International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.747.10

(01/2022)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Multimedia services

Requirements of distributed ledger systems for secure human factor services

Recommendation ITU-T F.747.10

ITU-T F-SERIES RECOMMENDATIONS

NON-TELEPHONE TELECOMMUNICATION SERVICES

TELEGRAPH SERVICE	
Operating methods for the international public telegram service	F.1–F.19
The gentex network	F.20–F.29
Message switching	F.30–F.39
The international telemessage service	F.40–F.58
The international telex service	F.59–F.89
Statistics and publications on international telegraph services	F.90–F.99
Scheduled and leased communication services	F.100–F.104
Phototelegraph service	F.105–F.109
MOBILE SERVICE	
Mobile services and multidestination satellite services	F.110–F.159
TELEMATIC SERVICES	
Public facsimile service	F.160–F.199
Teletex service	F.200–F.299
Videotex service	F.300–F.349
General provisions for telematic services	F.350–F.399
MESSAGE HANDLING SERVICES	F.400–F.499
DIRECTORY SERVICES	F.500–F.549
DOCUMENT COMMUNICATION	
Document communication	F.550–F.579
Programming communication interfaces	F.580–F.599
DATA TRANSMISSION SERVICES	F.600–F.699
MULTIMEDIA SERVICES	F.700–F.799
ISDN SERVICES	F.800–F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850–F.899
ACCESSIBILITY AND HUMAN FACTORS	F.900–F.999

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

Recommendation ITU-T F.747.10

Requirements of distributed ledger systems for secure human factor services

Summary

Recommendation ITU-T F.747.10 provides general requirements and functional capabilities for distributed ledger systems (DLS) for secure human factor services.

This Recommendation describes the requirements for the secure human factor distributed ledger service model, which can solve conflicting goals of privacy protection and big personal human factor data utilization. This Recommendation also includes the functional capabilities for human factor distributed ledger shared nodes to perform machine learning without decryption on encrypted human factor data. However, the computational burden of machine learning for encrypted data may be excessive. To solve this problem, this human factor distributed ledger service model provides procedures for allowing the use of two or more encryption key pairs and notifying the key type. In addition, this Recommendation involves the integrity maintaining requirements for secure human factor services to maintain a safe distributed ledger and, checked from the beginning, to distribute personal human factor information. Therefore, the application of distributed ledger system in the distribution of personal secure human factor information can ensure transparent tracking from the distribution process to the final use path.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T F.747.10	2022-01-17	16	11.1002/1000/14644

Keywords

Distributed ledger service model, privacy protection expansion, secure human factor, transparency tracking.

[*] 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 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 2022

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 F.747.10

Requirements of distributed ledger systems for secure human factor services

1 Scope

This Recommendation describes requirements for distributed ledger systems (DLS) for secure human factor services, covering:

- Background;
- General requirements for DLS for secure human factor services;
- Functional capabilities for DLS for secure human factor services.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 block [b-ISO 22739]: Structured data comprising block data and a block header.

3.1.2 consensus [b-ISO 22739]: Agreement among DLT nodes that 1) a transaction is validated and 2) that the distributed ledger contains a consistent set and ordering of validated transactions.

3.1.3 digital signature [b-ISO 22739]: Data which, when appended to a digital object, enable the user of the digital object to authenticate its origin and integrity.

3.1.4 distributed ledger [b-ISO 22739]: Ledger that is shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism.

3.1.5 distributed ledger technology [b-ISO 22739]: Technology that enables the operation and use of distributed ledgers.

3.1.6 fork [b-ITU-T TS FG DLT D1.1]: Creation of two or more different versions of a distributed ledger.

3.1.7 hash value [b-ISO 22739]: String of bits which is the output of a cryptographic hash function.

3.1.8 health [b-WHO]: A state of physical, mental and social well-being in which disease and infirmity are absent.

