TECHNICAL REPORT

ISO/TR 24374

First edition
2023-04

# Financial services — Security information for PKI in blockchain and DLT implementations

Reference number
ISO/TR 24374:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 68, *Financial Services*, Subcommittee SC 2, *Financial Services, security*.

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

Even though DLT/Blockchain-based solutions are at a relatively early stage of adoption and significant challenges remain, they hold the potential [7] for major opportunities across several sectors. While the financial sector has shown widespread early interest in DLT/Blockchain, other public and private sector organisations that rely on the keeping of records and management of secure transactions also benefit. DLT/Blockchain also provide opportunities in the healthcare, pharmaceutical, creative, and food sectors.

In light of the growing interest in DLT/Blockchain, standardisation efforts have gathered momentum, particularly with the setting up of the ISO technical committee https://www.iso.org/committee/6266604.html on Blockchain and electronic distributed ledger technologies (ISO/TC 307 Blockchain and distributed ledger technologies).

ISO/DTR 23245 states that: '(i) The essential part of key lifecycle management for blockchain is similar to an ordinary PKI type system (ii) Some blockchain applications do not have the revocation process for the key pair. In such cases different type of key management process is needed.'

Consideration of the major implications and the impact that DLT/ Blockchain will have on current PKI implementations for financial services is essential to minimise any potential disruption.

# Financial services — Security information for PKI in blockchain and DLT implementations

## 1 Scope

This document describes the management of cryptographic keys in a blockchain, or distributed system used in the financial sector

The objective of this document is to consider the impact of different types of key management processes that are required for PKI implementations in Blockchain and DLT projects

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

**3.1**
**blockchain**
*distributed ledger* (3.4) with confirmed blocks organized in an append-only, sequential chain using cryptographic links

Note 1 to entry: blockchains are designed to be tamper-proof and to create final, definitive, and immutable *ledger records* (3.10).

**3.2**
**consensus**
agreement among DLT nodes that a) a transaction is validated and b) that the *distributed ledger* (3.4) contains a consistent set and ordering of validated transactions

**3.3**
**consensus mechanism**
rules and procedures by which *consensus* (3.2) is reached

**3.4**
**distributed ledger**
*ledger* (3.9) that is shared across a set of DLT nodes and synchronized between the DLT nodes using a *consensus mechanism* (3.3)

[SOURCE: ISO 22739:2020, 3.44]

**3.5**
**distributed ledger technology system**
**DLT system**

system that implements a *distributed ledger* (3.4)

**3.6**
**distributed ledger technology**
**DLT**
technology that enables the operation and use of *distributed ledgers* (3.4)

**3.7**
**distributed ledger technology node**
**DLT node**
distributed ledger technology device or process that participates in a network and stores a complete or partial replica of the *ledger records* (3.10)

**3.8**
**hardware security module**
**HSM**
hardware implementation of a secure crypto-processor using an ITU-T X.509 certificate and a private key to provide secure authentication (ISO/IEC 19790:2012 security level 3 or higher)

**3.9**
**ledger**
information store that keeps records of transactions that are intended to be final, definitive, and immutable

**3.10**
**ledger record**
distributed ledger technology record comprising hashes of transaction records or references to transaction records recorded on a *blockchain* (3.1) or distributed ledger system

[SOURCE: ISO 22739:2020, 3.30]

## 4 Symbols and abbreviated terms

| | |
|---|---|
| API | Application Program Interface |
| BCP | Business Continuity Plan |
| BTC | Bitcoin |
| CA | Certificate authority |
| DHT | Distributed hash table |
| CRL | Certificate Revocation List |
| DTR | Draft technical report |
| ETL | Extract, transfer, and load |
| HSM | Hardware security module |
| KYC | Know your customer |
| LDAP | Lightweight Directory Access Protocol |
| MITM | Man-In-The-Middle |
| OCSP | Online certificate status protocol |
| PAX | Paxos Standard |
| PKI | Public key infrastructure |

| | |
|---|---|
| VPN | Virtual Private Network |
| WoT | Web of Trust |

# 5 Relevant issues - Distributed Ledger Technology (DLT) / Blockchain and PKI

## 5.1 DLT/Blockchain data security and privacy concerns

### 5.1.1 General

Blockchain and DLT systems involve nodes on a peer-to-peer network that store data, where the data finality is agreed upon via a consensus mechanism. Each node has a cryptographic module to conduct cryptographic operations as specified in the underlying protocol. Though blockchain networks and services do not have a centralized server, it does not mean protection of a node is not needed. Best efforts to protect each node is an essential part in securing the entire blockchain based system.

