International Telecommunication Union

ITU-T X.1406

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(07/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

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

Security threats to online voting systems using distributed ledger technology

Recommendation ITU-T X.1406

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.1406

Security threats to online voting systems using distributed ledger technology

Summary

Recommendation ITU-T X.1406 identifies security threats to online voting systems using distributed ledger technology (DLT) based on telecommunication or information and communication technology (ICT) infrastructure.

Recommendation ITU-T X.1406 proposes a reference model for such online voting systems and analyses security threats in online voting processes described in the models.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1406	2021-07-14	17	11.1002/1000/14734

Keywords

Distributed ledger technology, online voting, security threat.

* 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

Introduction

Distributed ledger technology (DLT) is emerging with great potential to enable innovative financial or non-financial decentralized services (e.g., identity management, credit management, crowd funding, peer-to-peer insurance, smart contracts, supply chain management, online voting and medical records) that eliminate the need for third party intermediaries. All these services using DLT are based on telecommunication or information and communication technology (ICT) infrastructure.

An online voting system that uses DLT is a successful use case for non-financial services in many countries. The use of DLT for online voting services offers opportunities to enhance growth and development of the telecommunication or ICT market. Online voting systems using DLT can provide benefits to the telecommunication or ICT industry by making it the indispensable infrastructure for future online voting services.

Therefore, online voting systems using DLT will have a profound impact on telecommunication or ICT users and industries including telecommunication or ICT service providers.

Recently, many countries (e.g., Denmark, Estonia, Republic of Korea, Spain, Ukraine and the USA) have implemented online voting systems using DLT based on telecommunication or ICT infrastructure. However, there are potential security threats in online voting processes using DLT [b-SR_NIA_KR].

This Recommendation proposes a reference model and security considerations for online voting systems using DLT based on telecommunication or ICT infrastructure and focuses on security threats that can be categorized as: threats to data confidentiality, data integrity and service availability; unauthorized access to information systems; and malicious behaviour in online voting processes on the grounds of the model.

Recommendation ITU-T X.1406

Security threats to online voting systems using distributed ledger technology

1 Scope

This Recommendation identifies security threats to online voting systems that use distributed ledger technology (DLT) based on telecommunication or information and communication technology (ICT) infrastructure. This Recommendation focuses on online voting systems with databases (DBs) based on client or server and private distributed ledger networks (DLNs) based on telecommunication or ICT infrastructure.

This Recommendation does not consider paper-based electronic voting systems (e.g., punch card voting machines) or direct-recording electronic voting systems.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 block [ITU-T X.1400]: Individual data unit of a blockchain, composed of a collection of transactions and a block header.

NOTE – A block may be immutable and considered as the digital entity described in clause 3.2.2 of [b-ITU-T X.1255], however, it can be applied to other networks or other computational facilities.

3.1.2 consensus mechanism [ITU-T X.1400]: Rules and procedures by which consensus is reached.

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

3.1.4 node [ITU-T X.1400]: Device or process that participates in a distributed ledger network.

NOTE – Nodes can store a complete or partial replica of the distributed ledger.

3.1.5 repudiation [b-ISO/IEC 20944-1]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.1.6 smart contract [ITU-T X.1400]: A program written on a distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated, and triggered by specific conditions.

3.1.7 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

This Recommendation defines the following terms:

3.2.1 online voting: Voting using electronic means based on telecommunication or ICT infrastructure to either aid or deal with the tasks of casting and counting votes.

3.2.2 distributed ledger network (DLN): Network of distributed ledger technology nodes that make up a distributed ledger system.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APT Advanced Persistent Threat

DB Database

DDoS Distributed Denial of Service

DLN Distributed Ledger Network

DLT Distributed Ledger Technology

IT Information Technology

PC Personal Computer

PII Personally Identifiable Information

QR Quick Response

URL Uniform Resource Locator

5 Conventions

None.

6 Model and security considerations of online voting systems using DLT

As shown in Figure 1, in the reference model of an online voting system that uses DLT proposed in this Recommendation, the main components are: voting client (voter); election administrator; candidates; election observers; voting server; voter list server; and a private DLN that has nodes [ITU-T X.1400], a consensus mechanism [ITU-T X.1400], etc.

6.1 Model of online voting systems using DLT

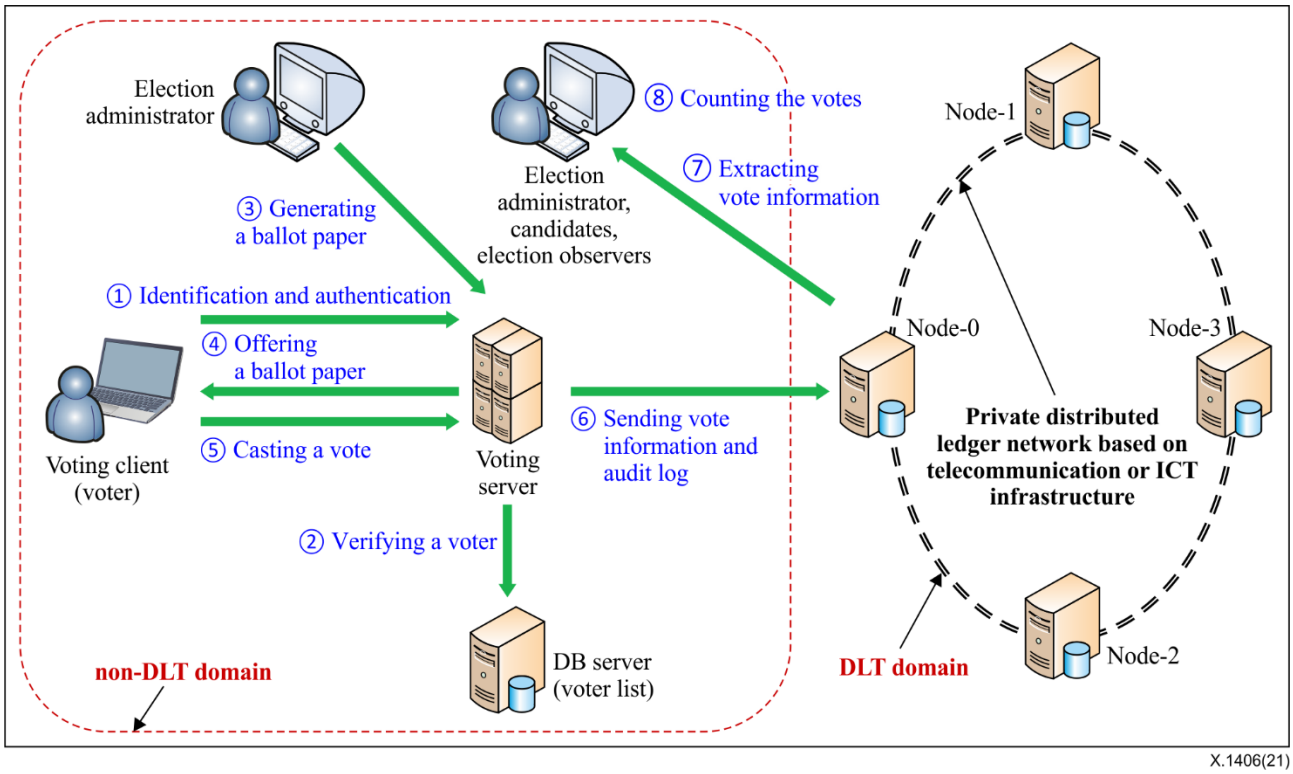

Figure 1 – Model of online voting system

As shown in Figure 1, the process of online voting in the reference model is as follows:

- step 1: the voting server identifies and authenticates a voter under the non-DLT domain;
- step 2: the voting server verifies a voter against the voters list under the non-DLT domain;
- step 3: the election administrator generates a ballot paper under the non-DLT domain;
- step 4: the voting server offers a ballot paper to a voter under the non-DLT domain;
- step 5: a voter casts a vote using a voting client under the non-DLT domain;
- step 6: the voting server requests the DLN to store vote information and an audit log, the DLN then stores vote information and the audit log by interaction between the non-DLT domain and DLT domain, see Figure 2 for more details;
- step 7: the election administrator, candidates and election observers request the DLN to extract vote information, the DLN then sends vote information to them by interaction between the non-DLT domain and DLT domain; and,
- step 8: the election administrator, candidates and election observers count votes under the non-DLT domain.