3.1.9 ledger [b-ISO 22739]: Information store that keeps records of transactions that are intended to be final, definitive and immutable.

3.1.10 Merkle tree [b-NIST]: A data structure where the data is hashed and combined until there is a singular root hash that represents the entire data structure.

3.1.11 mining [b-ITU-T F.751.0]: A reward-seeking activity in some consensus mechanisms.

3.1.12 node [b-ISO 22739]: Elementary component from which a data structure is built.

3.1.13 public distributed ledger system [b-ITU-T F.751.0]: DLT system which is accessible to the public for use.

3.1.14 transaction [b-ISO 22739]: Smallest unit of a work process, which is one or more sequences of actions required to produce an outcome that complies with governing rules.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 block depth: The level of a block appended to the distributed ledger system chain from its the initial block.

3.2.2 electronic human factor records: The systematized collection of person and population electronically stored human factor information in a digital format.

3.2.3 human factor: Principles to the design of optimal life-style conditions with regard to human well-being, safety and health, including the development of existing technologies and the acquisition of new ones.

NOTE – Adapted from [b-ISO 6385] and [b-Wickens].

3.2.4 personal human factor information: The information collected by directly measuring the human body and its environments and which is transmitted to personal human factor devices or other devices through a communication network to be used for electronic human factor records.

3.2.5 personal human factor device: A type of device that measures the human body and its environments, and exchanges information collected with other human factor devices.

3.2.6 secure human factor: The human factor in information security.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPU	Central Processing Unit
DLS	Distributed Ledger Systems
DLT	Distributed Ledger Technology
IP	Internet Protocol
PDLS	Public Distributed Ledger Systems
UUID	Universally Unique Identifier
VRF	Verifiable Random Function

5 Conventions

In this Recommendation:

– The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

– The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

– The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Background

In recent years, personal human factor information has increased dramatically due to the development of personal health collection devices as well as hospital-based personal medical record data. One of the best models for the management and sharing of personal human factor data is the distributed ledger service model. The characteristics of the distributed ledger systems provide reliability using a distributed database with multiple nodes involved, and ensure transparency of the retrieval data using digital signatures and hash values. However, human factor data can be very sensitive in terms of information protection. Therefore, the public distributed ledger service model requires personal human factor information protection requirements (see Figure 1).

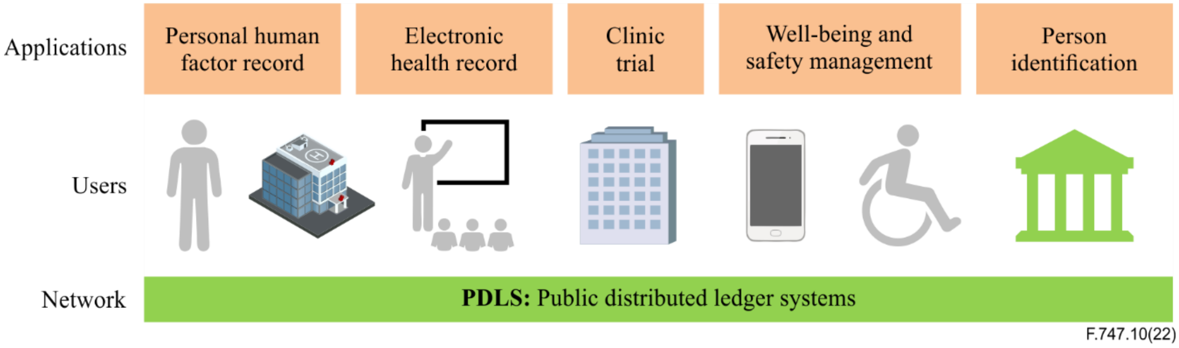
Applications
Personal human factor record
Electronic health record
Clinic trial
Well-being and safety management
Person identification
Users
Network
PDLS: Public distributed ledger systems
F.747.10(22)