At its most basic, blockchain technology projects are a peer to peer based distributed ledger or databased organized by a set of protocols combined with a blockchain, i.e., a series of encrypted sets of data that record immutable changes over time.

One of blockchains greatest assets is its write-once, append many distributed nature; it can be easily deployed across disparate nodes on the web, yet each record contains its own hash making it immutable. To this end, cryptography is the primary means to protect the applications, networks, infrastructure, and services from cyber-threats. However, the existing public key infrastructure (PKI) is based on a central certificate authority (CA) that can become a bottleneck which will affect the efficiency of the cryptographic protocols because of the overhead incurred by the verification of cryptographic signatures and certificates. Recently, blockchain has also been leveraged to aid PKI without the need for a central authority. But it also creates unique security [7] challenges which are described in clause 5.

### 5.1.2 From centralised to decentralized

Blockchain shifts data storage and protection from a centralized to a decentralized model. In traditional centralized models, security methods can be consolidated with the technology products they serve. Blockchain, however, requires innovative security measures to protect the dynamic and highly distributed financial products the technology aims to support.

As with any crypto-based infrastructure, protecting keys is paramount to ensuring a blockchain system's security.

A successful blockchain system needs highly reliable methods of interfacing with the strong key protection practices afforded by HSMs, secure elements, and other computing environments designed for secure execution of code, and all of these deliver the scaling and flexibility a decentralized blockchain model needs.

### 5.1.3 Instant exploitation

Anyone who obtains the key can monetize and exploit the asset instantly. As seen in security breaches in public blockchain settings, such as Bitfinex, Mt. Gox and others, the malicious transfer of 'value' can be instantaneous, irreversible, and significant. Participants in these systems lost millions of dollars because of compromised security systems. However, note that these attacks exploited vulnerabilities at the application layer—the wallets holding the keys to the assets—rather than the underlying blockchain protocol. So far, blockchain technology itself has proved tamper-proof, within the limits presented by the consensus mechanism adopted by the network.

### 5.1.4 Protecting the key is critical

The ability to add transactions to a transaction database broadens the technology's applicability.

Traditional PKI is CA based, so the security of PKI systems are at risk if one CA is compromised For example, a framework mitigates the problems with PKI such as the difficulties with rapid certificate revocation, elimination of single points of failure and CAs' malfunctions. Note that If the root CA were to be compromised, an attacker could gain control of the entire PKI and compromise trust in the entire system, including any sub-systems reliant on the PKI. [1]

## 5.2 Problems and attacks associated with PKI systems

### 5.2.1 Current Challenges of Public Key Infrastructure

The most commonly employed approach to PKIs is the Web PKI. It is a Certificate Authority based system that adopts a centralized trust infrastructure. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. Verification is required to check the authenticity of the party with whom the secure connection is established. The most important task is to establish the correspondence between the identity (identification data) and the user's public key. This problem is solved using a public key certificate — an electronic document used to prove ownership of a public key. The certificate contains the public key and user credentials, as well as the electronic signature of the trusted party that verifies the user. To ensure the integrity and authenticity of the certificate, it is signed by a trusted party – a certification authority.

Centralized Web PKI solutions have several significant problems.

a) There are some challenges associated with quick notification of key compromise, since the formation and distribution of the list of revoked certificates can take from several minutes to an hour, unless synchronous verification protocols like OCSP are used. As a result, there is no 100% guarantee that this key is still valid. This problem is also relevant for DLT systems, where a transaction could be signed by a key that is no longer valid or under the sole responsibility of the owner. If the certificate is verified online (by request to the certification authority), then the user's privacy is violated, since the certification authority will know the entire history of user interaction.

b) The definition of the list of trusted CAs in a PKI system could be complex and could require some specific out-of-protocol management, although successful collaborations have resulted in highly-federated environments, like the European Trusted Services List. A decentralized system could also be impacted by this problem.

c) The centre of the system is always an attack point and compromising the root certificate will expose the entire system to a bunch of vulnerabilities.

d) Identifier management is in the hands of a centralized organization and does not belong to the identifier owner himself.