As shown in steps 7 and 8 of Figure 1, the election administrator could use a smart contract to extract vote information from a node on the DLN and to count the votes. The smart contract has the authority to retrieve vote information stored in the form of a distributed ledger from the node.

As shown in Figure 1, online voting systems using DLT consist of both a DLT domain and a non-DLT domain. The non-DLT domain includes a voting client (voter), DB server (voters list), voting server and election administrator. In the DLT domain, participants with nodes in the DLN should include at least an election administrator, candidates and election observers.

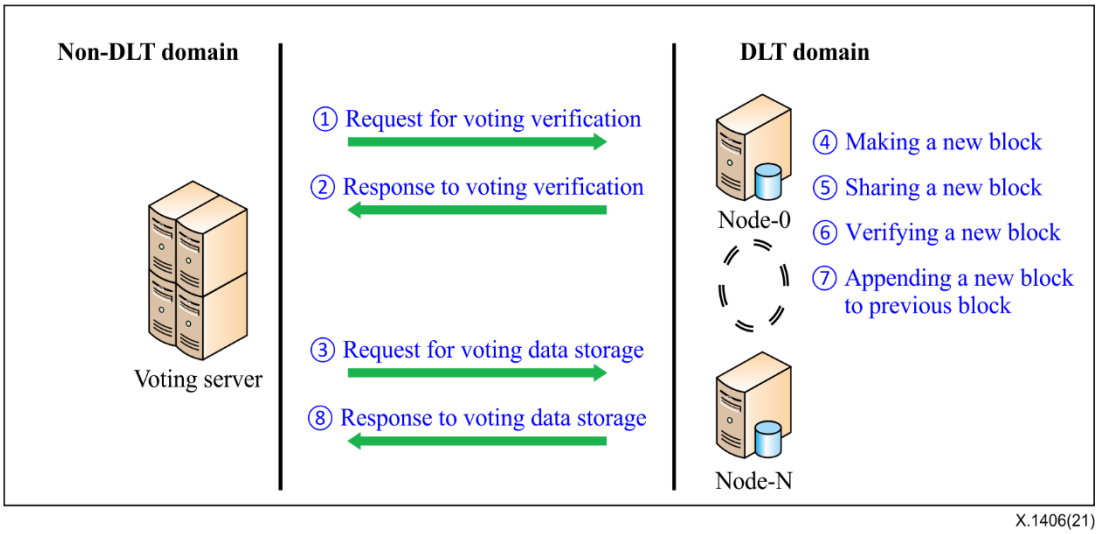

Figure 2 – Consensus process under online voting system

As shown in Figure 2, the consensus process under the online voting system in Figure 1 is as follows:

- step 1: the voting server requests voting verification from a node on the DLN with vote information and an audit log as voting data;
- step 2: the node on the DLN responds to the voting verification request;
- step 3: the voting server requests voting data storage from the node on the DLN;
- step 4: the node on the DLN makes a new block [ITU-T X.1400] storing the vote information and the audit log;
- step 5: the node on the DLN shares the new block with the other nodes on the DLN;
- step 6: each node on the DLN verifies the new block;
- step 7: each node on the DLN appends the new block to the previous block; and,
- step 8: the node on the DLN responds to the voting data storage request.

The vote information should include the candidate selection. The audit log should include at least:

- a timestamp to authenticate the voter;
- the authentication result (success or failure);
- a timestamp to verify the voter;
- the verification result (success or failure);
- a timestamp to generate a ballot paper;
- the generation result (success or failure);
- a timestamp to cast a vote; and,
- the result of casting a vote (success or failure).

As shown in Figure 3, the process for vote counting of an online voting system in Figure 1 is as follows:

- step 1: the election administrator, candidates and election observers request extraction of vote information from nodes on the DLN;
- step 2: each node on the DLN retrieves vote information;
- step 3: each node on the DLN responds with vote information to the election administrator, candidates and election observers;
- step 4: the election administrator, candidates and election observers count the votes; and,

- step 5: the election administrator, candidates and election observers mutually verify vote count results.

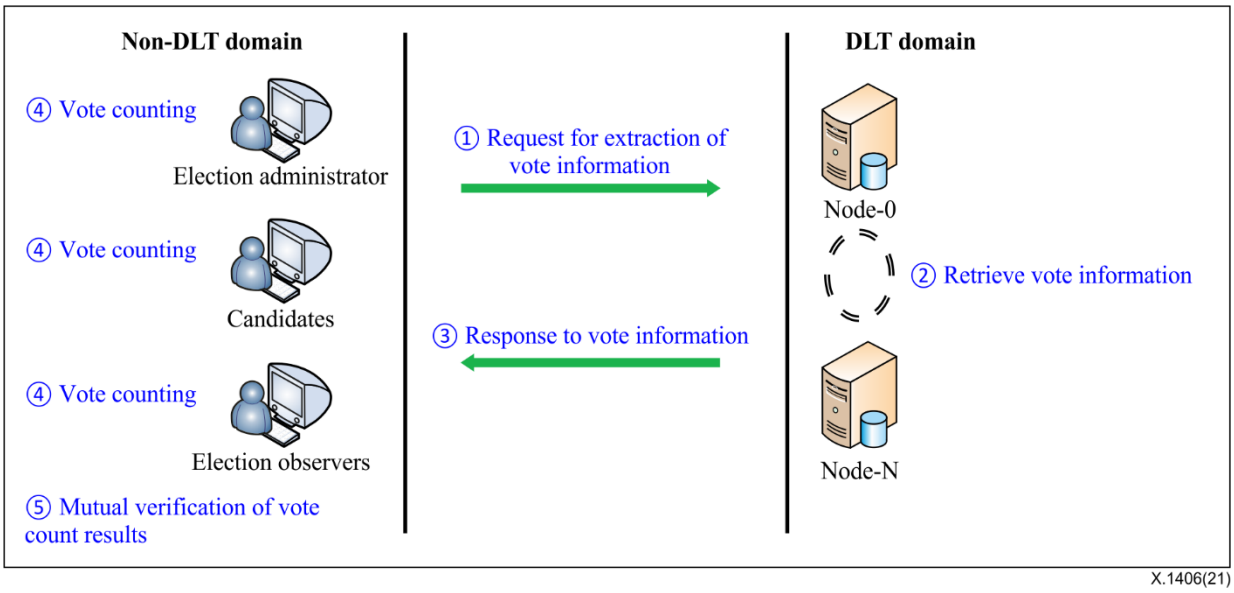

Figure 3 – 'Counting vote process' of online voting system

There are two types of key data in an online voting system: personally identifiable information (PII); and voting data. The PII is used to verify whether a voter is valid before voting. Voting data includes vote information and audit logs. Online voting systems using DLT should protect both PII and voting data as significant information assets.

As shown in Figure 4, when identifying and authenticating a voter and verifying whether a voter is valid before voting, the PII flow in the online voting system in Figure 1 is as follows:

- step 1: a voter sends PII to the voting server to verify identity;
- step 2: the voting server responds to the voter with the identification and authentication result, the voting server does not store the PII of the voter;
- step 3: the voting server sends the PII of the voter to the DB server, which maintains a list of valid voters;
- step 4: the DB server verifies the voter by comparison with the list of valid voters and then discards the PII of the voter; and,
- step 5: the DB server responds with the verification result to the voting server.