Figure 1 – Human factor distributed ledger service model

This Recommendation describes the security requirements of the human factor distributed ledger service model, which can achieve goals of privacy protection and personal health big data utilization. The Recommendation also introduces the functional requirements of distributed ledger shared nodes to perform machine learning without decryption on encrypted data. It describes the incentive requirements in the distributed ledger service model to improve the quality of life by automating the distribution of health products directly to consumers and producers. The application of distributed ledger technology starts with the ability to track and manage health information production and distribution. In other words, the application of distributed ledger technology in the distribution of personal human factor information can ensure transparent tracking from the distribution process to the final use path. For this reason, individuals represented by individual nodes participating in the distributed ledger system can trust and use the information distributed. In addition, it is possible to provide a method for fundamentally blocking illegal distribution of personal human factor information.

7 General requirements for distributed ledger systems of secure human factor services

This clause describes the requirements for a secure distributed ledger movement management procedure that can achieve the conflicting goals of personal information protection and the use of personal human factor information big data. It introduces the functional requirements of a distributed ledger shared node to perform machine learning without decryption on encrypted data. For example, homomorphic encryption is a cryptographic technique that can perform all computations performed by a computer without decryption even in an encrypted state. Even in data analysis including personal information to be protected, machine learning can be optionally performed without personal information leakage or data loss.

7.1 Functional requirements for public distributed ledger shared nodes

The following are the functional requirements for public distributed ledger shared nodes:

- Nodes are required to store the data of the distributed ledger chain accumulated from the first block.
- The completion status is required to be delivered to the other nodes, as a node executes a distributed confirmation algorithm, when the transaction is verified.
- In order to verify the validity of the distributed ledger generated at each round, the node is required to check the validity of the generated block by comparing it with the target hash value.
- Each node is required to update and maintain shared data such as the public key list of all other nodes and the distributed ledger.
- The node is required to propagate the transaction to other nodes until the agreement phase (e.g., transaction confirmation completion) in the transaction verification process.
- The node is required to encrypt data of a transaction that requires security using the cryptographic keys (e.g., public key certificate [b-ITU-T X.509], homomorphic encryption [b-ISO 18033-6], verifiable random function (VRF) [b-IETF draft-irtf-cfrg-vrf-08] and inform the encryption key type.
- The node is required to determine whether the decryption is necessary. If the decryption is needed, it decrypts and transmits it to the requesting node. If there is no decryption needed, the node encrypts it with the public key of the request node, and transmits it.

7.2 Authentication requirements for new participating node

Existing nodes are recommended to provide the functions outlined in clauses 7.2.1 to 7.2.3, to authenticate new participating nodes in a distributed ledger shared system.

7.2.1 Requirements for requesting new node authentication

- The new node is recommended to have at least two pairs of encryption keys to use (e.g., public key certificate [b-ITU-T X.509], homogeneous encryption keys [b-ISO 18033-6] before making a request.
- The new node is recommended to encrypt the request message with its own private key and to send the encrypted data and its public key together to the node.
- Each node is recommended to update the list of verified public keys of the new and existing nodes and to store the public key list of the distributed ledger shared system to participate, when the node verifies and transmits the authenticated information.

7.2.2 Authentication functional requirements for the node

- The node is recommended to verify the validity by decrypting the encrypted data transmitted from the new participation desired node received together with the public key, to encrypt the verified information and the public key list with the public key of the new node and transmits the encrypted information.
- The node is recommended to be a list of public keys of all the nodes participating in the distributed ledger shared system and update its corresponding public key list each time it handles authentication of the new node.
- Each time the node is recommended to update its public key list, it is required to encrypt the public key list with its own private key and send it to all nodes participating in the distributed ledger shared system.

- The node is recommended to permanently store the verified information about the nodes participating in the distributed ledger shared system together with the verification time and the address of the participating node.