There are significant sources of failures of PKI that neither the usability nor traditional computer security community is engaging. Specifically, there are incidents that illustrate systematic weaknesses of organizational practices that create risks for all who rely upon PKI. However, there are organizational and configuration choices that could avoid or mitigate some of these risks.[15]

In decentralized PKI, blockchain can act as a decentralized key-value storage. It is capable of securing the data read to prevent MITM (Man-In-The-Middle) attacks, and to minimize the power of third parties.

### 5.2.2 Attacks to PKI

PKI is exposed to risks due to potential failures of certificate authorities (CAs) that can be used to issue unauthorized certificates for end-users. Many breaches show that if a CA is compromised, the security of the corresponding end-users will be in risk. There are many cases where CA's errors or breaches have resulted in unauthorized certificates being issued.[12]

Another important weakness of PKIs concerns the reliability and security of certificate revocation lists (CRLs or associated OCSP servers), which are used to ensure proper lifecycle management of certificates, particularly the revocation, and are to be queried any time a certificate is used. Classically, the CRL for a set of certificates is maintained by the same (and sole) certification authority (CA) that issued the certificates, and this introduces a single point of failure into the system.

In fact, CRLs do not operate in real time; they are commonly updated periodically by the issuing CA, and there can be a delay between a security breach and the subsequent CRL update, resulting in the temporary use of compromised certificates. The theft of a certificate (with its associated private key) could be unknown to the CA, and the certificate is not revoked in this case.[10] See Annex A for possible solutions.

## 5.3 Security objectives

DLTs that use cryptographic PKI as their security mechanism are resistant to attackers who are not in possession of the appropriate keys. This, in addition to the shared data and tamper-resistant properties of blockchain solutions, means that DLTs have a high level of security. For this reason, provided that controls, see Annex B, such as key management follow industry best practice, DLTs are potentially [7] more robust from a cybersecurity perspective than systems relying on physical or network security, or which are locked with manually-generated passwords rather than cryptographic private keys. DLT also presents integration challenges with hardware security modules (HSMs) for key storage and generation, and security infrastructure such as virtual private networks (VPNs).

HSMs provide limited mechanisms for detection of key misuse, e.g., data encryption versus PIN encryption, signature keys versus encryption keys. DLTs could be based on cryptographic schemes that are not necessarily supported by HSMs, secure elements, nor properly managed by other security components, and that need to consume and process information signed with those keys Also if an attacker compromises a system or application that has permissions to use keys in the HSM, or if a rogue insider abuses such permissions, this will give them the ability to sign fraudulent cryptocurrency transactions. One such signature is enough to empty all cryptocurrency in a specific address[10].

Integration challenges with DLTs relate to their security model, which is largely based on PKI (public key infrastructure)[10]. Access rights to writing blockchain state data typically require data transactions to be signed by a specific private key, while reading blockchain state data requires access to either the ledger file (stored on several servers) or access to the interface mechanisms placed over the blockchain data. These interfaces are typically secured via a network credential system (linked to the corporate directory) or a custom password authentication mechanism. Note this varies between DLT systems and in fact does not exist for public permissionless DLT systems.

Security mechanisms are an important consideration when integrating highly secure, cryptographically-based blockchain security protocols with other, potentially looser access and control rules in existing legacy systems. Integration from a data point of view is relatively straightforward via standard programming interfaces, assuming that the data integration takes place within the established security framework and standard ETL processes. Once blockchain systems have a secure standard interface, (to be defined) they essentially become another enterprise component, albeit with the unique properties of DLT systems - specifically the immutable record of transactions in a decentralised network where peer nodes share data, assets, and value.

Blockchains can also be used to secure the data in other systems. For example, database backups can be timestamped with a hash of the data to ensure integrity of the backups for regulatory purposes.

Cryptographic approaches such as Merkle trees, [18] make it possible to secure large amounts of data at an individual data row level. A Merkle tree separates the validation of the data from the data itself — the **Merkle** tree can reside locally, or on a trusted authority, or can itself reside on a distributed system.

