TECHNICAL REPORT

ISO/TR 23244

First edition
2020-05

Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations

Reference number
ISO/TR 23244:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 307, *Blockchain and distributed ledger technologies,* in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information security,* Subcommittee SC 27, *cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document provides an overview of the issues and practical concerns related to privacy and personally identifiable information (PII) protection in the context of blockchain and distributed ledger technologies (DLT) and their applications.

Privacy and PII protection issues are widely considered as a major barrier for the adoption of DLT-based solutions. This document identifies and assesses known privacy-related risks and the way to mitigate them, as well as the privacy-enhancing potential of blockchain and distributed ledger technology.

Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations

1 Scope

This document provides an overview of privacy and personally identifiable information (PII) protection as applied to blockchain and distributed ledger technologies (DLT) systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22739[1)], *Blockchain and distributed ledger technologies — Terminology*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 29100, *Information technology — Security technique — Privacy framework is referred to in the text in order to provide terms and definitions*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22739, ISO/IEC 27000 and ISO/IEC 29100 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Abbreviated terms

The following abbreviations are used in this document:

DLT	distributed ledger technology
EU	European Union
ICT	information and communication technology
IoT	internet of things
PET	privacy enhancing technology
PII	personally identifiable information
ZKSNARK	zero-knowledge succinct non-interactive argument of knowledge

1) Under preparation. Stage at the time of publication: ISO/FDIS 22739:2020.

5 Privacy framework for blockchain/DLT systems

5.1 Overview

5.1.1 General

The following components relate to privacy and the processing of PII in blockchain and DLT systems and make up the privacy framework described in this document: These components are identified in ISO/IEC 29100:2011/Amd 1:2018, Clause 4, where they are further described.

— actors and roles;

— interactions;

— recognizing PII;

— privacy safeguarding requirements;

— privacy policies; and

— privacy controls.

In this document, respecting privacy means adhering to the privacy principles of ISO/IEC 29100:2011/Amd 1:2018, Clause 5. They are:

1) consent and choice;

2) purpose legitimacy and specification;

3) collection limitation;

4) data minimization;

5) use, retention and disclosure limitation;

6) accuracy and quality;

7) openness, transparency and notice;

8) individual participation and notice;

9) accountability;

10) information security;

11) privacy compliance.

These privacy principles apply to any ICT system containing or processing PII, including blockchain and DLT systems. Guidance on what constitutes PII can be found in ISO/IEC 29100:2011/Amd 1:2018, 4.4.

Even if a blockchain and DLT system appears to process no PII, the system and any processing, storage, transmission and disclosure can still have an impact on a PII principal. To evaluate whether PII is stored, transmitted or processed by a blockchain and DLT system, a PIA using the guidelines in ISO/IEC 29134, can be carried out. If the privacy impact assessment indicates that PII is stored, transmitted or processed, then the guidance provided in ISO/IEC 29100:2011/Amd 1:2018 can be followed.

There are multiple factors that affect the privacy safeguarding objectives.
ISO/IEC 29100:2011/Amd 1:2018, 4.5 provides corresponding guidance and identifies the following factors:

a) legal and regulatory factors;

b) contractual factors;

c) business factors; and

d) other factors such as privacy preferences of PII principal.

It is advisable to carefully evaluate and identify the relevant factors. For example, privacy is a fundamental human right according to the Universal Declaration of Human Rights of the United Nations and according to the laws of some jurisdictions, like the General Data Protection Regulation in the EU and under Article 21 of the Constitution of India, and thus needs to be treated accordingly if it is identified as applicable.

5.1.2 Actors and roles

There is guidance in ISO/IEC 29100:2011/Amd 1:2018, 4.2. In the case of blockchain and DLT systems, ISO/IEC 29100:2011/Amd 1:2018, 5.5.

5.1.3 PII principals

PII principals can have rights included in laws or regulations, such as the right to withdraw PII processing consent, to inquire about their PII on blockchain (and then require amendments) and the right to be forgotten. The situation is likely to become more challenging in the future. In certain jurisdictions, such as the EU, privacy is considered a fundamental human right which a PII principal essentially may not sell or give away, which makes agreements such as "PII in exchange for services" difficult to enforce.