7.2.3 Requirements for new node authentication verification of existing nodes

- Existing nodes are recommended to verify the digital signature of the public key list sent by the node and to update it with the new public key list.
- Existing nodes are recommended to verify the participation of the authenticated new node by checking the new public key list.

7.3 Security requirements for distributed ledger system

Existing nodes are recommended to follow the provisions in this clause.

- Attempts to manipulate information in an existing shared distributed ledger are required to be verified using an electronic signature and rejected in the distributed ledger.
- Among the main chains used in the distributed ledger system, chains with different contents from the longest chain before an arbitrary b-block depth at the time a new block is created are required to be rejected in the distributed ledger. Here b is a number larger than equal to 1.
- The data is required to be rejected in the process of creating the distributed ledger, when data with duplicate addresses (e.g., IP, UUID) are added to the distributed ledger system.
- It is required that the common random source (e.g., cryptographic nonce [b-NIST]) be the same for blocks of any d-block depth. Blocks after d-block depth are required to update the common random source by a g-block depth. When updated, the hash of the newly added block is recommended to be used as a random source.

  NOTE – Here d-block and g-block depth means any blocks with depth larger than 1.
- Chains containing blocks with different hash values of previous blocks and Merkle tree root values are required to be rejected in the distributed ledger.
- If an error node occurs amongst the constituent nodes of the distributed ledger system, the nodes without errors are recommended to be maintained if above the pre-defined consensus level for the DLS.

7.4 Integrity maintaining requirements for a distributed ledger system

Existing nodes are recommended to follow the provisions in this clause.

- Each node is recommended to eliminate an attempt to manipulate information in the existing shared distributed ledger. If such an attack is detected, the number of nodes is recommended to be accumulated to obtain the ratio of the hashing force. It is recommended to compare the current number of block trees with the value of the threshold value to calculate safety and transmit (broadcast) related information and node addresses to all nodes.
- Each node is recommended to remove the longest chains commonly used in the distributed ledger system and chains with different contents from the distributed ledger system.
- Each node is recommended to remove the chain containing blocks with different hash values or Merkle tree root values of the previous blocks in the distributed ledger and calculate the accumulated number of nodes that were subject to attacks to determine whether the distributed ledger is safe, and to transmit (broadcast) the relevant information and the address of the node.

- When an error or forgery node occurs among the components of the distributed ledger system, each node is recommended to remove and accumulate the number of nodes attempted to perform an error or attack to obtain a hashing power ratio. In the distributed ledger, the number of secure nodes is recommended to be maintained to be greater than the threshold value and related information and node addresses are recommended to be transmitted (broadcast).
- Each node is recommended to reject the data in the distributed ledger creation process when new data with duplicate addresses is added to the data of the distributed ledger system.

8 Functional capabilities for distributed ledger systems of secure human factor services

As an incentive, it is required to improve the quality of life in a distributed ledger service model by automating direct distribution of personal human factor information. The application of distributed ledger technology starts with the ability to track and manage human factor information production and distribution. In other words, the application of distributed ledger technology in the distribution of personal human factor information can ensure transparent tracking from the distribution process to the final use path. For this reason, individuals represented by individual nodes participating in the distributed ledger system can trust and use the information distributed. In addition, it is possible to provide a method for fundamentally blocking illegal distribution of personal human factor information.

8.1 Distributed ledger structure in distribution of personal human factor information

Following the convention, the first transaction of the ledger is a special transaction that starts a new incentive (e.g., virtual coins [b-ITU-T F.751.0]) that will be disbursed to the creator of the ledger. This incentive is rewarded to nodes to maintain a distributed ledger and distributed from the beginning to distribute personal human factor information. The techniques for providing and distributing these incentives are recommended to be agreed in advance because they operate as distributed systems. The reason to continually add a certain number of new incentives is the compensation for nodes (miners) that consume resources to operate the distributed ledger system. These nodes consume central processing unit (CPU) computational power, memory and coins.

