International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1405

(06/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

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

Security threats and requirements of digital payment services based on distributed ledger technology

Recommendation ITU-T X.1405

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	X.1140–X.1149
Security protocols (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.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	**X.1400–X.1429**
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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
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
IMT-T SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1405

Security threats and requirements of digital payment services based on distributed ledger technology

Summary

Recommendation ITU-T X.1405 focuses on payment services use cases. Based on the analysis of use cases, the service model is described and security threats and challenges are also analysed.

As various digital financial services based on digital ledger technology are developed and operated in the real world including transaction accounts, payments services, saving accounts, investment services and insurance services. Hence, this Recommendation also provides a list of security requirements that are specified against threats and challenges.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1405	2021-06-29	17	11.1002/1000/14722

Keywords

Challenges, digital financial services, distributed ledger technology, digital payment services, security requirements, threats.

* 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/.

© ITU 2021

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

Table of Contents

Recommendation ITU-T X.1405

Security threats and requirements of digital payment services based on distributed ledger technology

1 Scope

This Recommendation identifies security threats and specifies security requirements for digital payment services based on distributed ledger technology (DLT). Security threats and challenges are analysed based on use cases and security requirements are specified against the identified threats and challenges.

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 for distributed ledger technology*.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined 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 node [b-ITU-T X.1400]: Device or process that participates in a distributed ledger network.

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

3.1.4 digital financial services (DFS) [b-ITU-T DSTR-DFSECO]: Digital financial services include methods to electronically store and transfer funds; to make and receive payments; to borrow, save, insure and invest; and to manage a person's or enterprise's finances.

3.1.5 payment services [b-ITU-T DSTR-DFSECO]: The ability to transfer money into or out of an account: this may be done through a variety of different payments systems and providers. Remittances, transfers, merchant payments, bill payments, etc. are all examples of payments. Payments may be domestic or cross-border.

3.1.6 remittance [b-ITU-T DSTR-DFSECO]: A digital funds transfer which is the exchange of funds from one user to another through a DFS provider using electronic means, including a mobile handset, to either initiate and/or complete the transaction. A remittance could be domestic or international. International remittance transactions are normally cross-currency as well, the transaction requires someone – either the sending or receiving party, or the providers who are serving them, to affect the currency exchange.

3.1.7 permissionless [b-ISO 22739]: Not requiring authorization to perform any particular activity.

3.1.8 permissioned [b-ISO 22739]: Requiring authorization to perform any particular activity or activities.

3.1.9 token [b-ISO 22739]: Digital asset that represents a collection of entitlements.

3.1.10 smart contract [b-ITU-T X.1400]: Computer program recorded on the distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated, and invoked by specific applications and also automatically executed after all the preconfigured set of conditions are met.

3.1.11 DApp [b-ISO 22739]: Application that runs on a decentralized system.

3.1.12 sensitive data [b-ISO 5127]: Data with potentially harmful effects in the event of disclosure or misuse.

3.1.13 DLT user [b-ISO 22739]: Entity that uses services provided by a distributed ledger technology (DLT) system.

3.1.14 DLT system [b-ISO 22739]: System that implements a distributed ledger.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 sub-distributed ledger: Logically separated subset of a distributed ledger to enhance confidentiality.

3.2.2 participant: Entity who participates in the DLT system's decision making. For example, miners, validators, node owners, orderers, voters, etc.

3.2.3 orderer: Service that orders transactions into a block for validation and commits, or node that provides the service. Some DLT systems have this service and some do not.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DFS Digital Financial Services

DLT Distributed Ledger Technology

DoS Denial of Service

KYC Know Your Customer

5 Conventions

None.

6 A basic model of digital payment services using DLT

6.1 General

Digital payment services are used to transfer money from one account to another. Varieties of payment services exist but the difference between merchants and their systems are not given in the scope of this Recommendation. In the digital financial services (DFS) ecosystem, the challenges that telecommunications service providers have to cover; range from agent devices (including mobile devices and computing devices) to payment service provider networks.

