the extracted features, time stamp, and other necessary information;

c) The DLT-based digital integrity proofing platform generates a unique hash value for the electronic evidence through cryptographic hash functions (such as SHA256);

d) The business service platform generates a digital signature for the hash value with the owner's private key;

e) The business service platform submits the proof record to the smart contract address on the distributed ledgers;

f) The DLT-based digital integrity proofing platform checks whether the digital signature and information are complete and executes the smart contract and generates a record in the ledger;

g) The proof registration is packaged into a new block and the new block is broadcast to the network.

7.2.2 Digital integrity proof provenance

The key process of digital integrity proof provenance include:

a) The user queries the digital integrity proof on the distributed ledgers;

b) In case of online litigation, the litigation platform conducts forensics for the digital proof based on the records on the distributed ledgers.

8 Security threats for DLT-based digital integrity proofing

This clause analyses security threats to the stakeholders, i.e., user, DLT-based digital integrity proof platform, and the processes involved in DLT-based digital integrity proofing, namely, digital integrity proof registration, and digital integrity proof provenance. Threats to protocol, network and data components in DLT-based applications are described in detail in [ITU-T X.1401].

8.1 Security threats w.r.t user

8.1.1 User identity fraud

Registered users make illegal requests using false identities to obtain permissions that do not match their identity.

8.1.2 Private key leakage

The threats of private key leakage in a registry mainly include software client attacks and physical attacks (e.g., exposure of printed keys to others). The leakage of a private key enables other users to enter the DLT-based proof platform, compromising its security. The private key leak threat is described in detail in clause 6.3.2 of [ITU-T X.1401].

8.1.3 Private key loss

The threats of private key loss mainly include malware attacks, physical attacks (e.g., loss of private keys printed on paper), etc. These behaviours may lead to the disclosure of user privacy which allows malicious users to enter the DLT-based proof platform and destroy its security. The private key loss threat is described in detail in clause 6.3.3 of [ITU-T X.1401].

8.1.4 Privacy disclosure

The proof information of the owner may involve sensitive personal information such as name and ID information, and there may exist a problem of user privacy leakage during the proof registration process. The privacy disclosure threat is described in detail in clause 6.3.1 of [ITU-T X.1401].

8.2 Security threats w.r.t proof registration

8.2.1 Proof fraud

According to the feature extraction algorithm of digital proof, attackers could construct different feature values of similar content to the original document. In this way, attackers could write illegal content in distributed ledgers.

8.2.2 Proof tampering

The malicious user may tamper with the proof of the original document or destroy the integrity and availability of the proof, thereby resulting in writing the tampered proof into the distributed ledgers. Asymmetric encryption algorithm attacks can result in insecure transmission and storage. The asymmetric encryption algorithm attack is described in detail in clause 6.1.5 of [ITU-T X.1401].

8.2.3 Timestamp dependence attack

Attacks may manipulate the timestamp service of the DLT-based proof platform, resulting in the platform being unable to keep the sequence of proof registration events accurately, thus lacking the capability to provide an effective forensics basis for the provenance of proof.

8.2.4 51% attack

When attackers master more than 51% of the computing power, they can construct a new chain. The new chain can invalidate the main chain proof. Furthermore, a 51% attack may result in the successful registration of the infringer. The 51% attack is described in detail in clause 6.1.1 of [ITU-T X.1401].

8.2.5 Briber attack

When attackers with sufficient resources bribe nodes with voting rights, they can damage the rights and interests of a proof distributed ledger network. In this way, attackers write illegal proof information in the proof distributed ledger network. A bribing attack is described in detail in clause 6.1.1 of [ITU-T X.1401].

8.2.6 Block-withholding attack

On a DLT-based proof platform based on the proof of work (PoW) consensus algorithm, an attacker can keep a block they mined and mines the next block in secret if the attacker has enough power. By releasing more than one block when other miners generate a block, the attacker can make other miners waste their power. The target of the attack is a platform operator that accepts zero validation. It can invalidate the main chain proof. It may also result in the successful registration of the infringer. The block-withholding attack is described in detail in clause 6.1.1 of [ITU-T X.1401].