8.2 Two functions in distributed ledger structure in the distribution of personal human factor information

As a method to reduce the waiting time while increasing the mining speed, a technique of decomposing the structure of the basic distributed ledger into three functions can be optionally used. This can be seen as selecting the main chain in the distributed ledger protocol (e.g., the longest chain selection technique), which leads to the selection of the secure ledger among all ledgers at each depth of the ledger tree. Here, the depth of a ledger is defined as the distance from the origin ledger (the number of connected blocks in the ledger).

In a distributed ledger, the ledger serves three purposes. That is, it serves to elect the captain, add transactions to the main chain, and vote for the ancestor ledger through parent link relationships. In expressing the ledger as a conceptual action, it is divided into two functions (see Figure 2). The proposal function bundles transactions of the same depth in the original ledger tree. The voting function selects the ledger part of the ledger by voting for the same depth of transactions in the ledger tree. The selected ledger takes the partial ledgers of the transactions and forms the final ledger. This voting function operates at the same depth of the ledger tree and creates a parent-child connection. Therefore, the parent-child link of the original ledger tree has two functions that are explicitly separated: 1) Providing some order of ledgers in the transaction part at the same depth, 2) the voting function which helps to vote for each other to screen the ledger. The overall structure of the distributed ledger for the distribution of personal human factor information described below is shown in Figure 2.

Due to the distributed nature of DLS, it faces stability problems. In DLS, each node can record a transaction, but in the end, which node is selected is a result of the consensus algorithm [b-ITU-T F.751.0]. The design of a DLS is required to be taken into consideration as one of the many factors affecting stability, and the distributed ledger is recommended to recover stable service through adaptive processing of the system. In order to solve the stability problem of DLS, the common random source (e.g., cryptographic nonce [b-NIST]) is kept the same for d-block depths, and blocks after d-depths should update the common random source by g-block depths. When updated, the hash of the newly added block is used as a random source. If d = 1, it is restored to the basic update rule that forks every epoch, most vulnerable to contamination (balanced) attacks. In order to normally increase the security threshold, d may be increased. When d = ∞, all blocks use the nonce of the origin block as a common random source. This is the longest chain protocol that does not allow forking, allowing for private prediction of the chain by the contaminated owner of the secret key.