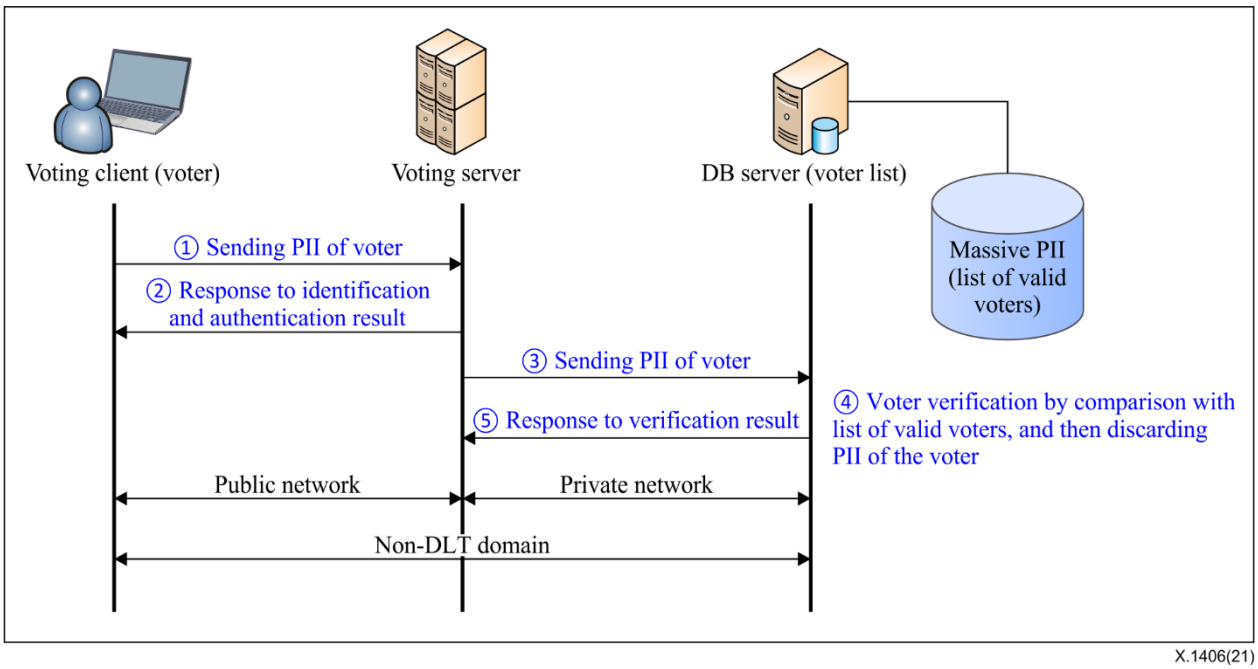

Figure 4 – PII flow in online voting system

As shown in Figure 5, when casting a vote, the voting data flow in the online voting system in Figure 1 is as follows:

- step 1: a voter sends vote information to the voting server;
- step 2: the voting server sends the vote information and audit log to a node on the DLN;
- step 3: all nodes on the DLN store the vote information and audit log as voting data; and,
- step 4: the node responds with the result from stored voting data to the voting server, which then responds with it to the voter.

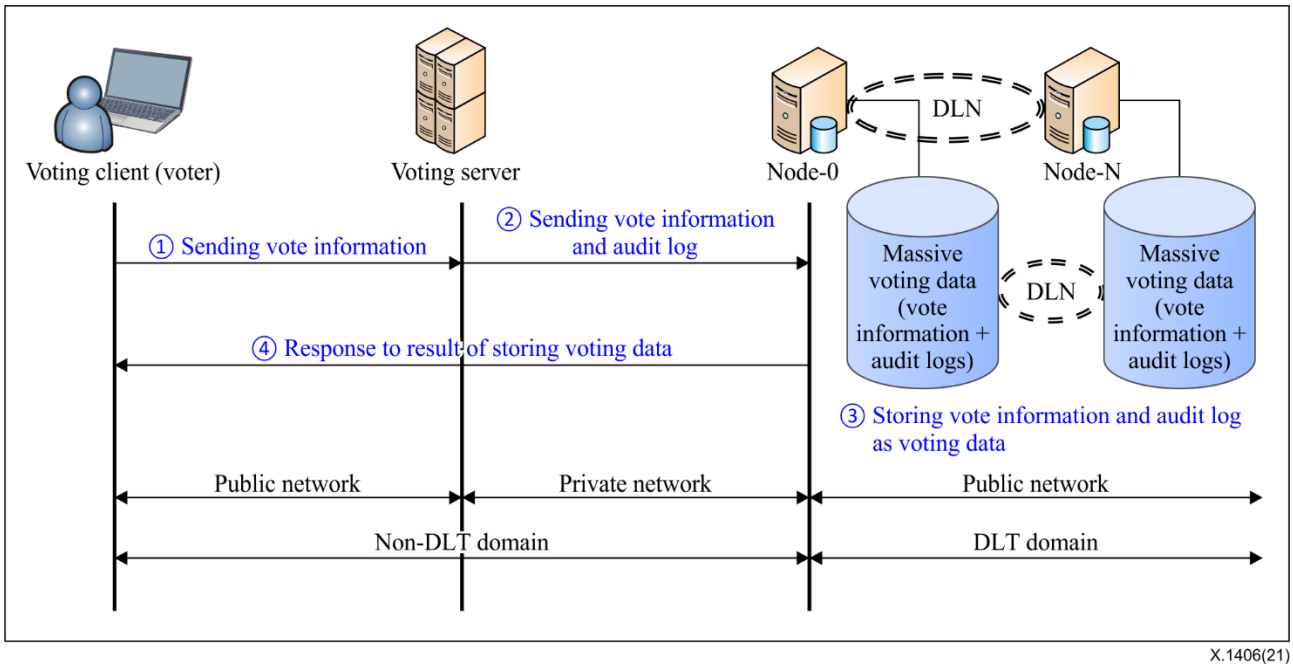

Figure 5 – Voting data flow when casting a vote

As shown in Figure 6, when counting the votes, the voting data flow under the online voting system in Figure 1 is as follows:

- step 1: the election administrator, candidates and election observers request vote information as voting data from each node on the DLN;
- step 2: each node on the DLN retrieves the vote information;
- step 3: each node on the DLN sends the vote information as voting data to the election administrator, candidates and election observers; and,
- step 4: the election administrator, candidates and election observers count the votes and then mutually verify the results of counting the votes, and discard the vote information.

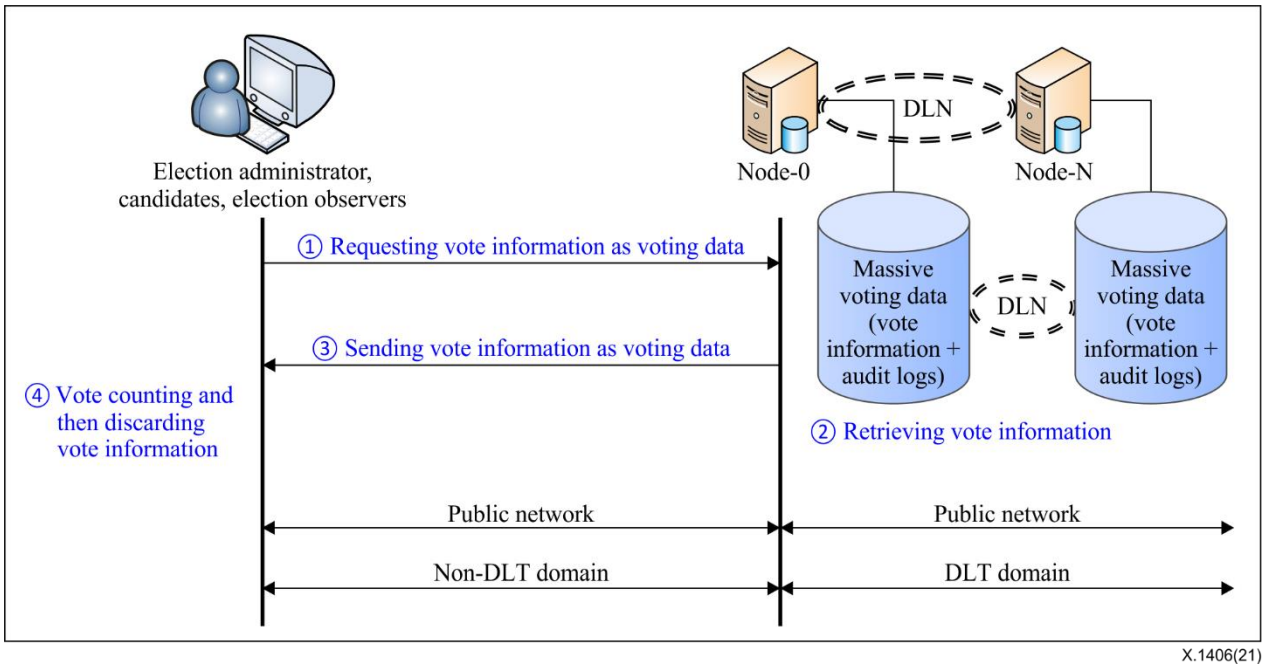

Figure 6 – Voting data flow when counting votes

6.2 Security considerations of online voting systems using DLT

Security considerations of an online voting service based on DLT should be identified. Security considerations of data confidentiality; verifiability; robustness; receipt-free status; correctness; integrity; uniqueness; voter authentication; coercion resistance; and zero trust are helpful to the development of countermeasures against identified security threats.