8.2.7 Chain-hopping attack

An attacker can switch between various blockchains by taking advantage of the difficult adjustment algorithms of the chain. It can lead to an unfair reward toward the attackers with a loss to the other users. It may also cause a considerable increase in the effective computing power in the mining pool. It may also result in the successful registration of the infringer. The chain-hopping attack is described in detail in clause 6.1.1 of [ITU-T X.1401].

8.2.8 Distributed denial of service attack

On a DLT-based proof platform, an attacker can disenable the network through distributed denial of service (DDoS) attacks, with sybil attack and eclipse attack being the common methods. This may result in the successful registration of malicious proof. The sybil attack is described in detail in clause 6.2.3 and the eclipse in clause 6.2.1 of [ITU-T X.1401].

8.2.9 BGP hijacking attack

An attacker can take advantage of the hijacked border gateway protocol and the network nodes of the distributed ledgers gets divided into two or more parts. As a result, the DLT is split into two or more parallel chains. At this time, the proof registration and the malicious proof registration can be done on parallel branches. After the attack stops, the proof distributed ledger is reunified with the longest main chain, other branches are discarded, and all proof records on these chains become invalid which can result in the successful registration of malicious proof.

8.3 Security threats w.r.t proof provenance

8.3.1 Malicious information writing attack

All transaction data in the DLT are non-removable. Once the information is written into the DLT it cannot be deleted. Attackers may write malicious information in the distributed ledgers by launching smart contract attacks, e.g., mishandled exceptions attacks, as described in detail in clause 6.1.2 of

[ITU-T X.1401]. The platform generates new blocks which lead to spam block attacks, thereby affecting the performance of a DLT-based proof platform.

8.3.2 Proof information disclosure

In proof provenance, an algorithm should be used to encrypt and store proof information. It is important to ensure the security of the encryption algorithm. Asymmetric encryption algorithm attacks can result in an insecure state of the DLT-based proof platform. The asymmetric encryption algorithm attack is described in detail in clause 6.1.5 of [ITU-T X.1401].

9 Security requirements for DLT-based digital integrity proofing

This clause describes security requirements for DLT-based digital integrity proofing based on the analysis of security threats outlined in clause 7. In addition, this clause describes the security requirements for the stakeholders, i.e., user, digital integrity proofing platform, and processes involved in DLT-based digital integrity proofing services, namely, digital proof registration, and digital proof provenance. The requirements for the security of data, network, consensus and application are described in detail in clauses 8.1 to 8.4 of [ITU-T X.1402].

9.1 Security requirements for a user

9.1.1 Protection of user identity

The following security requirements related to the avoidance of identity fraud are defined for DLT-based digital integrity proofing platform.

a) The DLT-based digital integrity proofing platform should specify the operating authority of different users. The platform should allow the user to use the private key to sign the information and send it to the DLT. The DLT should recover the public key based on the signature, identify the users based on the public key, and authenticate user operations;

b) When a user registers into the platform, the platform shall first audit the user's identity information and may then allocate a label to each user;

c) The DLT-based digital integrity proofing platform should write all the operations of each user into the distributed ledgers;

d) The DLT-based digital integrity proofing platform should require the provision of an identity authentication function for each proof registration, including access control, password, digital signature and biometric recognition, etc.

9.1.2 Private key protection

The following security requirements related to private key protection are defined for DLT-based proof platform.

a) The DLT-based digital integrity proofing platform should prevent private key leakage – a DLT-based proof platform operator should prevent malicious code from intruding into its client;

b) The DLT-based digital integrity proofing platform should prevent private key loss – users of a DLT-based proof platform should keep the private key in a safe place and avoid leaving the private keys on easily accessible non-physical and physical media (e.g., printing paper) without any protection mechanisms – potential countermeasures include personal identification number codes, passwords, fingerprints and other biometric information, etc.