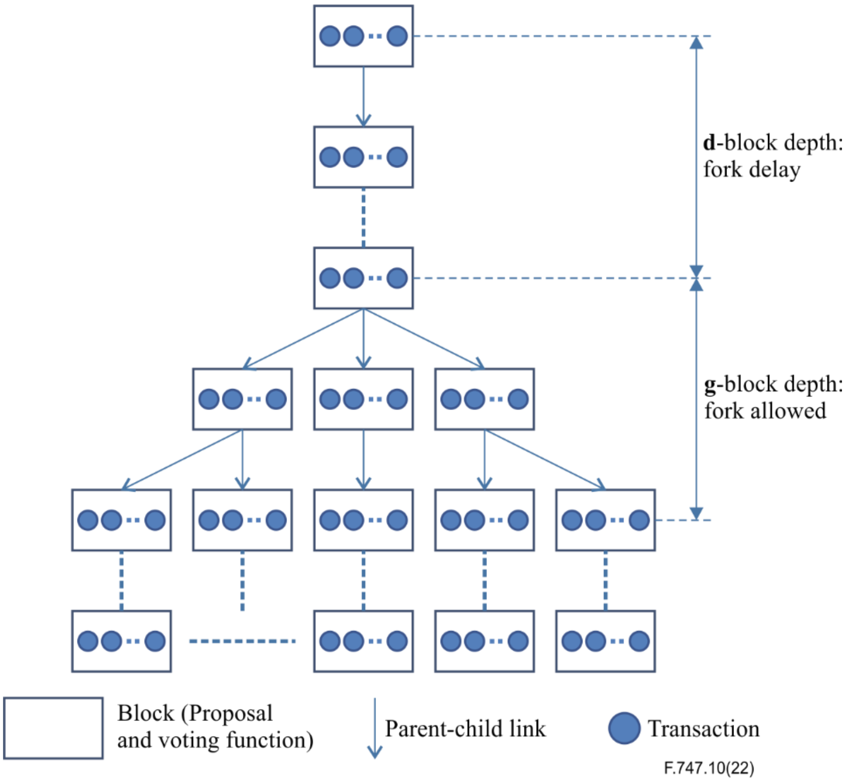

Figure 2 – Distributed ledger service model structure

8.3 Distributed ledger system maintenance methodologies

This representation of functional separation of a distributed ledger is much more complicated than that of a traditional distributed ledger, but it can improve the performance of the distributed ledger by deriving a faster consensus. This quick consensus deriving function can increase the number of ledgers in the transaction part without compromising the security of the distributed ledger in the proposed function. Therefore, the number of ledgers will be limited only by the capacity of the underlying communication network. The consensus can be optionally confirmed with low latency and high reliability since the voting function of multiple transactions will be voted in parallel to the ledger of the proposal for quick confirmation. The personal human factor information distributed ledger system is easy to manage because the general ledger generation rate has increased tremendously, and the number of partial ledgers of the proposed function per depth can be small.

This distributed ledger system can compromise transparency by concentrating the power of hashing into the proposed function of a specific transaction in the process of selecting the ledger. As shown in Figure 3, if an attacker's hashing power is strong in a specific ledger of the proposed function, it can be very vulnerable to security. Figure 3 shows an example of a chain of ledgers being destroyed or contaminated by the concentration of the hashing power of an attacker. If an attacker were able to gather more CPU computational power, memory, and coins in one place than all secure nodes, the attacker would have to decide whether to use it to steal honest node incentives or use it to cooperate. It would be necessary to provide an incentive policy so that it would be more beneficial for an attacker to follow the rules than to undermine the transparency of the personal human factor information distributed ledger system. This incentive is required to be adjusted to be distributed across participating nodes. The attacker can provide such a rule that it would be more profitable to associate with all other nodes. This rule is recommended to keep the number of honest nodes above the threshold value (e.g., CD (1 + α)/(α-1)/log(α)) according to the ratio of the hashing force of the attacker (α). Here C and D are capacity and delay of communication networks.

What can be seen from this formula is that if α is close to 0, the attacker's hashing power is weak, it can be said that there is no problem in the security of distributed ledger systems even if the number of the voter block-tree is a small number. However, if α is close to 1, that is, if the attacker's hashing power is strong, the number of the voter block-tree should be increased exponentially. At this point, it can be observed that it becomes very vulnerable to security.