Impact of threats on distributed ledger technology (DLT) based payment systems vary according to its implementation primarily on the basis of permissionless and permissioned DLT services.

Therefore, two different service use cases are further explained to analyse the effects of general threats on DFS and DLT.

6.2 Use case of digital payment service based on permissionless DLT

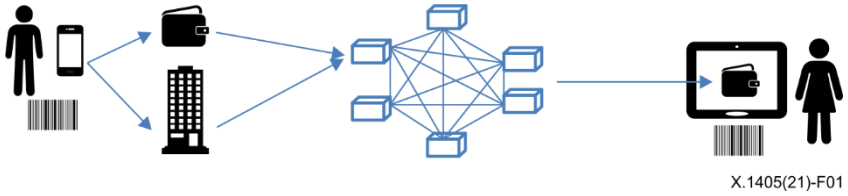

Figure 1 – Permissionless use case

Generally, a sender should know the receiver's account to pay. In permissionless DLT systems, DLT users do not need any permission for sending any transaction nor registration to use the services. The receiver's account is typically a hash of the receiver's public key. Also, the sender should have a token which is used in the DLT system to save or transfer value. These tokens are stored in a digital wallet which are either software or hardware.

To send a specific amount of value, a sender accesses their digital wallet in their own terminal device or in the custody of a custodian. The payment transaction is signed with the sender's private key and then sent to the DLT system network.

The payment should be accepted when the nodes in the distributed ledger network record the transaction in the ledger enough to be believed that further modifications will not take place.

6.3 Use case of digital payment service based on permissioned DLT

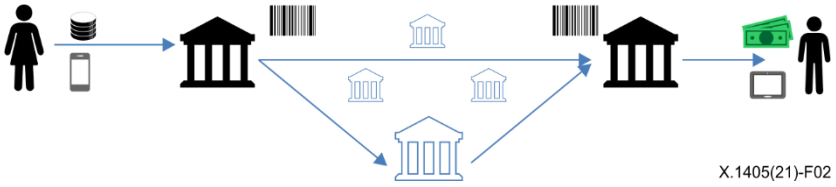

Figure 2 – Permissioned use case

Users should register themselves to the DLT system to use its services. The system verifies the user's identity and opens the user's account. The sender accesses their terminal to execute payment to the receiver's account. If there exists a sub-distributed ledger (sub-DLT) which manages users, and the receiver is registered with a different sub-distributed ledger from the sender's, then the sender's sub-DLT sends the transaction of the sender to the receiver's sub-DLT for recording. According to the DLT implementation, a third sub-DLT might be required to connect sender's and receiver's sub-DLTs.

If those sub-DLTs use different tokens, the sender's token should be converted to the receiver's, or another third one that can be commonly converted for both the sender's and receiver's payment transfer.