9.1.3 Privacy protection

The DLT-based digital integrity proofing platform should adopt relevant security protection measures in the information processing links of collection, storage, use, sharing, transfer, public disclosure, etc., to prevent illegal collection, abuse, and leakage of owner information, and to maximize the protection of the legitimate rights and interests of the owner.

9.2 Security requirements for proof registration

9.2.1 Avoidance of proof fraud

The following security requirements related to avoidance of digital proof fraud are defined for a DLT-based proof platform.

a) The DLT-based proof platform should provide consensus algorithms with a level of security assurance (LoSA) and a consensus mechanism strength (CMS) [ITU-T X.1404], e.g., practical byzantine fault tolerance (PBFT), to avoid digital proof forgery;

b) The DLT-based proof platform should monitor the effective computing power of the network, to detect abnormal changes and to prevent chain-hopping attacks;

c) The DLT-based proof platform should enhance the difficulty of eigenvalue construction algorithms while ensuring that the operating efficiency of the system is within a reasonable range.

9.2.2 Avoidance of proof tampering

The following security requirements related to the avoidance of digital proof tampering are defined for a DLT-based proof platform.

a) The DLT-based proof platform should use encrypted hardware;

b) The DLT-based proof platform should use encryption algorithms to ensure the secure transmission of proof information. The related third-party services should use encryption algorithms to ensure the secure storage of proof information. The platform and related third-party services should choose appropriate encryption algorithms, which should have a compromise between security and computing cost, and key length – it might choose to increase the length of keys to offset the risks caused by the increasing computing power.

9.2.3 Protection of proof registration

The following security requirements related to registration security control are defined for a DLT-based proof platform.

a) The DLT-based digital integrity proofing platform shall synchronise to a trusted third-party time service;

b) The DLT-based digital integrity proofing platform should provide warnings of security attack, vulnerability, malicious code, threat analysis and data leakage, as well as other threat intelligence information, and identify the problems existing in the platform through vulnerability scanning and automated security testing;

c) The DLT-based digital integrity proofing platform should provide identity authentication and access control to mitigate security attack risks, e.g., malicious tampering and remote attack;

d) For mobile applications, the DLT-based digital integrity proofing platform should provide security protection methods, e.g., reinforcement and source confusion to prevent reverse analysis, decompilation and embedding of malicious code;

e) The platform can use the monitoring point technology to write to the client through hard coding so that the client will accept all of the effective transactions before the monitoring point, thereby preventing 51% attack – the monitoring point should: introduce an improved proof of stake (PoS) consensus mechanism with margin and penalty measures; set a time stamp for the transaction; set third-party reliable node authentication to authenticate identity; and not accept zero confirmation;

f) The platform can deploy port filtering for abnormal traffic cleaning, cloud security defence, and high defence for domain name system (DNS) resolution in the system to provide secure implementation, and should regulate data block size to avoid spam attacks;

g) The DLT-based digital integrity proofing platform should provide evidence collection and tracing of security incidents, analyse the reasons and provide methods to contain attacks.

9.3 Security requirements for proof provenance

9.3.1 Prevention against malicious information writing

To ensure the security of proof provenance the DLT-based digital integrity proofing platform should:

a) regulate the size of the data block to prevent nodes from generating spam blocks;

b) ensure that unauthorized and anonymous entities cannot search or access account data and transaction data in distributed ledger system nodes;

c) use libraries that guarantee calculation safety, such as SafeMath;

d) perform code reviewing to avoid integer flow and mishandled exceptions to prevent attacks in smart contracts;

e) use unpredictable random generators to prevent malicious users to control the outcomes of the smart contracts;

f) The design of access control during program development should be as strict as possible to prevent the ownership of smart contract functions from being tampered with by attackers to obtain the highest operating authority.