6.2.1 Data confidentiality

To protect information from access by unauthorized parties, an online voting system must build in safeguards for data input, storage, access and use.

6.2.2 Verifiability

In an online voting system, the ballot result should be verified after voting by voters. The online voting system should provide two kinds of verifiability: individual verifiability, which involves voters verifying their own vote after voting; and universal verifiability, which entails verification of whether the final voting tally has been computed correctly.

6.2.3 Robustness

Robustness is the ability of an online voting system to cope with errors during execution and erroneous input. An online voting system with robustness should guarantee that the final tally should be correctly computed even in the presence of faulty behaviour from a number of parties.

6.2.4 Receipt-free status

Receipt-free status of an online voting system ensures not only that voters can keep their vote private, but also that individuals must keep it private. This means that voters do not have the ability to prove to any third party that they have cast a particular vote. Voters should neither obtain nor be able to construct a receipt proving the content of their vote. In a receipt-free voting scheme, voters cannot prove their vote to anyone; this makes vote-buying impractical.

6.2.5 Correctness

Correctness of an online voting system means that it records and counts all votes and shall do it correctly.

6.2.6 Integrity

Integrity of an online voting system prevents any attacker tampering with data during the whole voting process (i.e., votes should not be modified, forged or deleted without detection).

6.2.7 Uniqueness

Uniqueness of an online voting system ensures that only one vote per user is counted.

6.2.8 Voter authentication

Voter authentication of an online voting system ensures that voters must identify themselves to be entitled to vote and no one can imitate other voters to vote.

6.2.9 Coercion resistance

Coercion resistance of an online voting system means that it is infeasible for anyone to determine whether a voter complies with coercion demands. A coercion resistant online voting system offers not only receipt-free status, but also defence against randomization, forced abstention and simulation attacks – all potentially in the face of corruption of a minority of tallying authorities.

6.2.10 Zero trust status

Zero trust status of an online voting system means that a voter does not need to trust anyone, including other voters and voting authorities, to ensure data confidentiality, integrity and correctness of the voting process.

7 Security threats in the online voting process

Potential security threats that could occur during the online voting service using DLT should be identified. Security threats are categorized as: threats to data confidentiality, data integrity or service availability; unauthorized access to information system; and malicious behaviour.

7.1 Threats to data confidentiality

Threats to data confidentiality due to security incidents (e.g., advanced persistent threat (APT) attacks) and information technology (IT) disasters (e.g., human error), which target key information systems that make up online voting systems using DLT, should be identified.

7.1.1 Disclosure of PII of a voter during transmission

- As a voting server identifies and authenticates a voter, the PII of the voter could be disclosed during transmission between a voting client (e.g., personal computer (PC) or smart phone) and the voting server.
- As a voting server verifies whether a voter is valid, the PII of the voter could be disclosed during transmission between the voting server and the DB server with the list of valid voters.

7.1.2 Disclosure of vote information and audit log during transmission

- As a voter casts a vote, vote information could be disclosed during transmission between a voting client (e.g., PC or smart phone) and voting server.
- As a voting server stores vote information and its audit log as voting data in a distributed ledger, the voting data could be disclosed during transmission between the voting server and a node on a DLN.
- As one node shares vote information and audit log as voting data with other nodes on a DLN, the voting data could be disclosed during transmission among nodes on the DLN.

7.1.3 Disclosure of voters list from database

A massive list of valid voters could be disclosed from a DB server running a vulnerable operating system or DB application.

7.1.4 Disclosure of vote information and audit logs from a database on a DLN

Massive vote information and audit logs as voting data could be disclosed from a node running a vulnerable operating system or DB application on a DLN.

7.2 Threats to data integrity

Threats to data integrity due to security incidents (e.g., APT attacks) and IT disasters (e.g., human error), which target key information systems that make up online voting systems using DLT should be identified.

7.2.1 Tampering with a ballot paper during transmission

- Ballot papers generated by an election administrator could be tampered with during transmission between an election administrator client (e.g., PC) and a voting server.
- As a voter tries to cast a vote, a ballot paper could be tampered with during transmission between a voting client (e.g., PC or smart phone) and a voting server.

7.2.2 Tampering with vote information and audit log during transmission

- As a voter casts a vote, vote information could be tampered with during transmission between a voting client (e.g., PC or smart phone) and a voting server.
- As a voting server tries to store vote information and its audit log as voting data in a distributed ledger, voting data could be tampered with during transmission between the voting server and a node on the DLN.
- As one node shares vote information and its audit log as voting data with other nodes on a DLN, the voting data could be tampered with during transmission among nodes on DLN.

7.2.3 Tampering with vote information and its audit log in a database on a DLN

Massive vote information and audit logs as voting data could be removed from a node running a vulnerable operating system or DB application on a DLN.

7.2.4 Tampering with a database voters list

A massive list of valid voters could be tampered with by a DB server running a vulnerable operating system or DB application.

7.3 Threats to service availability

Threats to service availability due to security incidents (e.g., APT attacks) and IT disasters (e.g., human errors), which target key information systems that make up online voting systems using DLT, should be identified.

7.3.1 Reduced service continuity of a DLN

The availability of a DLN that processes (replicates, shares, synchronizes, etc.) massive vote information and audit logs as voting data with a consensus mechanism could be reduced by a distributed denial of service (DDoS) attack on the network infrastructure.

7.3.2 Reduced service continuity of nodes on DLN

The availability of nodes on a DLN that maintain massive vote information and audit logs as voting data could be reduced by a DDoS attack on the operating system or DB application.

7.3.3 Reduced service continuity of voting

- The availability of a voting server that identifies, authenticates and verifies a voter could be reduced by a DDoS attack on the operating system or application.
- The availability of a DB server that maintains a massive list of valid voters could be reduced by a DDoS attack on the operating system or DB application.

7.4 Unauthorized access to an information system

Unauthorized access due to security incidents (e.g., APT attacks) and IT disasters (e.g., human error), which target key information systems that make up online voting systems using DLT, should be identified.

7.4.1 Unauthorized access to a voters list in a database

Unauthorized access could occur to a voter list server or DB that stores and retrieves massive personal data of voters.

7.4.2 Unauthorized access to a voting server

Unauthorized access could occur to a voting server that provides voting services to voters, an election administrator, voter list server and DLN revealing voter identification and verification, voting rights verification, electronic ballot creation and transmission, audit log creation and transmission, etc.

7.4.3 Unauthorized access to nodes on a DLN

- Unauthorized access could occur to the DLN infrastructure (e.g., network devices and lines) that transmits to replicate, share and synchronize massive critical data (e.g., vote information and audit logs) consensually among nodes.
- Unauthorized access could occur to nodes that are key components of the DLN, which stores and maintains massive critical data (e.g., vote information and audit logs).

7.5 Malicious behaviour

Voters, election administrators, election-related stakeholders (e.g., supporters of candidates, etc.), software developers, and so on, who could behave maliciously should be identified.

7.5.1 Repudiation of ballot generation by an election administrator

An election administrator could repudiate without authority the generation of electronic ballots provided to voters using voting clients (e.g., PCs or smart phones) through a voting server.

7.5.2 Multiple voting by a voter

A voter could exercise multiple voting using voting clients (e.g., PC or smart phone) through a voting server.

7.5.3 Repudiation of voting by a voter

A voter could repudiate without authority the voting (e.g., selection of a candidate) on an electronic ballot using a voting client (e.g., PC or smart phone).

7.5.4 Casting a vote under coercion

A voter could be coerced to make an unwanted voting choice (e.g., selection of a candidate).

7.5.5 Infection with malware

- Malware could be inserted during the development and distribution of software related to online voting systems using DLT (e.g., voting software for voter, critical information transfer modules and software for counting the votes).
- Voting clients (e.g., PCs or smart phones) used by voters and election management clients (e.g., PCs) used by election administrators could be infected with malware.

7.5.6 Fraudulent voting

There could be fraudulent voting with a stolen identity.

7.5.7 Bribery attack

Attackers could affect the result of the vote by bribing the voter. Bribery is hard to prevent in real world voting. However, cryptography can be used to make online voting system receipt-free, thus, preventing bribery attacks.

7.5.8 Randomization attack

In a randomization attack, an attacker coerces voters by requiring that they submit randomly composed balloting material. In this attack, the attacker is unable to know which candidate voters vote for. As a result, the attacker nullifies the voter choice with a large probability.