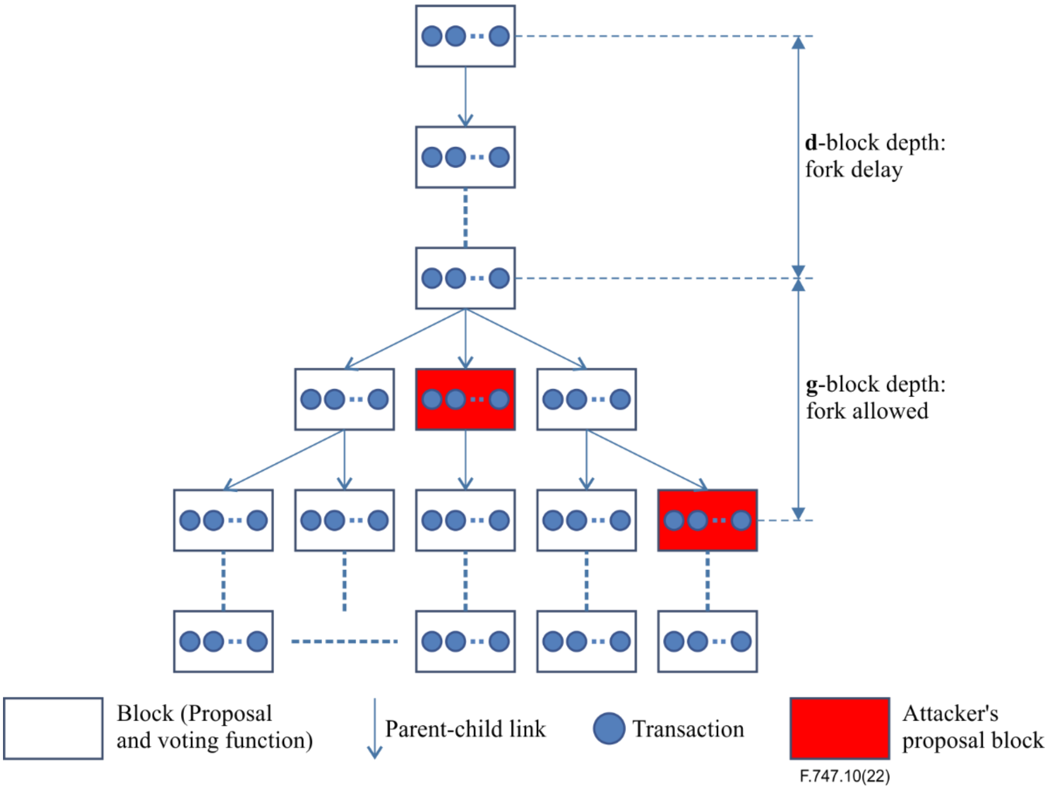

Figure 3 – Example of pollution prevention in distributed ledger service model

In the process of selecting the proposal block, the function of the block is recommended to be determined by adjusting the power of hashing and coins. At this time, it can be seen that if the attacker's hashing power and coins is strong, the security is very vulnerable. If an attacker could gather more computational power and coins than all honest nodes, a decision would need to be taken whether to use it to steal the benefits of an honest node, or to use it to cooperate. Incentive policies are recommended to be provided so that it would be more beneficial for attackers to adhere to the rules than to undermine the system and the legitimacy of their own wealth. Using a policy that prevents profits from being concentrated on a specific proponent block, this is recommended to involve providing such a rule that attackers would benefit more from allocating with all other nodes.

Annex A

Application to secure human factor distributed ledger service model

(This annex forms an integral part of this Recommendation.)

The distributed ledger scenario shown in Figure A.1 can safely and transparently manage not only hospital-centred personal human factor data, but also personal-centred human factor data such as personal health collection devices. In the example of using personal health information sharing in Figure A.1, reliability can be provided by using a distributed ledger in which multiple nodes participate, and digital signatures and hash values can be used to ensure transparency in search data. However, personal human factor data can be very sensitive in terms of data protection. Such sensitive data is registered in an encrypted state using an encryption technique capable of processing big data. The mobility procedure for sensitive personal human factor information follows the requirements and procedures of the distributed ledger shared system in clause 7.2 using an encryption algorithm (see Figure A,1). In addition, the distributed ledger system for personal human factor information is required to be operated to satisfy the requirements for the incentive function in clause 8.3 for activation and maintenance.