9.3.2 Protection of proof information

To ensure the security of proof information the DLT-based digital integrity proofing platform should:

a) use encrypted hardware to store the proof information of off-chain;

b) choose appropriate encryption algorithms which should have a compromise between security and computing cost, and key length – it might choose to increase the length of the keys to offset the risks caused by increasing the computing power;

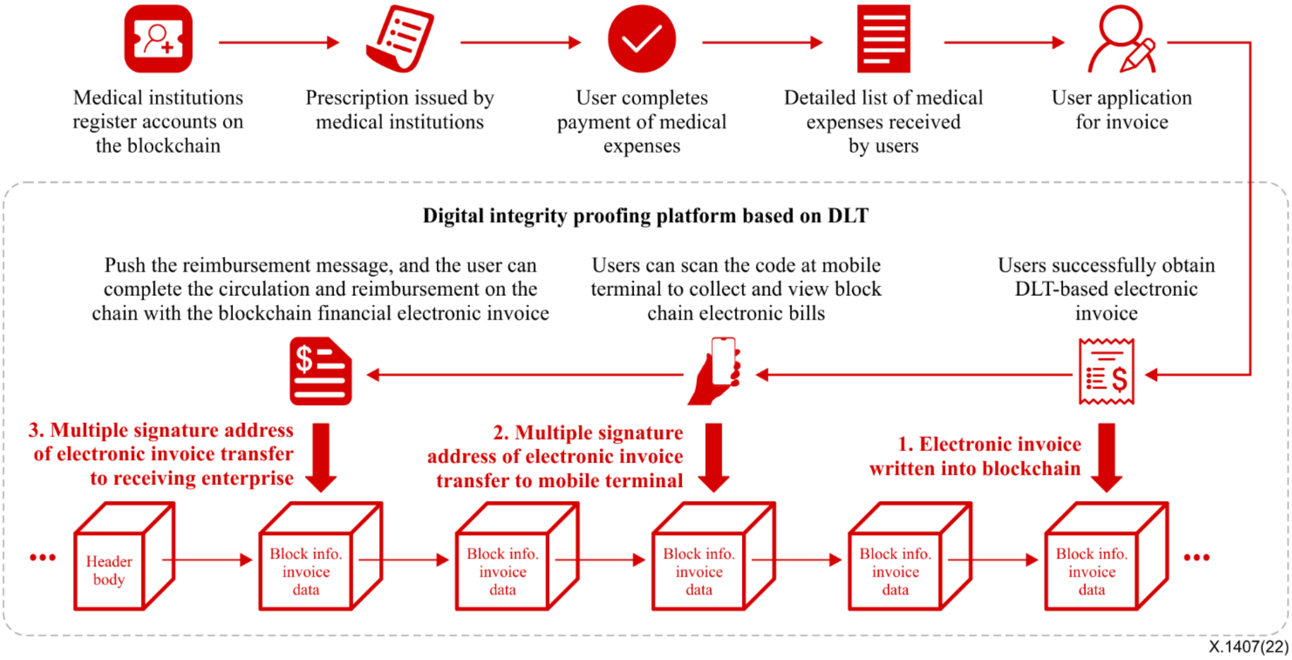
c) use an effective access control mechanism to ensure controllable access to proof information.

Appendix I

Use case of e-invoice based on distributed ledger technology

(This appendix does not form an integral part of this Recommendation.)

Under the consensus mechanism only invoices written by tax authorities can be verified and approved, and invoices written by any other nodes cannot be confirmed, thus ensuring the authenticity of invoices. With smart contracts, transactions and invoicing occur simultaneously, and consumer payments and invoicing takes place seamlessly. An overview is given in Figure I.1. For details, please refer to [b-IEEE 2142.1-2021] Recommended practice for e-invoice business using blockchain technology.