6.4 A simplified model of digital payment systems based on DLT

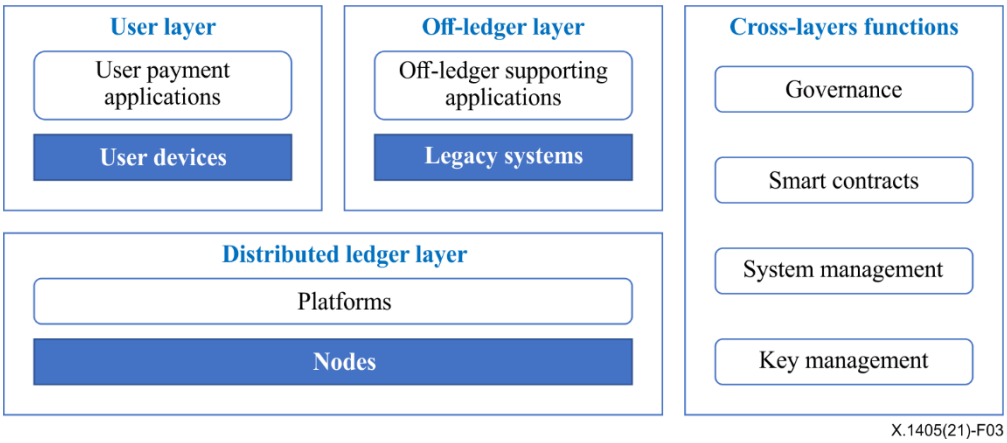

Figure 3 – A simplified model of digital payment systems based on DLT

From both previous use cases, a simplified model of digital payment systems is derived as seen in Figure 3. The user layer includes user devices and digital payment applications using DLT and may interact with off-ledger supporting applications such as legacy ICT systems performing payment functions. Off-ledger supporting applications should address contractual or regulatory requirements that cannot be achieved in the DLT layer, for example, a know your customer (KYC) requirement or an anomality detection. Distributed ledger layer (DLT layer) includes nodes and platforms running on them. This platform also includes many components such as interfaces, consensus mechanism, event management, etc. Cross-layer function includes many functions that cover governance, system management, smart contract management, key management, etc. Those functions can be performed across all three layers. In permissionless DLT systems, most functions tend to be merged and performed in the platform, but in permissioned DLT systems, these functions tend to be distributed into several components in the DLT systems.

7 Security threats and challenges

7.1 General threats and challenges for DLT

7.1.1 Introduction

General threats for DLT and their details are provided in [ITU-T X.1401]. The general security capabilities of DLT responding to these threats are addressed in [ITU-T X.1402].

In [ITU-T X.1401], threats for DLT are categorized into protocol (see clause 6.1 in [ITU-T X.1401]), network (refer clause 6.2 in [ITU-T X.1401]) and data (see clause 6.3 in [ITU-T X.1401]) layers. In this Recommendation, the threats are listed below with references to the corresponding clause numbers of [ITU-T X.1401].

7.1.2 Consensus mechanism threats

These threats are described in clause 6.1.1 in [ITU-T X.1401].

7.1.3 Smart contract threats

These threats are described in clause 6.1.2 in [ITU-T X.1401].

7.1.4 Virtual machine threats

These threats are described in clause 6.1.3 in [ITU-T X.1401].

7.1.5 Cryptographic hash algorithm threats

These threats are described in clause 6.1.4 in [ITU-T X.1401].

7.1.6 Asymmetric cryptographic algorithm threats

These threats are described in clause 6.1.5 in [ITU-T X.1401].

7.1.7 Threats from practical quantum computers

These threats are described in clause 6.1.6 in [ITU-T X.1401].

7.1.8 Node routing table threats (NRTT)

These threats are described in clause 6.2.1 in [ITU-T X.1401].

7.1.9 Network DDoS threats

These threats are described in clause 6.2.2 in [ITU-T X.1401].

7.1.10 Node identity threats

These threats are described in clause 6.2.3 in [ITU-T X.1401].

7.1.11 Network routing threats

These threats are described in clause 6.2.4 in [ITU-T X.1401].

7.1.12 Account data and transaction data threats

These threats are described in clause 6.3.1 in [ITU-T X.1401].

7.1.13 Private key leakage threats

These threats are described in clause 6.3.2 in [ITU-T X.1401].

7.1.14 Private key loss threats

These threats are described in clause 6.3.3 in [ITU-T X.1401].

7.1.15 Transaction threats

These threats are described in clause 6.3.4 in [ITU-T X.1401].

7.2 General threats and challenges for traditional financial systems

7.2.1 Account set-up threats

Traditional financial systems possess the threat of physical theft of identity credentials or counterfeiting of identity documents. DLT-based identity management makes counterfeiting identity documents easier.