## 5.4 Summary of the use of asymmetric key cryptography in blockchain networks

Here is a summary of the use of asymmetric-key cryptography in many blockchain networks.

- Private keys are used to digitally sign transactions.
- Public keys are used to derive addresses.

- Public keys are used to verify signatures generated with private keys.
- Asymmetric-key cryptography provides the ability to verify that the user transferring value to another user is in possession of the private key capable of signing the transaction.

Some permissioned blockchain networks can leverage a business's existing public key infrastructure for asymmetric-key cryptography to provide user credentials – rather than having each blockchain network user manage their own asymmetric-keys. This is done by utilizing existing directory services and using that information within the blockchain network. Blockchain networks which utilize an existing directory service can access it via existing protocols, such as the Lightweight Directory Access Protocol (LDAP) [10], and utilize the information from the directory natively, or import it into an internal certificate authority within the blockchain network.[9]

### 5.5 Private key storage

If a user loses a private key, then any digital asset associated with that key is lost, because it is computationally infeasible to regenerate the same private key. If a private key is stolen, the attacker will have full access to all digital assets controlled by that private key. The security of private keys is so important that many users use special secure hardware to store them; alternatively, users can take advantage of an emerging industry of private key escrow services.

These key escrow services can also satisfy KYC laws in addition to storing private keys, as users provide proof of their identity when creating an account. Private key storage is an extremely important aspect of blockchain technology. When it is reported in the news that "Cryptocurrency XYZ was stolen from…", (one of the biggest cryptocurrency thefts ever) [13] it almost certainly means some private keys were found and used to sign a transaction sending the money to a new account, not that the blockchain network itself was compromised. Note that because blockchain data cannot generally be changed, once a criminal steals a private key and publicly transfers the associated funds to another account, that transaction generally cannot be undone.

## 6 Security and privacy activities

### 6.1 Cryptographic tools

The security of an arrangement is central to the safety and soundness of the financial system. Cryptographic tools, such as public key cryptography, play a central role in ensuring the security of existing systems and are of critical importance in DLT arrangements. While current cryptographic tools are considered effective and are widely used today, future technological advancements could render existing cryptographic tools less secure and effective. This issue is of particular concern for an arrangement with a weak governance [3] structure, which is not able to react quickly enough to emerging security issues and threats. Integration of DLT in existing infrastructures or transition from current systems to DLT-based ones could also generate security breaches that are not inherent in the new technology but could have a strong operational impact. Thus, arrangements are likely to not only rely upon cryptographic tools themselves but could also take a layered approach to security and leverage additional tools.

Questions to be considered include.

- What are the key operational risks for the arrangement, particularly those that could affect its resilience and reliability, security, and operational capacity and scalability? How does the arrangement generally manage these risks?
- How do these risks and their management differ from traditional arrangements, if at all?
- How does the arrangement layer security that goes beyond the reliance on cryptography need to adapt?

### 6.2 Governance activities

Governance structures can improve the safety of an arrangement (for example, by enhancing decision-making pertaining to the arrangement's design and technological evolution or by the involvement of a broad spectrum of stakeholders) or weaken it (for example, by slowing incident responses related to operational issues in the case of highly complex governance structures). An arrangement that involves the sharing of information and of ledger maintenance will need to have an especially well-thought-out governance structure. Recent governance challenges relating to several unrestricted DLT use cases have highlighted the critical importance of having a clear understanding of the governance arrangements surrounding change and incident management, and of the enforcement of governance decisions.[4]

Industry has high expectations about blockchain applications as a new enabler to shorten middleware costs and provide additional value such as trust and security. These high-expectations shown by communities on this topic represent a risk for its coming applications and how blockchain is impacting society. [16]

### 6.3 Operation activities

DLT presents integration challenges with hardware security modules (HSMs) for key storage and generation, and security infrastructure such as virtual private networks (VPNs). HSMs do not typically provide mechanisms for detection of key misuse and have no quorum authorization structures for key usage in place. [17]

DLT solutions within a financial institution are also likely to require integration with legacy financial systems running on several different platforms, such as mainframes, web servers, database servers and, more recently, web services or RESTful microservices [19].

The issues involved in integrating legacy systems are ongoing for financial institutions. For example, an institution can have a mainframe application that requires a screen-scraping service to provide an automated interface to data, while also ensuring that decades of business rules are applied to the raw data as it is entered into or extracted from the system.