Medical institutions register accounts on the blockchain
Prescription issued by medical institutions
User completes payment of medical expenses
Detailed list of medical expenses received by users
User application for invoice
Digital integrity proofing platform based on DLT
Push the reimbursement message, and the user can complete the circulation and reimbursement on the chain with the blockchain financial electronic invoice
Users can scan the code at mobile terminal to collect and view block chain electronic bills
Users successfully obtain DLT-based electronic invoice
3. Multiple signature address of electronic invoice transfer to receiving enterprise
2. Multiple signature address of electronic invoice transfer to mobile terminal
1. Electronic invoice written into blockchain
Header body
Block info. invoice data
Block info. invoice data
Block info. invoice data
Block info. invoice data
Block info. invoice data
X.1407(22)

Figure I.1 – Use case overview of DLT-based electronic invoice

The use case of electronic invoices based on distributed ledger technology by medical institutions is described as follows:

a) Medical institutions register an account on the blockchain, connect to the DLT-based invoicing system and set the invoicing conditions on the chain

b) The medical institution issues a prescription

c) The user completes the payment of medical expenses with a prescription

d) The user receives a detailed list of medical expenses after the payment is completed

e) The user applies for invoicing

f) The user successfully obtains a blockchain electronic invoice

g) Users can scan the code on the mobile terminal to receive and view the blockchain electronic invoice

h) The mobile terminal can push reimbursement messages, and users can use the blockchain electronic invoice to complete the circulation and reimbursement on the chain.

The invoicing process based on the payment may include the following phases:

– Phase A: transaction

– Phase B: invoice issuance
– Phase C: reimbursement
– Phase D: tax clearance

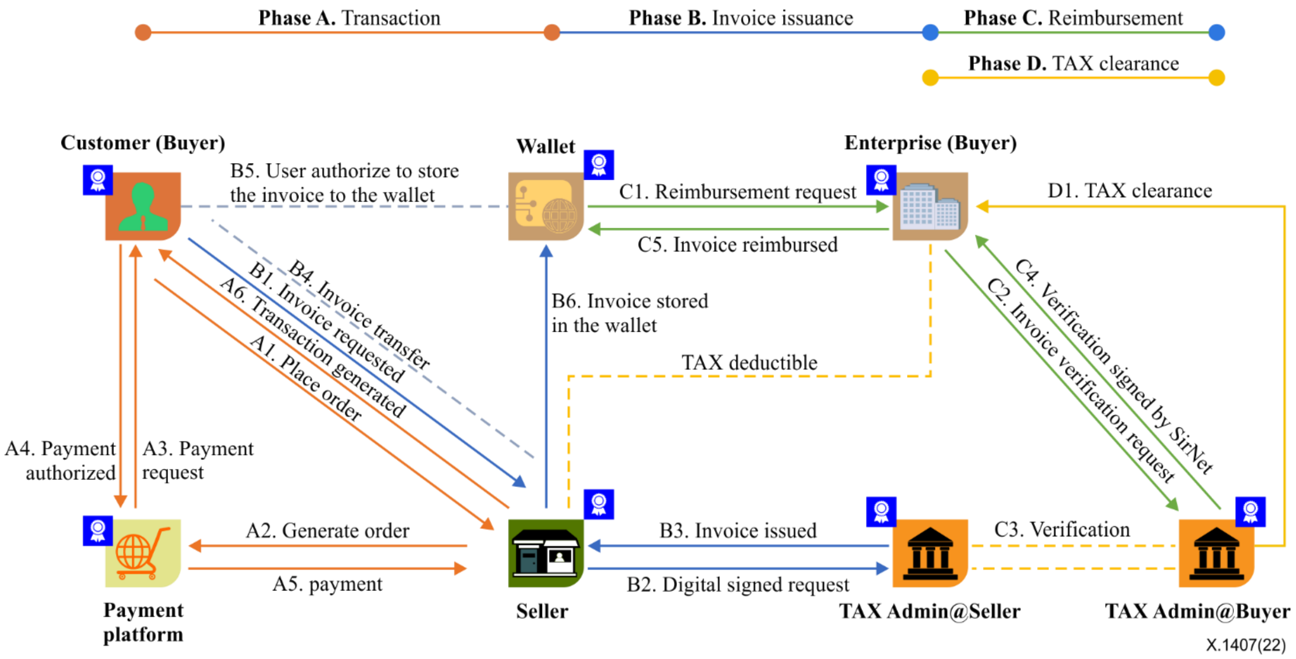


Figure I.2 – Use case flow chart of DLT-based electronic invoice

In the transaction phase, when the customer (i.e., buyer) places an order, the service provider (i.e., seller) generates the order over the payment platform, the payment platform then confirms the order after the customer authorization is received, and the receipt is generated when the payment is processed. The receipt could be in the form of a payment block over a payment chain or a record in a centralized database.