7.2.2 Transaction threats

Traditionally, financial systems possess the threat of physical theft of payment credentials and counterfeit signatures. Further, remote commerce may also enable payment mechanisms with fewer protections; credentials used online or in stores may be breached and thefts of personal identification numbers (PINs), etc. are much easier.

7.2.3 Scheme threats (scam)

Traditional cash collection systems, SMS and e-mail spam can affect more targets; a further collection of funds via electronic transfers makes large-scale scams easier.

7.2.4 Systematic threats

Traditionally, back-office branch account manipulations, etc. The complexity of large-scale MIS systems may make regulatory control difficult and may give rise to systematic frauds.

In DLT, the implementation protocols continue to evolve for scalability and performance. Those protocol changes might bring forks. Also, some new techniques such as sharding or segregated witness may be insecure.

7.2.5 Money laundering / terrorist financing threats

Traditionally, cash and bank account transfers. Pervasive DFS could enable large scale small-value transfers, which are harder for regulators to detect as till now only few mechanisms and regulations exist to control digital currencies and for overseeing their use.

7.3 Threats and challenges specific for DLT-based digital payment systems

7.3.1 Insecure custodial and safekeeping services threats

Poor security of custodians and inappropriate customer wallets usage. In some cases, the trust of custodians is not guaranteed.

7.3.2 Interoperability challenges

Most DLT systems are developed with their own proprietary standards and technologies, and therefore cannot interoperate with other DLT systems. This lack of interoperability and supporting standardizations introduces elements of inconsistency and challenges in the use of DLT systems and may create a barrier for entry of new DLT systems.

7.4 Threat analysis for digital payment services using DLT

7.4.1 Analysis of traditional financial threats on digital payment services based on DLT

Traditional financial services include payment services, and the threats on them are applied to the payment services, too. However, even the same might affect differently and in different scenarios depending on the structure of the target system. In order to derive specific security requirements, it should be understood which parts of the system are affected by which threats and how. Some of the threats explained in the previous clauses can be realized in several scenarios, each of which can be broken down into smaller activities. For example, clause 7.2.1 account set-up threats can be realized when attackers steal a user's device and get the private key by exploiting the vulnerability of the device. If the user uses a paper wallet and someone copies the paper, the key is compromised without theft. In some permissionless DLT systems, a DLT account is derived from the private key. Some permissioned DLT systems may require other kinds of online or offline documents but it depends on the specific system's membership policy. That sort of key theft is also a component of clause 7.2.2 transaction threats. On the other hand, transactions in DLT systems may bring other kinds of threats that are not of main concern in the exposure of sensitive data.

Scheme threats in clause 7.2.3 are not technical threats. The vulnerable component is an uninformed human. To address this kind of threat, off-ledger or non-technical processes are required. Money laundering and terrorist financing are also a human threat, not uninformed, but highly-crafty humans who make well use of a DLT system that works perfectly for its original purpose. What makes the transactions and payment different from others is not in the DLT system.

Systematic threats are rather special. Those threats consist of fraudulent humans and flawed systems. In many cases, there are insiders present, which is contrary to scam or money laundering cases. Flawed systems cover plenty of components and related threats. The most famous threats to DLT payment is double spending. Network partitioning increases the likelihood of successful double spending attacks by delaying the consensus reached for the entire network. Those many DLT systems vulnerabilities and attacks are addressed in [ITU-T X.1401] and [ITU-T X.1402]. However, the

insiders familiar with the system will be able to plant well-developed smart contracts like a Trojan in a traditional ICT system.

7.4.2 Threats and challenges on permissionless DLT systems

As the threats/attacks affect one or more parts of the DLT systems, different DLT systems may have different vulnerabilities according to their implementation. Figure 4 shows how permissionless DLT systems might be vulnerable to some common attacks. In general, a permissionless DLT system does not check or limit the participant's qualifications. It allows all the participants to validate transactions and leaves everything to the user's discretion.