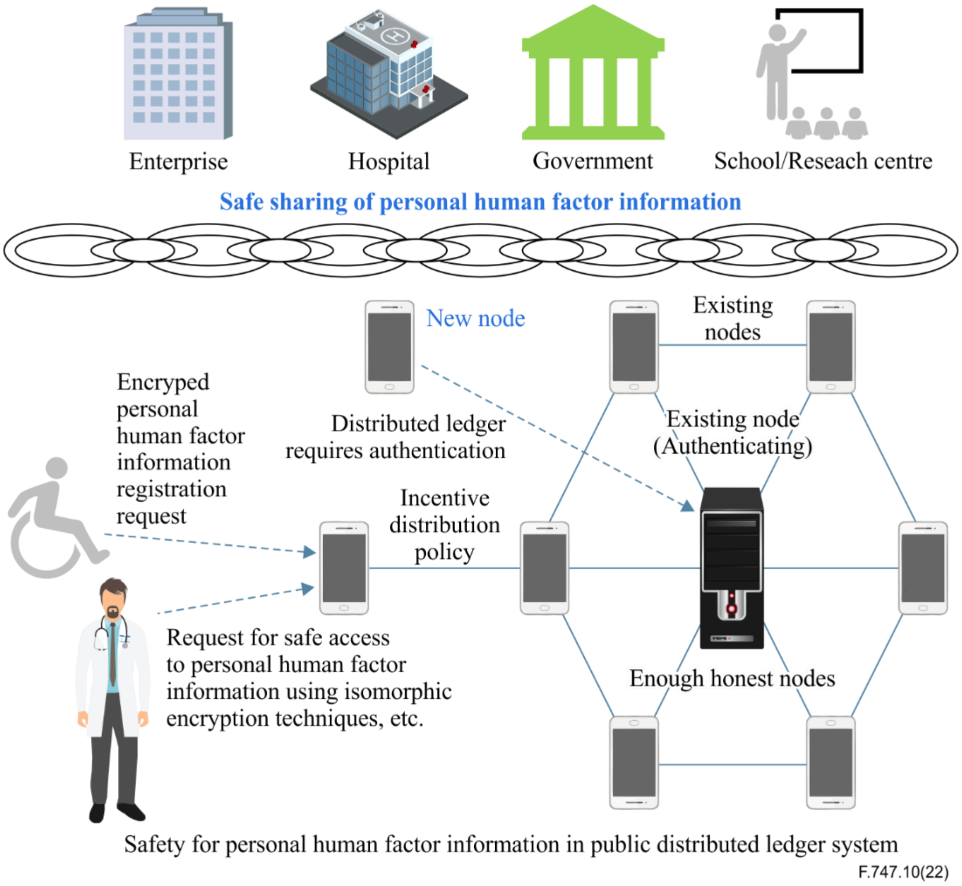
Enterprise
Hospital
Government
School/Reseach centre
Safe sharing of personal human factor information
New node
Existing nodes
Encryped personal human factor information registration request
Distributed ledger requires authentication
Existing node (Authenticating)
Incentive distribution policy
Request for safe access to personal human factor information using isomorphic encryption techniques, etc.
Enough honest nodes
Safety for personal human factor information in public distributed ledger system
F.747.10(22)

Figure A.1 – Scenarios for secure distributed ledger service model

Bibliography

[b-ITU-T F.751.0] Recommendation ITU-T F.751.0 (2020), *Requirements for distributed ledger systems*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T TS FG DLT D1.1] Technical Specification ITU-T FG DLT D1.1 (2019), *Distributed ledger technology terms and definitions*.

[b-IETF draft-irtf-cfrg-vrf-08] IETF draft-irtf-cfrg-vrf-08 (2020), *Verifiable Random Functions (VRFs)*. https://tools.ietf.org/html/draft-irtf-cfrg-vrf-08

[b-ISO 6385] ISO 6385:2016, *Ergonomics principles in the design of work systems*.

[b-ISO 18033-6] ISO 18033-6:2019, *IT Security techniques – Encryption algorithms – Part 6: Homomorphic encryption*.

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary*.

[b-NIST] NISTIR 8202 (2018). *Blockchain Technology Overview*.

[b-WHO] World Health Organization (2006), *Constitution of the World Health Organization – Basic Documents*, Forty-fifth edition, Supplement.

[b-Wickens] Wickens, D., Gordon, S., Liu, Y. (1997), *An Introduction to Human Factors Engineering*. pp.2-7. New York, NY: Longman.

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