In the invoice issuance phase, the invoice is issued by the origin TAX admin of the merchant based on the customer's request from the customer's wallet for instance, and the payment receipt is used as the unspent transaction output (UTXO) for the invoice issuance. The participating nodes include the core consensus nodes anchored on the core layer of the ledger as well as the simplified payment verification (SPV) nodes, such as the merchant node, personal wallet node, etc.

In the reimbursement phase, the customer associating enterprise (CAE) as an SPV node verifies the invoice when the customer initiates the reimbursement process, and the invoice in the personal wallet is repaid as a UTXO.

In the TAX clearance process, the destination TAX admin nodes and the CAE SPV node join the process, the invoice is used as UTXO to repay the VAT.

There are several advantages to the electronic invoice system using DLT as follows:

1. Ensure that the invoice is authentic and the whole process of invoice collection, invoice issuing, circulation, entry, reimbursement is traceable.
2. The invoice data is tamper-proof and the tax bureau, the billing party, the circulation party, and the reimbursement party participate jointly in the bookkeeping process.
3. DLT-based e-invoice does not need tax-disk and special equipment. For traditional invoices, it requires multiple tax-disks for each store in the case of chain stores; The DLT-based e-invoice is automatically reimbursed by the ERP and the number of stores does not bring additional cost.

4. For traditional invoices, if the number of invoices approved by the tax authorities cannot meet the business needs due to a temporary increase in business volume, the taxpayer may apply for additional invoices to the tax authorities. However, DLT-based invoices are supplied on demand and do not need additional application processes.

5. It takes time and effort to collect and purchase traditional invoice papers from the tax bureau; while DLT-based e-invoices are paper free.

Appendix II

Use case for verification of academic certificates based on distributed ledger technology

(This appendix does not form an integral part of this Recommendation.)

Verification of certificates is a time-consuming process as it may require days or weeks. Employers are concerned about the authentication of qualifications and spend considerable time communicating with universities to verify the integrity of certificates and to ensure applicants hold an impeccable qualification. Blockchain will provide transparency and simplify sharing the authenticated certificates with a variety of employers or any other parties.

Employers can prove the integrity of the academic certificate by using DLT. DLT provides a recognized secure source to store students' qualifications, accessible by a variety of institutions and universities. It provides a persistent public record, safeguarded against changes to the institution or loss of its private records.

This pattern consists of the following components:

Users

– Issuer (University)

– Recipient (Students)

– Verifier (Employers)

Systems

– The nodes of universities.

– Blockchain platform

Data

– The certificates hashes

– Electronic certificate file

The process of checking the integrity of the certificate depends on checking the hash value of the certificate and comparing the hash with the hashes stored in the blockchain as displayed in Figure II.1. The steps include:

– University issues a new electronic certificate for a student and uploads the file into DLT.

– DLT hashes and stores the file of the certificate.

– To show proof of integrity, the student or employer uploads the document of the certificate into the DLT platform.

– DLT generates the hash for the document and then compares the generated hash value with the hashes stored on the blockchain.

– If the generated hash match one of the hashes stored in the blockchain then the certificate is authentic.