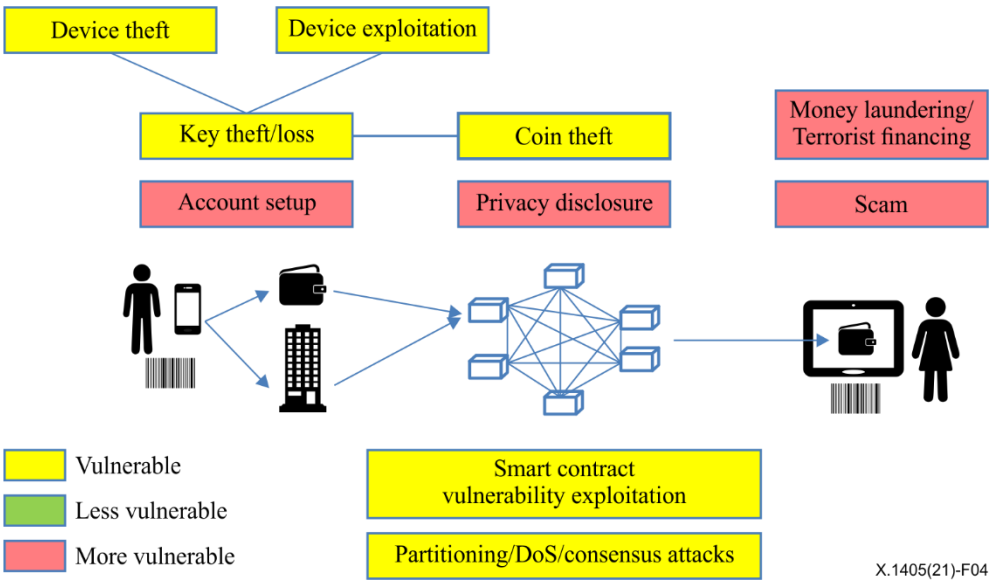

Figure 4 – Threats and challenges on permissionless DLT systems

7.4.3 Threats and challenges on permissioned DLT systems

On the other hand, in permissioned DLT systems, participants are limited and supervised by the rule outside of the DLT system. Permissioned DLT systems usually connect traditional ICT systems that comply with the off-ledger rules, contrary to the permissionless systems that operate according to the rules coded on the ledger. Figure 5 indicates that the permissioned DLT systems have some means to address the same threats compared to the permissionless DLT systems.

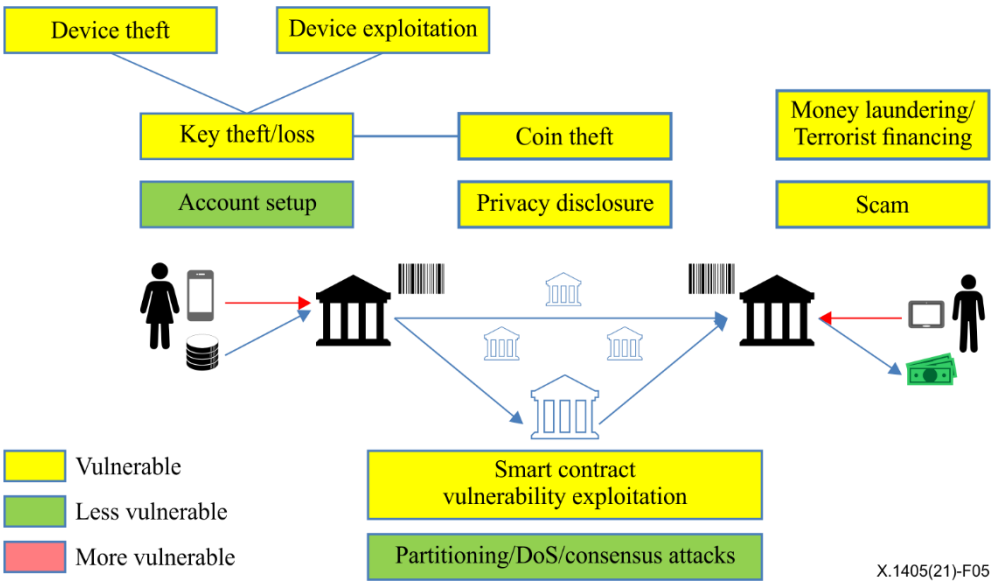

Figure 5 – Threats and challenges on permissioned DLT systems

Table 1 shows how the threats and challenges work with use cases described in clause 6.