7.5.9 Forced-abstention attack

A forced-abstention attack is related to that in clause 7.5.8. In this case, the attacker coerces voters by demanding that they refrain from voting. If attackers can see who has voted, they can use this information to threaten and effectively bar voters from participation.

7.5.10 Collusion attack

A collusion attack involves multiple parties (including voters and some voting authorities) cooperating to break the security of the online voting system.

Appendix I

Use cases of online voting systems using distributed ledger technology

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

This appendix references three use cases of a DLT-based online voting system:

The government of the Republic of Korea conducted a proof-of-concept to demonstrate the prevention of voter fraud in vote casting and counting, and the ability for direct voter verification of their vote; The Istanbul Technical University proposed a proof-of-concept and successfully demonstrated that disadvantages of conventional physical elections such as waiting times can be greatly reduced; and Plymouth University (United Kingdom) proposed a proof-of-concept to demonstrate voter anonymity based on a multi-tiered architecture operating two distinct blockchains.

I.1 Use case in the Republic of Korea

In 2018, the government of the Republic of Korea (National Election Commission) implemented a DLT-based online voting service demonstration project that uses DLT to prevent tampering with voting and counting results, and to enable stakeholders to directly verify the result. [b-PR_NEC_KR]

As shown in Figure I.1, voters whose identities have been verified can vote through the online voting system provided by the National Election Commission and verify the results of voting after the vote. Participants with nodes in the DLN consist of the National Election Commission, candidates and election observers.

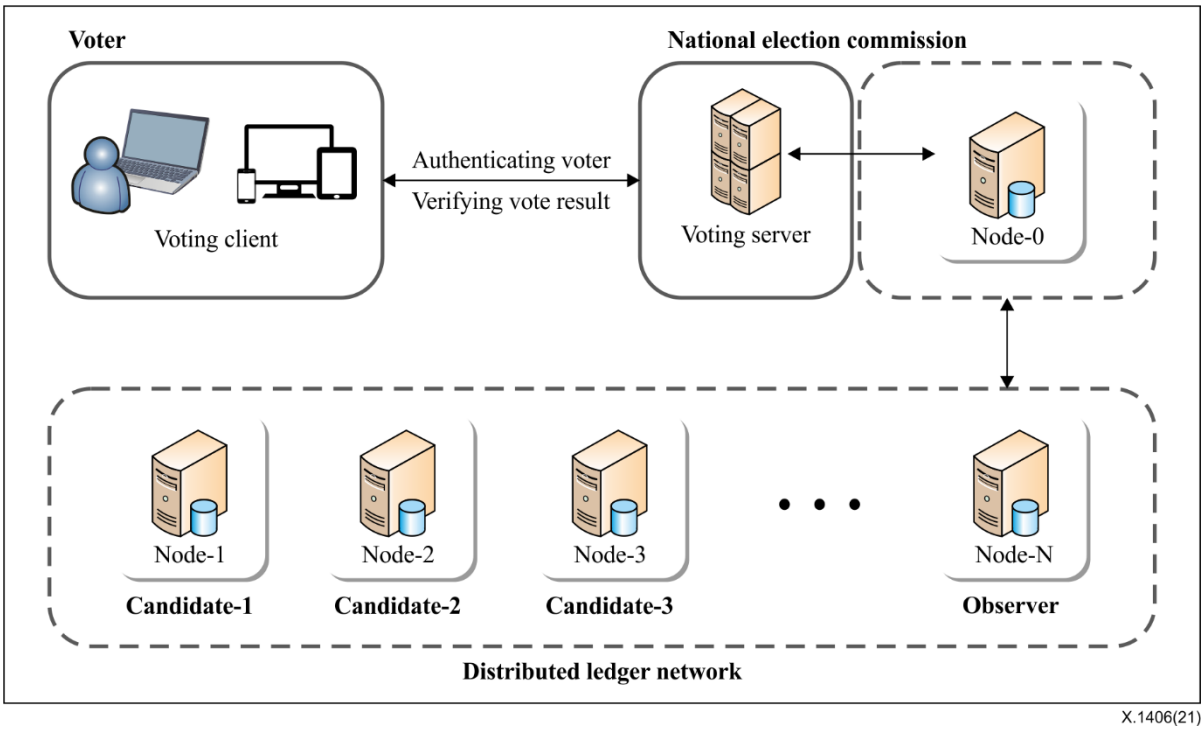

Figure I.1 – Online voting service in the Republic of Korea

As the voting data is distributed by and stored on DLT, online voting is enhanced in transparency and security because tampering with the voting result is actually impossible even if a cyberattack occurs.

As shown in Figure I.2, the main components of the online voting system in Republic of Korea are the voting client (voter), election administrator, vote-counting server, voting server, voter list server and DLT systems, which have nodes, a consensus protocol, etc. The DLT system stores encrypted

vote information and audit logs as voting data. As voting data is anonymized, the DLT system stores vote information and audit logs that cannot be used to identify voters.

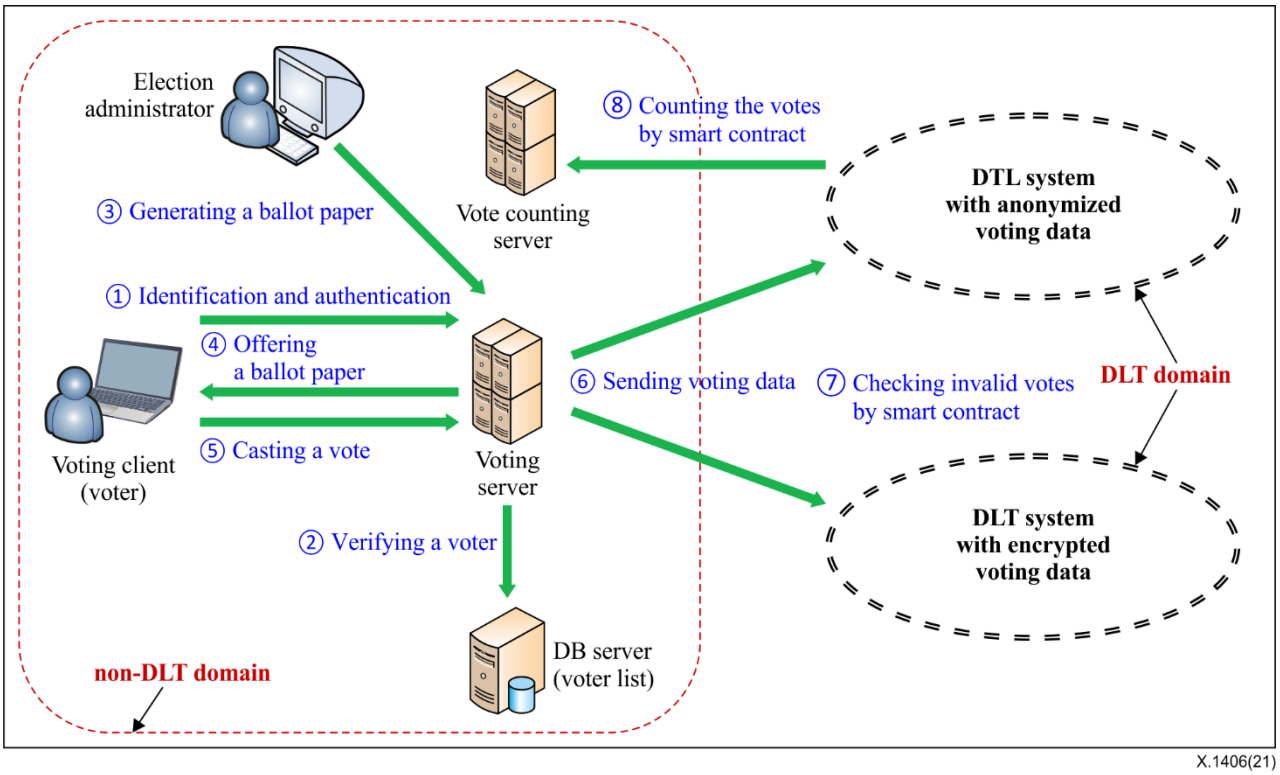

Figure I.2 – Diagram of online voting system in the Republic of Korea

Figure I.2 is a schematic diagram of the online voting system as follows:

- step 1: the voting server identifies and authenticates a voter under the non-DLT domain;
- step 2: the voting server verifies a voter against the voters list under the non-DLT domain;
- step 3: the election administrator generates a ballot paper under the non-DLT domain;
- step 4: the voting server offers a ballot paper to a voter under the non-DLT domain;
- step 5: a voter casts a vote using a voting client under the non-DLT domain;
- step 6: the voting server requests the DLT systems to store vote information and audit log by interaction between the non-DLT domain and DLT domain;
- step 7: the DLT systems check invalid votes by smart contract and then store vote information and audit log by interaction between the non-DLT domain and DLT domain; and,
- step 8: the DLT system with anonymized voting data counts the votes by smart contract and then sends the result to the vote-counting server.