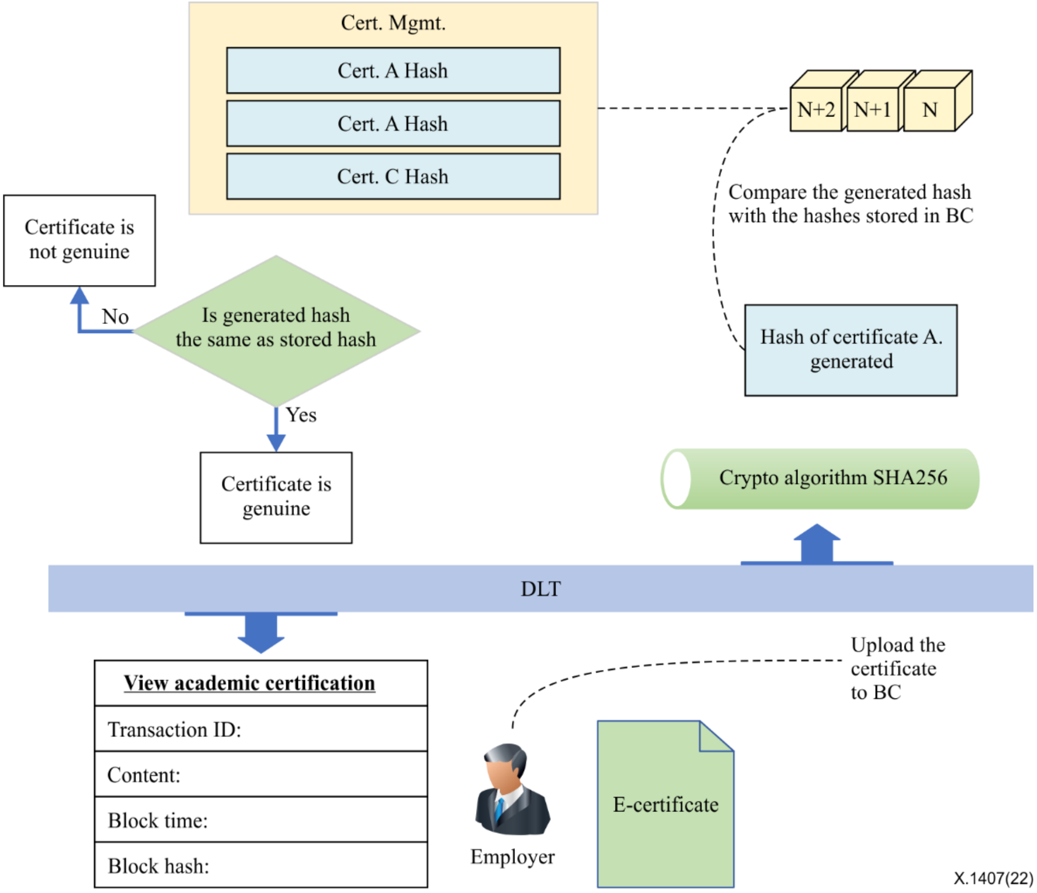

Cert. Mgmt.
Cert. A Hash
Cert. A Hash
Cert. C Hash
N+2
N+1
N
Compare the generated hash with the hashes stored in BC
Certificate is not genuine
No
Is generated hash the same as stored hash
Hash of certificate A. generated
Yes
Certificate is genuine
Crypto algorithm SHA256
DLT
View academic certification
Transaction ID:
Content:
Block time:
Block hash:
Upload the certificate to BC
Employer
E-certificate
X.1407(22)

Figure II.1 – Use case overview of DLT-based verification of academic certificate

Benefits of using DLT to authenticate the academic certificates:

– DLT solves the current difficulties in the validation and authentication process.

– DLT can group all the universities in one single platform.

– DLT technology encourages employers to work with universities systematically.

– DLT helps save and share authentic and integral information as one source of truth.

– DLT saves time, cost, and effort.

Bibliography

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

[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 23257] ISO 23257:2022, *Blockchain and distributed ledger technologies – Reference architecture.* [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-ISO 22739] ISO 22739: 2020, *Blockchain and distributed ledger technologies – Vocabulary*.
<https://www.iso.org/standard/73771.html>

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

[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-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

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