Table 1 – Possibility of response to threats to digital payment services according to use cases

Threats	Permissionless	Permissioned
Key theft/loss	Depending on the key management	Depending on the key management
Account set-up	No registration	Depending on the security of the user registration process and key management
Sensitive data disclosure	Public access to transaction data	Depending on the operation policy of sub-DLT systems
Smart contract vulnerability exploitation	Depending on the vulnerability of the smart contract code	Depending on the vulnerability of the smart contract code and management process
Partitioning attack	Depending on the peer management implementation	Depending on the node management implementation
Denial of service (DoS) attack	Depending on the transaction (block) validation policy	Depending on the node management policy and the transaction (block) validation policy
Consensus attacks	Depending on the consensus algorithm (ex. Nakamoto consensus)	Depending on the consensus algorithm (ex. PBFT consensus)
Money laundering / terrorist financing	No restriction	Depending on the anti-ML/ATF policy and implementation
Scam	No restriction	Legal intervention

8 Security requirements for digital payment systems based on DLT

8.1 Security requirements

This section specifies security requirements against the security threats and challenges of digital payment systems based on DLT. General security threats and challenges of DLT are addressed in [ITU-T X.1402].

8.2 Security requirements on user devices

8.2.1 Device shall have the capability of protecting the stored data on theft/loss, for example, using remote inactivation.

8.2.2 Important data, for example, private key, etc. in devices shall be backed up appropriately.

8.2.3 User shall be properly authenticated while accessing the device.

8.2.4 During the usage of the app, both integrity checks for the device and app shall be performed.

8.2.5 Generation and management of keys shall be done in a secure manner. For example, keys shall be stored in an encryption and not in plain text, and key recovery mechanisms for legitimate users shall be provided.

8.3 Security requirements on nodes

8.3.1 Nodes shall verify peers in communication.

8.3.2 Servers run nodes shall be sanitized and hardened.

8.3.3 Node security shall be regularly checked.

8.4 Security requirements on distributed ledger system management

8.4.1 Secure cryptographic algorithms and keys shall be used.

8.4.2 If necessary, the user's real name shall be verified on the creation of an account.

8.4.3 Transactions shall be monitored to detect attacks and anomalies, where applicable, including fraud, scam, money laundering, terrorist financing, etc.

8.4.4 Incident response procedures shall be in place for fault, hacking, denial of service (DoS) attack, where applicable, illegality, etc.

8.5 Security requirements on sensitive data

8.5.1 Data confidentiality shall be provided for sensitive data, for example, by encryption or subchannel, etc.

8.5.2 If necessary, privacy-enhanced techniques such as zero-knowledge proof protocols or user-controlled credentials shall be used in the identification and authentication process.

8.5.3 Sensitive data that might need to be deleted in the future shall not be recorded on a distributed ledger in principle.

8.5.4 If necessary, additional protection shall be in place such as a multi-signature or an off-ledger storage.

8.6 Security requirements on smart contracts

8.6.1 Smart contract code shall be validated before registration.

8.6.2 The registration of a smart contract shall be authorized.

8.6.3 The vulnerabilities and risks related to smart contracts shall be consistently managed.

8.6.4 Code review testing shall be done for smart contracts.

8.6.5 Regular functions shall be standardized into libraries.

8.7 Security requirements on key management

8.7.1 Keys shall be managed according to a pre-defined security policy. That is, keys shall be created, stored, transported, updated, archived, recovered and destroyed including backup copies securely in time.