There are several advantages to the online voting system using DLT in the Republic of Korea, namely to ensure:

- integrity of voting data using the DLT systems in which stakeholders (e.g., election administrator, candidates and election observers) participate as nodes;
- accuracy of voting results and the validity of votes using a smart contract;
- anonymous voting for privacy using a DLT system with anonymized voting data; and,
- re-voting using the digital signature of a voter if necessary.

I.2 Use case in Turkey [b-PR_TR]

Istanbul Technical University in Istanbul, Turkey proposed an online voting system using DLT to eliminate disadvantages of conventional elections. Security and data integrity of votes are provided and waiting time for vote counting decreased significantly.

As shown in Figure I.3, this use case of an online voting system is about the citizen and government. Government in this system only authorizes citizens who can vote or prevents citizens who have already voted in that election from voting again. Also, government and citizens determine the candidates that will be participating in that election. The ballot box information, candidates and citizen ballot box relation are provided by the government, which is the trusted party in elections. The vote of a citizen is added to the DLT system, so that any vote has a guarantee from the system of being immutable. Since the DLT system contains all citizen votes anonymously at the end of the election, the official results are announced within minutes after the election terminates. Any concerned third party can get vote counts to be sure that voting can really be trusted.

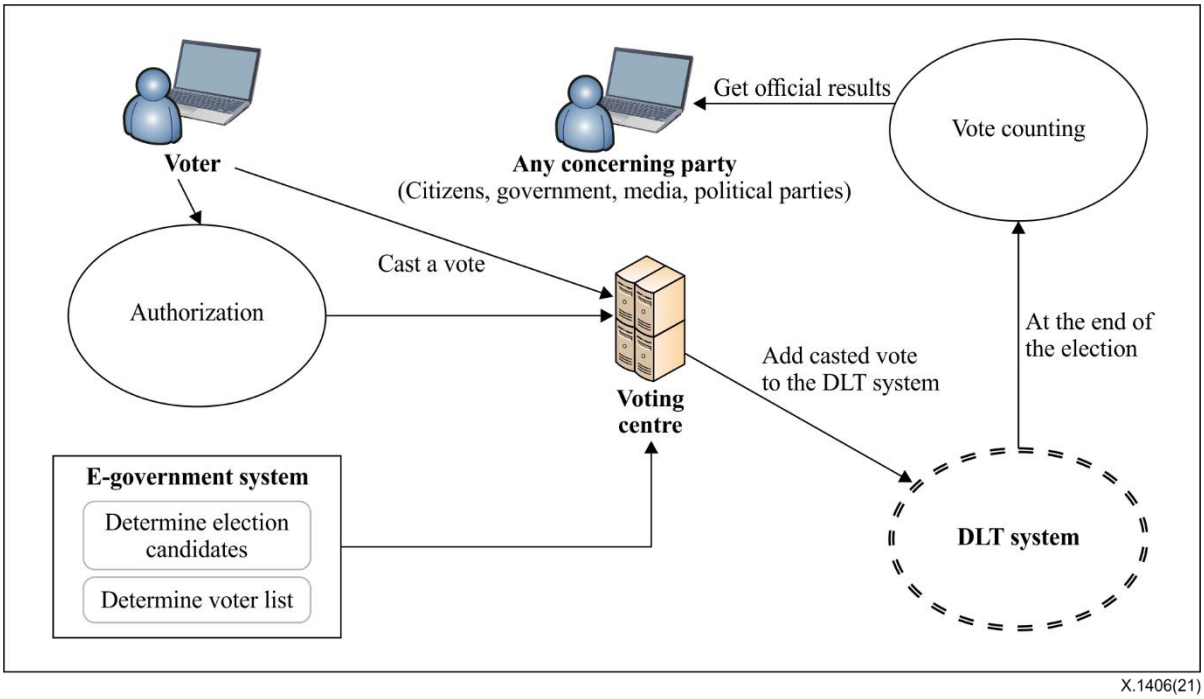

Figure I.3 – Online voting system in Turkey

As shown in Figure I.4, the structure of the system has levels. The number of levels in the system differs according to the necessities of the country. In order to provide a fast, consistent and secure system, the system is designed with an architecture containing levels. The level number (e.g., level 0, level 1, etc.) will change from country to country according to the features of that country. The rationale for using an architecture containing levels is explained later in detail. Furthermore, the consensus of the system is satisfied using delegated proof of stake (DPoS) algorithms.

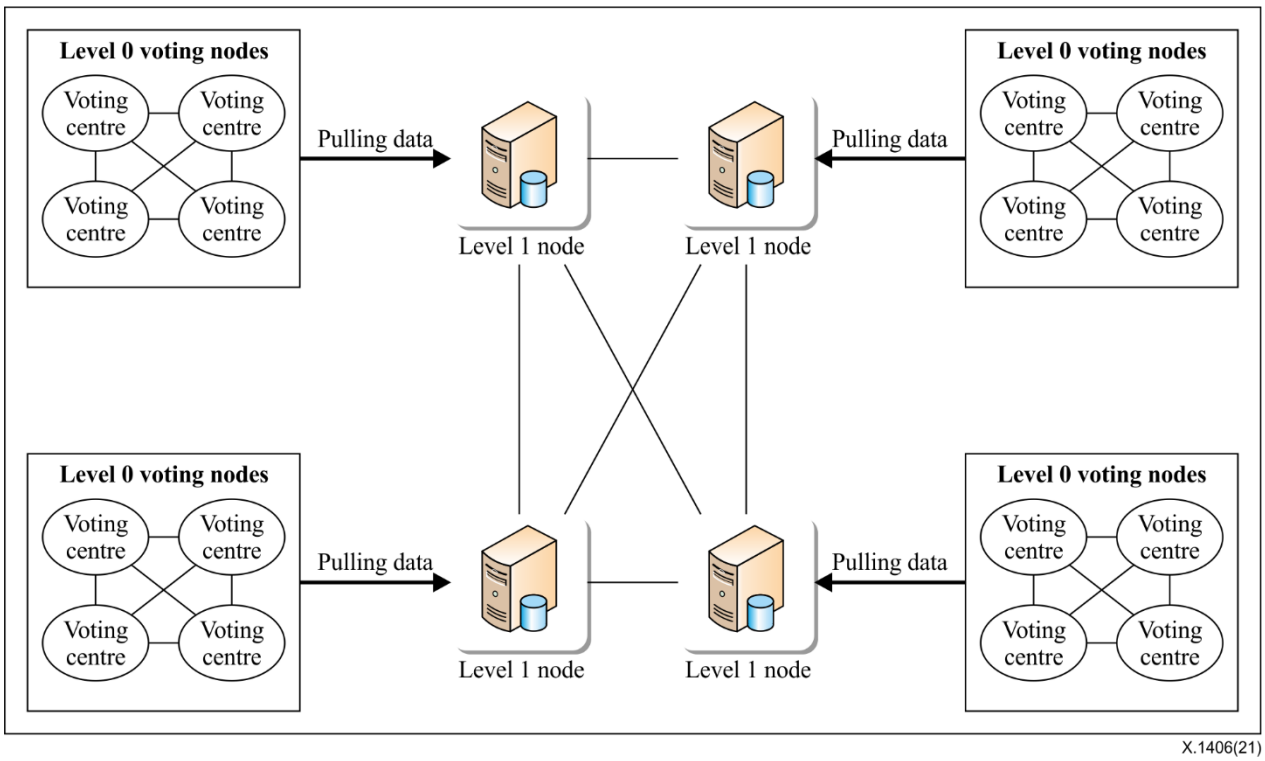

Figure I.4 – Architecture of online voting system in Turkey

If the whole country is represented by a single DLT system, synchronization of the system would have performance issues due to the vast number of ballots and the distance between voting centres. Distance in connected systems is always cause of latency. For a system that includes the whole country under the same DLT system, latency between two voting centres would be a big problem, because for Turkey, expected latency would be at least 100 ms. This is a huge value for a system that consists of 10 000 centres, at which there would be simultaneous voting. In this case, synchronization of the system would take lots of time. So, in order to decrease latency, the DLT systems are distributed over levels. There will be different DLT systems at each level, from lowest to highest, and connections between levels will be provided by a secure system.

