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;

d) Legislation covering ICT, ICT-related or enabled crimes, fraud, and human rights;

e) Legislation covering PII storage and location requirements; and

f) Legislation covering the definition of PII controller and processor.

These jurisdictional differences can affect what is possible for an extra-national blockchain and DLT system and can be a significant problem if the nodes of a blockchain and DLT system reside in multiple different jurisdictions where different laws and regulations apply, but also when they store and process PII of citizens from different countries or jurisdictions.

5.4.2.5 Intra-jurisdictional conflicts

There are conflicts between privacy laws and other laws in the same jurisdiction. It can be difficult to understand which laws take precedence and thus overrule any privacy statute. Examples where privacy statutes could be overruled include: laws relating to national security requiring the collection and storage of PII of individuals; national registries (such as land and real estate) where PII relating to ownership is publicly published.

Such conflicts could make compliance with some of the privacy principles problematic.

5.4.2.6 Impact of changing legislation & public expectations

Changing legislation and public expectations could tighten the requirements and penalties associated with privacy. The decentralised nature of blockchain and DLT systems make adapting to changing regulations more challenging.

At the same time, recognition of the benefits of blockchain and DLT by society as well as better awareness of decision-makers and the public in general can result in changes in the legislation and regulation in various jurisdictions aimed at dismantling unreasonable barriers to blockchain adoption, including relaxing some privacy-related requirements.

5.4.3 Storage of PII on blockchain and DLT systems

Placing PII on a blockchain and DLT system can result in any user, operator or administrator being able to view that PII. Such public access, unless directly authorized by relevant legislation or legally permitted by a data subject's informed consent, violates the purpose, legitimacy and specification principle; the minimization principle; the use, retention and disclosure principle; and the consent principle.

The application of the privacy principles listed in ISO/IEC 29100:2011/Amd 1:2018 implies that it is unwise to store PII in the ledger, unless laws and regulations applying to that PII permit the storage of that data in an immutable form. In addition, any PII stored in the ledger would have to be organized in such a way as to limit access to that data to a known and authorized set of users and to limit the logging thereof. This almost certainly excludes public blockchain and DLT systems from storing PII in the ledger.

A blockchain and DLT system can contain the PII of DLT system users, other DLT system stakeholders; there can be PII of other individuals who are entirely unconnected to the DLT system. To determine what PII is stored, a PIA using the guidelines in ISO/IEC 29134, can be carried out.

5.4.4 Contractual factors

5.4.4.1 General

There is guidance given in ISO/IEC 29100:2011/Amd 1:2018, 4.5.2. In blockchain and DLT systems, 5.5 through 5.7 could apply.

5.4.4.2 Agreements

User agreements, service level agreements, contracts, terms of service, by-laws and rules relating to blockchain and DLT systems can contain privacy-related clauses, which can provide legal certainty for stakeholders of a particular system. However, as blockchain and DLT systems can be decentralised and operate across multiple jurisdictions, setting the governing jurisdictions for the privacy-related clauses of user agreements, service level agreements, contract, terms of service, by-laws and rules can be difficult.

Additionally, any user agreements, service level agreements, contracts, terms of service, by-laws and rules need to balance the privacy rights given to individual users against the rights and needs of the community and the technical capability of the blockchain and DLT system.

5.4.4.3 Smart contracts

Smart contracts can, in the course of execution, reveal PII or reveal information allowing the identification of a PII principal indirectly. In some cases, the PII principals could not be aware that their PII has been revealed. Protection of PII can be included and agreed by the contracting parties when creating such smart contracts.

Further, a smart contract that does not count as a legal contract can perform automated processing of PII. Such automatic processing is prohibited in some jurisdictions.

Should PII be revealed, there can be difficulties in deciding who has to notify the PII principals, as the PII controller can be difficult to identify (see 5.1.3) and there can be difficulties in deciding how to notify the PII principals.

5.4.5 Business Factors

5.4.5.1 System lifetime and lifecycle

Blockchain and DLT systems can have a very long lifetime (e.g. land registers, which could be hundreds of years). With the privacy legislation becoming increasingly rigorous and providing more rights to data subjects including the deceased, and with the advances in methods and techniques for data analytics and profiling, there is a risk that a system conceived as containing no PII or designed to be fully compliant with the current privacy legislation can, in time, become non-compliant.

The life cycle of any information system is about 10 years with industrial IoT systems commonly having planned lifecycles of up to 30 years, so blockchain and DLT systems with long-term goals could need to migrate. Any migration can present risk, including the risk to PII. Migrating blockchain and DLT ledger records and maintenance are areas that could benefit from further study and practical experimentation.