8.7.2 Different keys shall be used for different purposes, e.g., encryption, integrity, authentication, key transport, random bit generation and generation of digital signatures.

8.8 Governing rules for security

8.8.1 Governing rules shall be established and be stated clearly on-chain or off-chain to inform users of their roles and responsibilities.

8.8.2 Users shall be informed of their responsibility to use the services securely.

8.8.3 Participants shall implement security measures to protect digital payment including cryptocurrencies and to oversee its use according to the governing rules.

8.8.4 Governing rules shall allow users and participants to monitor the DLT system's governance as appropriate. For example, changing the governing rules or the incompliance of the DLT system to the rules shall be communicated for their own interest.

9 Mapping between security threats and requirements for digital payment services

Table 2 provides a mapping between the security threats and challenges for digital payment systems based on distributed ledger technologies in clause 7.2 and the security requirements in clause 8.

Table 2 – Mapping the security threats for digital payment systems and the security requirements

Requirements		Threats						
		7.2.1	**7.2.2**	**7.2.3**	**7.2.4**	**7.2.5**	**7.3.1**	**7.3.2**
8.2	8.2.1	✓	✓					
	8.2.2	✓	✓					
	8.2.3	✓	✓					
	8.2.4	✓	✓					✓
	8.2.5	✓	✓					
8.3	8.3.1				✓		✓	
	8.3.2				✓		✓	
	8.3.3				✓		✓	✓
8.4	8.4.1	✓	✓				✓	✓
	8.4.2	✓				✓		
	8.4.3		✓	✓	✓	✓	✓	✓
	8.4.4	✓	✓	✓	✓	✓	✓	✓
8.5	8.5.1	✓	✓				✓	✓
	8.5.2	✓					✓	
	8.5.3	✓	✓				✓	✓
	8.5.4	✓	✓		✓		✓	
8.6	8.6.1		✓		✓			✓
	8.6.2		✓		✓			
	8.6.3		✓		✓			✓
	8.6.4		✓		✓			
	8.6.5		✓					✓
8.7	8.7.1	✓	✓	✓	✓		✓	✓
	8.7.2	✓	✓				✓	✓
8.8	8.8.1		✓		✓		✓	✓
	8.8.2	✓	✓	✓			✓	
	8.8.3		✓		✓	✓	✓	✓
	8.8.4		✓		✓	✓	✓	✓

Bibliography

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

[b-ITU-T FG-DFS_Financial-Inclusion] Technical Report ITU-T FG-DFS Focus Group Digital Financial Services (2017), *Distributed Ledger Technologies and Financial inclusion.* https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Report-on-DLT-and-Financial-Inclusion.pdf

[b-ITU-T DSTR-DFSECO] Technical Report ITU-T DSTR-DFSECO (2019), *Digital financial services – The digital financial services ecosystem.* https://www.itu.int/pub/T-TUT-DFS-2019

[b-ITU-T FG-DFS_SecurityReport] Technical Report ITU-T FG-DFS Focus Group Digital Financial Services (2017), *Security Aspect of Digital Financial Services(DFS).* https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf

[b-ITU FIGI] ITU FIGI Report of security workstream (2020), *Security aspects of distributed ledger technologies*. https://figi.itu.int/wp-content/uploads/2021/04/Security-Aspects-of-Distributed-Ledger-Technologies-1.pdf

[b-ISO 5127] ISO 5127:2017, *Information and documentation – Foundation and vocabulary*. https://www.iso.org/standard/59743.html

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

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. https://www.iso.org/standard/73906.html

[b-ENISA] ENISA (2017), *Distributed ledger technology & cybersecurity – Improving information security in the financial sector*. https://www.enisa.europa.eu/publications/blockchain-security

[b-SWIFT] SWIFT (2016), *Position paper – SWIFT on distributed ledger technologies.*

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, 2021