At the lowest level, there will be a DLT system that consists of nodes (servers in voting centres) where citizens will vote in an election. Due to the relatively small number of nodes in the system, synchronization will take an affordable amount of time at the lowest level. When the number of nodes is arranged in a good pattern (i.e., DLT system overload will not cause enormous latency), the system will perform well. A citizen will go to the voting centre and enter the system with the identity that is provided by the government. The construction of a system that works on the government system that will hold citizen data for a specified election is under consideration. If a citizen has not yet voted, they will be able to cast their ballot for one of the candidates. Candidate details will be held in a DB stored in a government-related system. When the authentication process is satisfied, a citizen will vote by choosing one proposed candidate or a blank vote for those who do not want to vote for any of the candidates. In this system, proposed candidates will be taken from a DB that includes relations between ballot boxes and candidates. Thus, there will be only appropriate candidates. Most authentication systems used across government-related systems are managed by an e-government system. When a user passes the authentication phase, it will be apparent whether a vote has previously been cast. If a citizen has not yet voted, the citizen will choose a desired candidate according to the steps explained in the foregoing.

At the second lowest level, there will be a cluster of DLT systems that stores data that are coming from the level below. In this level, DLT facilities make the system consistent. For Turkey, it is considered that two levels will be enough. The system at the second level can have about 700 nodes,

considering the population of the country. That greatly improves performance of the system because the number of connected nodes in this structure decreases considerably. Additionally, if the number of the nodes at the second or upper levels is increased, performance increases exponentially. For a country that has more citizens, the number of levels can be increased in order to decrease collisions between transactions. Consequently, system can be considered as scalable.

Communication between levels is ensured using communication protocols. Periodic communication is needed. So, there will be a time delay between level synchronization. Because, if each vote was considered instantly, there would be a huge bottleneck. This synchronization will provide consistency through the system. For Turkey, this synchronization time should be 5 min i.e., at the end of each 5 min period, each node cluster will send DLT system data to the upper level node. At this level, data will be synchronized between nodes using a different synchronization algorithm. A two-levelled example is shown in Figure I.4. There are voting centres that use the same DLT system in their selected area. Also, voting centres can deploy numerous voting servers. Moreover, all level 1 nodes use the same DLT system.

The vote centres are DLT system nodes. There will be a file at each node (voting centre) that stores the number of data that indicates the number of votes accepted from the upper level at the previous synchronization step. At every specified time interval, voting will be stopped for a very short time period (it is expected to be 1 min for Turkey) in order to synchronize DLT system data between levels. When the data arrives at an upper level from lower DLT system nodes, it will be checked in order to satisfy consistency.

If data consistency is ensured, a flag indicates the data is accepted. At this point, nodes at level 0 await an answer from level 1 (and level 1 from level 2, so on). If a flag indicates the votes are accepted, the files at each node (voting centres) will be updated. So, nodes at the lower level of two will always know how many votes have been accepted at the upper level. Additionally, data will be added to the DLT system at the level at which data has arrived (if the communication is between level 0 level 1, the indicated level is level 1). This data will be considered as a transaction block, i.e., all new votes (votes coming after previously added votes) are considered as a vote cluster and as an array in computer scientific terms. This vote cluster will be a block that will be added to the DLT system.

In the synchronization phase, if the data coming to the upper level from different servers are inconsistent, that is a case that should be considered with care. If consensus cannot be satisfied, the data will not be accepted by the higher of the two levels and a "decline" flag will be sent to the lower one. In this case, the same data should be resent to the upper level. Until consistency is satisfied, this procedure will continue, to satisfy consistency at each level.

All nodes at the lower levels know that the data is accepted if the answer so states; in which case, they can continue working. However, in order to satisfy consistency through the system, delays between synchronizations should be arranged very carefully. If the delay between levels is a short amount of time, the time spent for synchronization may increase greatly. In contrast, if the delay is a long amount of time, the data to be sent between levels acquires an enormous size and data transfer is a problem. So, in order not to create a bottleneck in the system, this delay between levels should be chosen carefully. With well-designed synchronization times between levels, a high performance providing a consistent system is obtained.

I.3 Use case in the United Kingdom [b-PR_UK]

Plymouth University, United Kingdom, has proposed an architecture to solve the issues of digital voting by using blockchain technology. The voting mechanism and architecture, and voting process are as follows.

Figure I.5 shows the network is a multi-tiered, decentralized infrastructure that houses two distinct blockchains; the network is divided into three abstract tiers: national; constituency; and local.

The local tier contains all digital polling stations across the country, each of which is associated with a constituency node. A local node is set up only to communicate with other local nodes under the associated constituency node and the constituency node itself. The constituency tier contains all nodes deemed to be at a constituency level. These nodes would be directly connected to each other and to a subset of polling stations depending on location. The national tier is a collection of nodes that are not tied to location, their sole purpose is to mine transactions and add blocks to the vote blockchain. All constituency nodes communicate to a national node and national nodes can communicate with each other.

Independent bodies will monitor and audit the voting process. These bodies will host or have access to a national node and will be able to verify that the unencrypted results match the encrypted votes. Individuals and organizations can volunteer to be a national node. These applications are processed by the government to ensure that they meet the minimum requirements set by a governing body.

As part of the design, there is an encryption method based on public and private keys and a structure is implemented in which the data is segregated within the blockchain. This segregation has been achieved by getting the constituency level nodes to generate key pairs. The public keys are then distributed to the connected polling station nodes, which then use the public key to encrypt any vote made at that polling station. The data is then stored in an encrypted format within the blockchain and propagates out to the entire network.