5.4.5.2 IoT and blockchain.

As the internet of things continues to grow, it is being used in conjunction with blockchain and DLT systems.

IoT systems could collect and process PII, and this could bring about the issue of profiling and surveillance on individuals.

A challenge is to understand what IoT-related data could be safely placed onto a blockchain or DLT system while respecting privacy principles and complying with legal and regulatory requirements of relevant jurisdictions.

5.5 Privacy policies

There is guidance given in ISO/IEC 29100:2011/Amd 1:2018, 4.6. In blockchain and DLT systems, 5.6 through 5.7 could apply.

The privacy policy and notices associated with a blockchain and DLT system can be used to state how the system implements privacy principles, such as those stated in ISO/IEC 29100:2011/Amd 1:2018 and legal and regulatory documents.

The policy can state how the blockchain and DLT system can:

a) minimize the number of people/organizations who can access PII – provide access to those who have a “need-to-know” concerning any given element of PII and who can only use the PII for explicitly stated purposes (ISO/IEC 29100:2011, Principles 3, 4 and 5);

b) collect, store and notarize the consent and notice of the PII principals/data subjects (ISO/IEC 29100:2011, Principles 1 and 8);

c) provide openness, transparency and notice, for instance to notify PII principals/data subjects when their PII is accessed or modified by some person or organization;

d) retain PII for as long as necessary for the stated purposes of processing and delete and dispose of PII when the purpose for processing it is at an end (ISO/IEC 29100:2011, Principles 4 and 5);

e) keep PII accurate, complete and up-to-date (which implies potentially modifying the information) (ISO/IEC 29100:2011, Principle 6); and

f) provide PII principals with the right to access and review their PII, to request that PII be amended, corrected or removed (ISO/IEC 29100:2011, Principle 8).

NOTE Deleting and disposing of PII (ISO/IEC 29100:2011, Principles 4 and 5) can be a major challenge in an immutable environment such as a blockchain and DLT system.

5.6 Privacy controls

5.6.1 General

There is guidance given in ISO/IEC 29100:2011/Amd 1:2018, 4.7. In blockchain and DLT systems, ISO/IEC 29151, provides a set of privacy controls.

Blockchain and DLT architectures can have a major impact on privacy and the protection of PII. Figure 1 shows a typical blockchain and DLT system architecture, with the major services and components identified.