In a blockchain or DLT system, the ability of a PII principal to withdraw consent, make amendments and delete information can conflict with the immutability of the ledger.

5.1.4 PII controller

With a distributed system, shared and used by multiple parties, legal questions arise about who is responsible for the system, particularly with respect to PII collection and PII processing. It is typical in many jurisdictions to describe the role of PII controller, responsible for the collection and processing of PII – and for notifying and obtaining consent from the PII principals about the collection and use of PII. Within public blockchain and DLT systems it can be difficult to identify the PII controller and can be unclear even for private blockchain and DLT systems.

Some jurisdictions are beginning to treat the nodes on a blockchain/DLT that validate transactions and generate blocks as joint PII controllers.

5.1.5 PII processor

A PII processor processes PII on behalf of a PII controller. This relationship can be contractual. A PII processor in turn can also subcontract processing activities to a "subprocessor". Within public and private blockchain and DLT systems it can be difficult to identify the PII processor(-s) and/or subprocessor(-s).

5.2 Interactions

There is guidance given in ISO/IEC 29100:2011/Amd 1:2018, 4.3. There are no special considerations in the case of blockchain and DLT systems.

5.3 Recognizing PII

5.3.1 General

There is guidance given in ISO/IEC 29100:2011/Amd 1:2018, 4.4. There are no special considerations in the case of blockchain and DLT systems.

5.4 Privacy safeguarding requirements

5.4.1 General

There is guidance given in ISO/IEC 29100:2011/Amd 1:2018, 4.5. For blockchain and DLT systems, 5.4.2 to 5.6.1 can apply.

5.4.2 Legal and regulatory factors

5.4.2.1 General

There is guidance given ISO/IEC 29100:2011/Amd 1:2018, 4.5.1. For blockchain and DLT systems, ISO/IEC 29100:2011/Amd 1:2018, 5.5, 5.6, 5.7, 5.8 can apply.

5.4.2.2 Legal and regulatory environment

Blockchain and DLT systems can involve many stakeholders living and working in different countries and different legal and regulatory environments. The challenge for a blockchain and DLT system and its stakeholders is to provide legal certainty through enforceable agreements, contracts and associated mechanisms, under an agreed and recognised legal jurisdiction.

A further challenge is that as some blockchain and DLT systems could not have a clearly defined "owner" or be a clearly identified legal entity, it can be difficult to apply the accountability principle as laid out in ISO/IEC 29100:2011/Amd 1:2018 and some jurisdictions can have difficulty in interacting with a system without clearly defined legal status.

5.4.2.3 Legal requirements to disclose

Courts and authorities can require disclosure, deletion, modification or addition of certain information or transactions. Complying with such legal requirements can be difficult for blockchain and DLT systems and their users, operators and administrators. A disclosure request and the disclosed data can identify a PII principal and/or provide relevant search attributes which can result in non-PII becoming PII, or allow a PII principal to be indirectly identified.

Modifying, deleting or adding information or transactions can be difficult on a blockchain or DLT system as this can destroy the integrity and immutability of the ledger; also, it can be difficult to gain agreement between users, operators and administrators to modify, alter or add to the ledger; and finally, the system may not have the capabilities to perform such activities.

If the legally required activities cannot be carried out, then users, operators and administrators can be subject to legal remedies such as the penalties stipulated in the EU General Data Protection Regulation.

The ability to modify, delete or add information is a serious risk for any organization or individual who have to comply with a legal request. In blockchain and DLT systems, the decryption of data could not be possible by users or operators.

5.4.2.4 Jurisdictional differences

A blockchain and DLT system can operate across multiple jurisdictions which can result in the need to comply with conflicting legal and regulatory requirements.

Possible jurisdictional differences include but are not limited to:

a) Definition of PII;

b) Application of the "right to remember" or the "right to be forgotten";

c) Legislation and legal process;