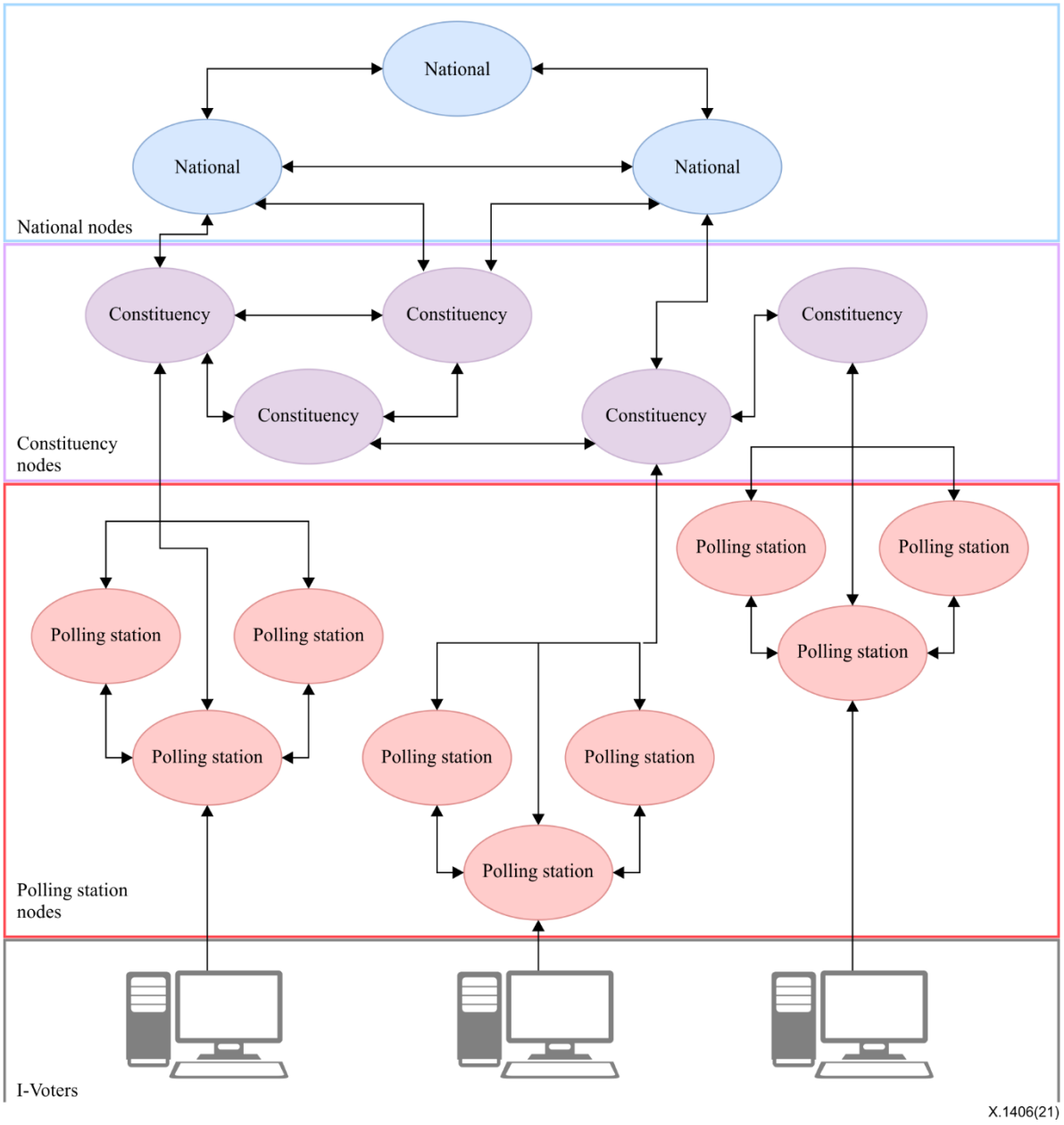

Figure I.5 – Overview of node architecture [b-PR_UK]

Due to the fact that each constituency will have a different public key means that chunks of data within the blockchain will be encrypted differently to a chunk of data next to it. The method has been applied to prevent any one person being able to decrypt the voting data before the voting deadline expires. If a hacker manages to get hold of a constituency private key, they would only be able to decrypt certain sections of the blockchain, so would never know the full outcome of the vote. Once the voting deadline has passed, the software within the constituency nodes publishes the private keys to allow the blockchain network to decrypt the data, which in turn means the votes can then be counted.

When it is time to vote, authentication of a user requires three distinct pieces of evidence: their identification number (e.g., United Kingdom citizens have national insurance numbers); the password supplied on registration; and their ballot card, which contains a QR code. As there are two methods of voting (web browser, physical polling station), the way the user will input the authentication details shall differ; however, in order to vote, they are required to provide all three pieces of information. It is also important to note that each user will have been registered in a certain constituency, so they will only be able to vote at a local polling station within that constituency or via the Internet at the

uniform resource locator (URL) provided on the ballot card. (Each constituency is to be equipped with its own web server and URL to ensure votes are aggregated within the right network.)

As shown in Figure I.6, behind the scenes, the polling station will consult the voter blockchain to ensure the voter has not already used their vote. If the user does the right to vote, then the station will allow the user to continue to the voting screen. If not, the system will respond to the user appropriately.

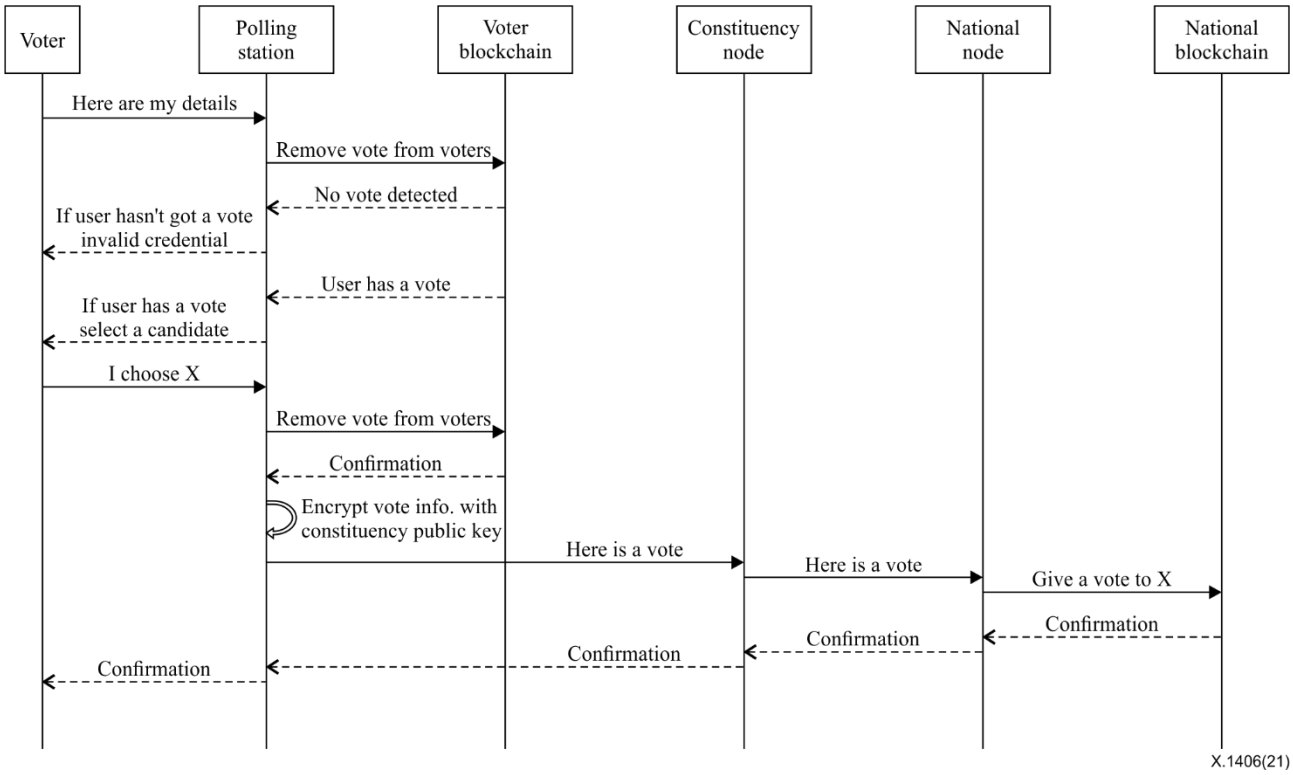

Figure I.6 – Diagram of voting architecture [b-PR_UK]

After selecting their vote (from the selection of options including abstention) and then confirming the submission, the vote will become a transaction, it will be encrypted with the public key of the relevant constituency. This transaction is then passed to the constituency node, where it is added to a block and the update is then pushed to all other nodes connected to that particular constituency node. The connected nodes then pass the data on to their peers until the whole network is updated. Once the vote has been confirmed, the polling station will then generate a transaction to remove the vote of the user within the voter blockchain. It is important to note that there are two distinct blockchains being held: one which contains transactions relating to which users have registered and which users still have a vote; the second containing the contents of the vote (such as what party was voted for). Through the use of these two distinct blockchains, voter anonymity when selecting their vote can be ensured.

Bibliography

[b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

[b-ISO/IEC 20944-1] ISO/IEC 20944-1:2013, *Information technology – Metadata registries interoperability and bindings (MDR-IB) – Part 1: Framework, common vocabulary, and common provisions for conformance*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-PR_NEC_KR] Republic of Korea (Internet). *National Election Commission*. Seoul: National Election Commission. Available [viewed 2021-09-24] at: http://www.nec.go.kr/portal/bbs/view/B0000342/39054.do?searchYear=2018&menuNo=200602

[b-PR_TR] Bulut, R., Kantarcı, A., Keskin, S., Bahtiyar, S. (2019). *Blockchain-based electronic voting system for elections in Turkey*. New York, NY: arXiv (Cornell University), 6 pp. Available [viewed 2021-09-24] at: https://arxiv.org/ftp/arxiv/papers/1911/1911.09903.pdf

[b-PR_UK] Barnes, A., Brake, C., Perry, T. (undated). *Digital voting with the use of blockchain technology*. Plymouth: Plymouth University. 19 pp. Available [viewed 2021-09-25] at: https://www.economist.com/sites/default/files/plymouth.pdf

[b-SR_NIA_KR] National Information Society Agency (2017). 블록체인 활용 전자투표 주요사례 및 시사점 [Special report on key cases and implications of electronic voting using blockchain]. Seoul: Government of the Republic of Korea. Available [viewed 2021-09-23] from: https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=82618&bcIdx=18560&parentSeq=18560

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