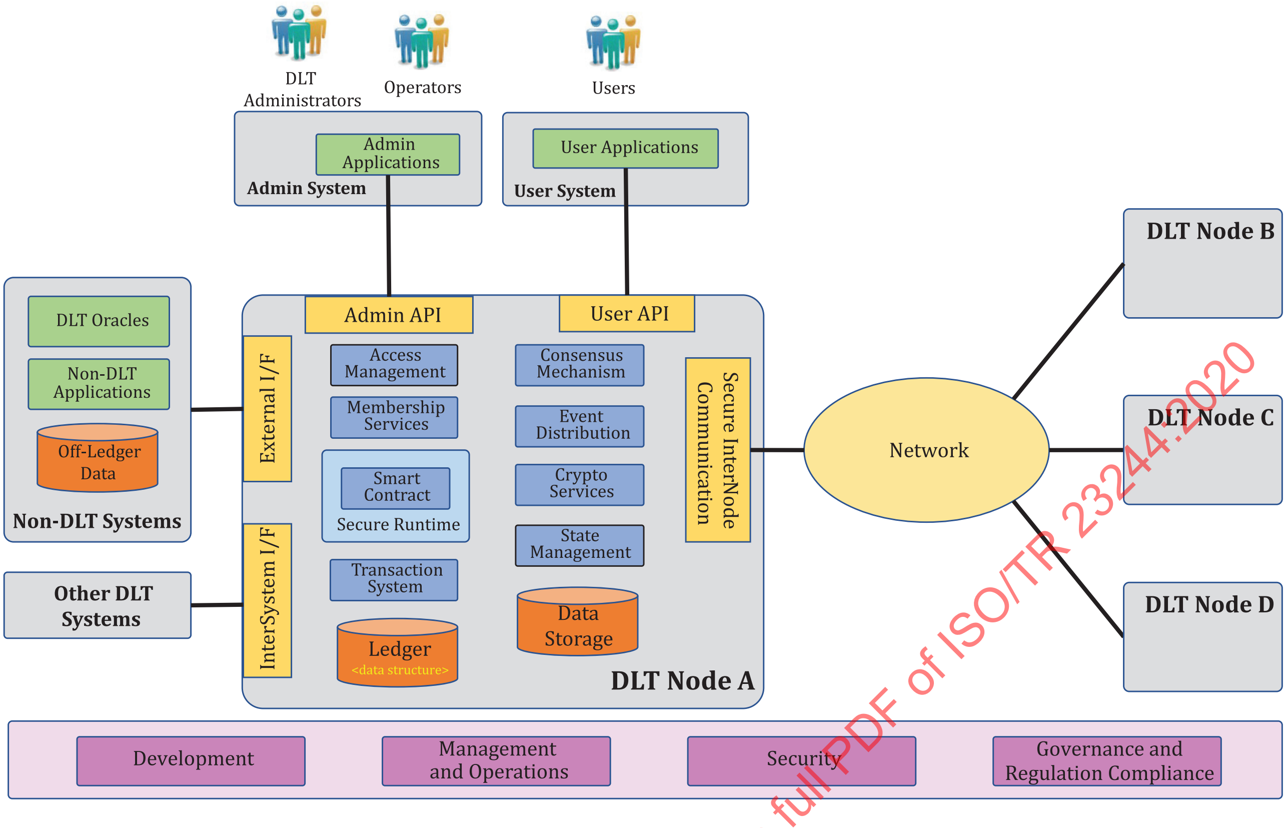

Figure 1 — Blockchain and DLT system architecture

Within this architecture, the application of access management, security and cryptographic services to applications, APIs and storage across both DLT and non-DLT systems can protect PII through technical and non-technical means. Many information security controls, which protect the confidentiality, integrity and/or availability of information and data are also suitable for the protection of PII. The selection of controls can be made using risk management techniques, business and information security policies and the capabilities of the services in the architecture.

It is also plausible to use the “privacy by design” paradigm in blockchain and DLT development to produce blockchain and DLT systems that provide appropriate PII protection.

5.6.2 On-chain and off-chain PII data storage and privacy considerations

5.6.2.1 General

PII can plausibly be contained in 2 datastores:

a) on-chain; and

b) off-chain.

5.6.2.2 On-chain PII storage

Personal information can be stored within blockchain blocks. If PII has to be modified, deleted, updated or changed in some way, then possible options include a hard fork in the chain or the cessation of the chain itself.

As the blockchain increases in size and as transactions are added, the accumulation of data within the blockchain itself and links to external databases and storage could lead to aggregation effects, resulting in the direct or indirect identification of a PII principal. Advances in analysis and profiling capabilities can also lead to aggregation or other effects, again resulting in the direct or indirect identification of a PII principal.

5.6.2.3 Off-chain storage

Where data is held off-chain, privacy and PII protection can be addressed by adopting the approach of ISO/IEC 29100.

Blockchain and DLT systems typically use hashes of files to allow the actual data to be held off-chain whilst a record of the file, confirming the existence of the file at a certain moment in time and its provenance and authenticity and enabling verification of its integrity, is held on the blockchain. This facilitates large related files to be held off-chain whilst the integrity of the data referenced is maintained through the use of the hashing function on the data. Identifiers can be used to point to PII held off the chain, where these identifiers are not derived from the data itself, and can probably only have a one-way relationship.

Storing information "off-chain" provides strong privacy of the transaction details. The off-chain system can be configured to restrict access to the transaction details to authorised parties only, supporting use cases where participants could wish to keep details of their bilateral transactions private from other blockchain participants.

However, storing information "off-chain" negates many of the advantages of using a blockchain in the first place. Although the use of hashes can highlight breaks, without transaction details, the blockchain could no longer be a single, shared "source of truth." The issuance and trading of negotiable, fungible digital assets is no longer possible without reference to an on-chain position-keeping system.

Additionally, storing transaction information off-chain typically requires that both counterparties maintain their own record, or delegate that responsibility to a trusted third party, which brings with it the same costs and disadvantages as restricting read access to the blockchain.

A major challenge for blockchain and DLT systems is the ability to ensure that a file or a block on a node and any associated off-chain storage has been deleted.

Blockchain and DLT can also integrate with distributed file systems. These file systems also have the same challenge of ensuring that if a file is deleted confirmation is received that the file was deleted on each node.

5.6.3 Privacy enhancing technologies applicable to blockchain and DLT Systems

5.6.3.1 General

Privacy enhancing technologies offer an ability to protect data through a variety of means. Some of the current approaches include:

a) cryptographic techniques;

b) network techniques;

c) blockchain frameworks; and

d) channel-based techniques.

5.6.3.2 Cryptographic techniques

5.6.3.2.1 General

Typically, data is encrypted on blockchain and DLT systems using a variety of cryptographic mechanisms. Using cryptographic techniques typically requires associated services such as key management.