Most of the integration problems to be overcome relate to DLT infrastructure, security models and the complexity of allowing smart contracts to accept off-chain data sources. Addressing these issues requires a unified security architecture that ties both legacy username and password systems to directory systems and the Public Key Infrastructure (PKI) specific to DLTs.

It is essential that the most secure component (i.e., the tamper-resistant PKI hardware infrastructure) is not compromised by poor security implementation elsewhere, such as unencrypted password databases, unsecured key stores, or open Application Programming Interfaces (APIs).

With respect to physical and environmental security, this is likely to include use of hardware security modules, physical security measures such as CCTVs, physical barriers, traditional key security, and access controls.

## 7 Blockchain and DLT controls

### 7.1 Technical Controls

The existence of a blockchain will not remove the need for technical controls, see Annex B, within the organisation.

Controls such as the ISO/IEC 27001 (Information Security Management System) will continue to apply.

# 8 Security and privacy processes

## 8.1 General

See Table 1 for a comparison of the differences between public and private blockchains.

**Table 1 — Public versus private blockchains**

| | Public blockchain | Private blockchain |
|---|---|---|
| Participation in network | Open | Closed |
| Transactional privacy | Transactions are usually pseudonymized and only directly tied to a public key. Truly anonymous transactions are limited to a few projects | Similar to public blockchains, but privacy can usually be improved by methods more suitable to permissioned blockchains |
| Economic incentive for participation | Built-in | Contractually organized |
| Centralization | Fully decentralized | Varying degree of decentralization |
| Commonly used for paid social networking | Payments, remittances, prediction markets, distributed storage, paid social networking | Asset servicing, foreign exchange (FX), provenance tracking, trade finance, health care, insurance contracts |

## 8.2 Standard advice on organisation security and privacy processes

### 8.2.1 General

This subclause provides advice on risk analysis for private and public blockchains.

### 8.2.2 Standard advice on risk analysis

The risk profile of public and private blockchains varies significantly. As a new technology, blockchain brings with it specific risks not relevant to other IT systems, see Table 2. Not factoring blockchain-specific risks into the technology assessment can easily leave companies open to security breaches.

**Table 2 — Risks and threats to private and public blockchains**

| RISKS | THREAT | MITIGATION |
|---|---|---|
| Strategic | Chosen network<br>Underlying platform | (to be filled in) |
| Consensus mechanism and network management | The potential for inappropriate, unauthorized, or inaccurate transactions to be recorded in the blockchain | Controls |
| Information Security | Account takeover<br>Malicious actor taking over 51 % of network nodes | (to be filled in) |
| Cryptography, key management, and tokenization | Private key theft | Procedures to ensure these keys are managed appropriately.<br>Monitoring attempts to access private keys. |
| Chain permissions management and privacy | Usage by unauthorized parties pose a significant risk both to the integrity and privacy of the blockchain and to the transactions being recorded. | Private blockchains require authentication of participant identities in addition to user access management policies and procedures |

**Table 2** *(continued)*

| RISKS | THREAT | MITIGATION |
|---|---|---|
| Data management and segregation | Management of all aspects of data, including confidentiality, integrity, and the availability of data | Data is managed appropriately |
| Interoperability and integration | Incorrect data from being written onto a blockchain | Comprehensive examination of interoperability and integration.<br>Controls developed for the blockchain change management and testing<br>Checks for completeness and accuracy |
| Scalability and performance | Blockchain will perform under the stresses of a production environment | Assess whether a solution is production capable and if it can be scaled to grow and align with their use case going forward |
| Business continuity and disaster recovery | Reliance on the other participants of the blockchain network to maintain functionality.<br>Technology and operational failures as well as cyberattacks | Produce a plan for addressing business continuity and disaster recovery.<br>Policies and standards |
| Governance, risk, and compliance | Changes to blockchain software, onboarding of new nodes, or other activities | Clear and documented roles, responsibilities, and accountabilities.<br>Reviewing broader regulatory requirements and standards, including both industry-specific and generally applicable rules |

## 8.3 Technical Design Elements

In solutions involving PKI, Business Continuity planning (BCP) involves ensuring the technical integrity of the key generation mechanisms (certificate authorities, hardware security modules), the business processes involved in the secure transportation of the private keys, and the authorisation layer around these mechanisms.