Advances in cryptography can render existing cryptographic techniques obsolete. Obsolete techniques can be easier to attack, resulting in threats to the integrity and immutability of the ledger and any PII stored within the ledger. For example, quantum computers are considered as a very real threat to existing cryptographic systems and their security.

A challenge for blockchain and DLT systems is to be able to change or upgrade the cryptographic techniques; as the information in ledger transaction records is encrypted, it is viewed as immutable, and switching to a different form of cryptography if the original algorithm is broken is seen as problematic. Migrating cryptography of encryption is not an easy problem. It should be noted also that there can be a need to keep the old encrypted records for later revealing.

5.6.3.2.2 Public key cryptography

Public key cryptography is the foundation of blockchain technology and forms the basis of many of the privacy techniques surveyed in this report.

Public key cryptography is primarily used for two things:

a) encryption and decryption of sensitive data; and

b) digital signatures to prove the authenticity of a message.

5.6.3.2.3 Homomorphic encryption / fully homomorphic encryption

Homomorphic encryption allows arithmetic operations (e.g. addition, multiplication) to be carried out on encrypted values; when the result is decrypted, it yields the same result that would have been achieved had the same calculation been carried out on the unencrypted inputs. See ISO/IEC 18033-6.

Many cryptosystems are partially homomorphic. For example, the RSA cryptosystem is multiplicatively homomorphic. If two numbers are encrypted separately using the same key, the ciphertexts multiplied, and the result then decrypted, then the same result would be obtained as would be if the two original numbers were multiplied.

One practical blockchain and DLT application of homomorphic encryption is to allow untrusted third parties to carry out computation on encrypted data.

5.6.3.2.4 Format preserving encryption

Format-preserving encryption is designed for data that is not necessarily binary. In particular, given any finite set of symbols, like the decimal numerals, a method for format-preserving encryption transforms data that is formatted as a sequence of the symbols in such a way that the encrypted form of the data has the same format, including the length, as the original data.

a) to encrypt a 16-digit credit card number so that the ciphertext is another 16-digit number;

b) to encrypt an English word so that the ciphertext is another English word; and

c) to encrypt an n-bit number so that the ciphertext is another n-bit number (this is the definition of an n-bit block cipher).

5.6.3.2.5 Zero knowledge proofs

Zero-knowledge proofs are cryptographic protocols that allow one party to prove to another party that a statement is true without revealing any information apart from the fact that the statement is true.

There are many different zero knowledge proof protocols. The specific implementation can provide differing levels of privacy. There are some implementations that hide both sender, receiver and amount.

5.6.3.2.6 Pedersen commitments

Commitments are a cryptographic mechanism which allow one to keep a piece of data secret (termed the blinding factor) but "commit" to it by publishing a hash of the data.

Having "committed" to the piece of data by publishing the hash, the publisher can later reveal both the blinding factor and the data, allowing others to verify that the hash of the blinding factor and data matches the hash that they published.

Pedersen commitments are also used in CryptoNote-based blockchains to hide the amounts transacted.

5.6.3.2.7 Ring signatures

In order to verify a standard digital signature, the verifier needs to know which public key was used to create the signature. This is what allows observers to trace the flow of funds from address to address. Ring signatures were invented by Rivest, Shamir and Tauman in 2001 as a means of creating a signature with a group of potential signers, without revealing which member of the group actually created the signature.

A ring signature is created using group of keys, which includes the signer's own key (for which he possesses the secret key) and a number of other public keys chosen by the signer (no consent or participation by the other public keys' owners is required). A third party can verify that the resultant signature was created using one of keys in the group, but it is not possible to identify which key in the group belongs to the signer.

5.6.3.2.8 Blind signatures

A blind signature scheme allows a message to be signed by someone without revealing the message to the signer. This is done by first "blinding" the message with a blinding factor. Then the signer signs with his private key the message+blinding factor. Finally, the party that blinded the message can unblind the result to get the signed message.

5.6.3.2.9 One-time use payment addresses

Re-using the same payment address makes it easy for an observer to watch the transactions being received and sent. An obvious solution is to avoid re-using addresses; this is an approach generally referred to as one-time use payment addresses. When using this approach, the sender generates a new address each time they wish to receive a transaction. Because the new address has no prior transaction history on the blockchain, it's more difficult for an observer to assemble a comprehensive view of transaction flows.

5.6.3.2.10 Stealth addresses

One-time use payment addresses can be unwieldy to manage. Each new address needs to be generated by the recipient and communicated to the sender, which could result in the creation of a new email each time a communication from another party is to be received.

Stealth addresses remove this requirement by allowing the sender to generate the new one-time use payment address. To use a stealth address, the recipient generates a parent key pair and publishes the public key - this is the stealth address. Any sender can then use the stealth address to generate a new one-time use payment address. The recipient uses their parent private key to calculate the one-time use payment address' secret key, which is required in order to spend the funds.

There is no way for an observer to link a one-time use payment address to the stealth address used to generate it. More importantly, only the recipient can calculate the one-time use payment address' secret key. Despite the fact that it is the sender who generated the new one-time use payment address, the sender does not know the secret key and there is no way for he or she to calculate it.

5.6.3.3 Combining cryptographic techniques

Table 1 provides examples of how different cryptographic techniques could be combined to enhance privacy and PII protection.

Table 1 — Overview of effect of combining privacy enhancing technologies on the overall privacy of a blockchain and DLT system

Privacy enhancing technology method	Sender	Receiver	Block/Ledger entry
Stealth addresses	No privacy protection	Privacy protection	No privacy protection
Pedersen commitments	No privacy protection	No privacy protection	Privacy protection
Ring signatures	Limited privacy protection	No privacy protection	No privacy protection
Zero knowledge proofs	Privacy protection	Privacy protection	Privacy protection

For example, combining stealth addresses with zero knowledge proofs can provide privacy protection for both the sender and the receiver and protect privacy in the ledger.

5.6.3.4 Network techniques

5.6.3.4.1 Mixing data sharing controls between blockchain and DLT nodes

Transactions in a public blockchain can be linked and open to graph analysis. It is simple to follow the flow of funds from address to address. One-time use payment addresses do not solve this. The path of the funds from sender to receiver is clear. Mixing is a technique to confuse this path.

Typically, a mixer can take inputs and outputs from a number of users simultaneously and then shuffle the inputs and outputs to break the connection. That is, if Alice is sending some funds to Charlie, and Bob is sending the same amount to David, a mixer could take Alice's fund and send it to David, while taking Bob's amount and sending it to Charlie.

5.6.3.4.2 Blinding of identifiers

A blinding factor is a randomized string of letters and numbers that is multiplied by the value being transacted to obscure the network from knowing how much is really being transferred. Multiplying the blinding factor by the value being transferred produces a new public key called a "Pedersen commitment". The sender and receiver each create their own Pedersen commitment and subtract the receiver's Pedersen commitment from the sender's (output — input). When the transaction is published to the blockchain, validating nodes just see the resulting Pedersen commitment.

5.6.3.4.3 Tor/I2P/Dandelion++

These technologies can be used to protect IP addresses and hence hinder the indirect discovery of the PII principal using an IP address.

This provides an anonymous network built on top of the internet. That allows users to create and access content and build online communities on a network that is both distributed and dynamic. It is intended to protect communication and resist monitoring by third parties.

5.6.3.5 Blockchain frameworks — Coco framework

The Coco Framework is not a standalone blockchain protocol; it provides a trusted foundation that delivers efficient consensus algorithms and flexible confidentiality schemes – a framework with which existing blockchain protocols can be integrated to deliver complete, enterprise-ready ledger solutions.

5.7 Privacy and identity management

Specific details on blockchain and DLT identity management can be found in future ISO reports or standards.

6 Privacy impact assessment

6.1 General

The PIA for blockchain and DLT systems can follow ISO/IEC 29134. Depending upon the use case a risk profile can be created and reviewed.

6.2 Privacy impact assessment as part of the overall risk management program

A challenge with blockchain and DLT systems is understanding who, where and when should carry out risk assessments and who is the risk owner. Understanding the overall risk to the systems and having an overall view can be challenging in the distributed environment. It is challenging to understand who needs to treat the identified risks and how reporting on risk treatment could occur.

The same challenges occur with PII because of the difficulty in identifying the PII controller and processor(s) in a public blockchain.

6.3 Privacy threats

Blockchain and DLT systems can be exposed to threats to information contained in the system, including PII.

Typical threats include:

a) uncontrolled access to information and PII;

b) accidental or deliberate exposure of PII;

c) poor implementation of security technologies, including cryptography;

d) loss or publication of cryptographic keys;

e) loss or publication of access credentials;

f) exploitation of obsolete or out-of-date hardware, middleware and software; and

g) attacker writing sensitive PII into the ledger.

6.4 Privacy vulnerabilities

Blockchain and DLT systems, being based on ICT systems, can be exposed to vulnerabilities similar to those already experienced by those ICT systems.

Typical vulnerabilities include:

a) poor password management (to include using default passwords);

b) lack of access management;

c) poor patching and updating processes;

d) poor coding practices (to include the use of backdoors);

e) poor user training; and

f) poor physical security.