In addition, business recovery plans need to deal with issues such as redundancy and avoiding data loss or service outage without increasing the attack surface area and reducing operational security.

BCP needs to involve internal security teams, with possible validation from external specialists, to ensure that best practices are adhered to during setup, implementation, and testing. [11]

## 8.4 Legal Risk

Having a well-founded, clear, transparent, and enforceable legal basis is a core element of payment, clearing, and settlement arrangements. [5] DLT can increase legal risks if there is ambiguity or lack of certainty about an arrangement's legal basis. Because the application of this technology to payment, clearing and settlement activity is new, the legal underpinning for certain activities is not as well established as that for traditional systems (for example, in terms of identifying the applicable jurisdiction or relevant laws).

Conversely, DLT can be used to help reduce certain legal risks. For example, automating certain terms and conditions of legally binding agreements (such as automating interest payments as outlined in a contractual agreement) can reduce the risk that contract terms are not enforced as specified in the agreement within the agreed time period[4].

# 9 Blockchain based PKI implementations

Permission Type: With respect to the permission type of blockchain, permission-less blockchain and permissioned blockchain are explained here. The permission-less blockchain is sometimes called public blockchain which is implemented for Internet-scale applications such as domain name holder verification. The permissioned blockchain, which is sometimes called private blockchain, is better suited for small-scale use cases with a small number of participants. As such, both, permission-less and permissioned blockchains can be used, depending on the use case and the number of participants. For most applications that implement large-scale PKIs, permission-less (public) blockchains are preferable to improve stability, security, transparency, and end-user acceptance.

Revocation: Revocation certificate support in a PKI is essential. Revocation is the only way to ensure the long-term validity of certificates. Revocation traditionally relied on trusted third parties to manage; the use of blockchains spreads this trust over all entities. Thus, it is positive that revocation information can be practically shared by using blockchain.

Certificate Format: A minimum number of custom extensions provides support for a standard certificate format.

PKI Type: Domain-specific use cases, which are generally decentralized, can benefit from hierarchical PKIs.

Storage Type: Only a minimum amount of data is stored on the blockchain due to costs and performance reasons.

Updatable Key: Long-term applications provide support for updating issuer keys

Privacy: Select Privacy by design and appropriate privacy-enhancing technologies. The requirement for privacy-enhancing technologies depends on the use case. Consider legal requirements regarding privacy if for example PKI links individuals to personally identifiable data.

Incentives: Incentives for participants are necessary to establish a stable infrastructure on custom blockchains,

It is noted that two of the shortcomings identified are a lack of privacy and a lack of evaluation. Also, privacy is essential due to legal requirements involving individuals covered by data protection legislation.

See [8] for further information.

# Annex A
(Informative)

## A.1 informative Use cases

a) A major crypto wallet service launched a new lending product for all users, not just institutions. Its crypto lending service has been rolled out to all users across more than 180 countries.

b) A United States-based cryptocurrency exchange announced that it is embracing traditional forex trading, going live with nine new fiat currency pairs as of March 12, 2020. Users worldwide — notably excluding United States residents — will be able to use the platform to directly trade between euros, U.S. dollars, Canadian dollars, Japanese yen, pound sterling and Swiss francs.

c) A coffee company's mobile app users will soon be given the option to pay for their drinks. They are looking at retail applications.

d) Stylised process flow of a DLT-based payment system is shown in Figure A.1

In the example in Figure A.1, the transaction process involves three broad steps.

1) To initiate a payment, entity A uses cryptographic tools to digitally sign a proposed update to the shared ledger that would transfer funds from its account on the ledger to entity B's account.

2) Upon receiving the transfer request, other nodes authenticate entity A's identity and validate the transaction by checking to make sure that entity A has the necessary cryptographic credentials to make an update to the record in question. Validation would include, among other things, verifying that entity A has sufficient funds to make the payment. Nodes also take part in the consensus process to agree on the payments that are included in the next update to the state of the ledger.

3) After the update has been accepted by the nodes, the properties of the asset are modified such that all future transactions regarding the asset are initiated using the cryptographic credentials of entity B.

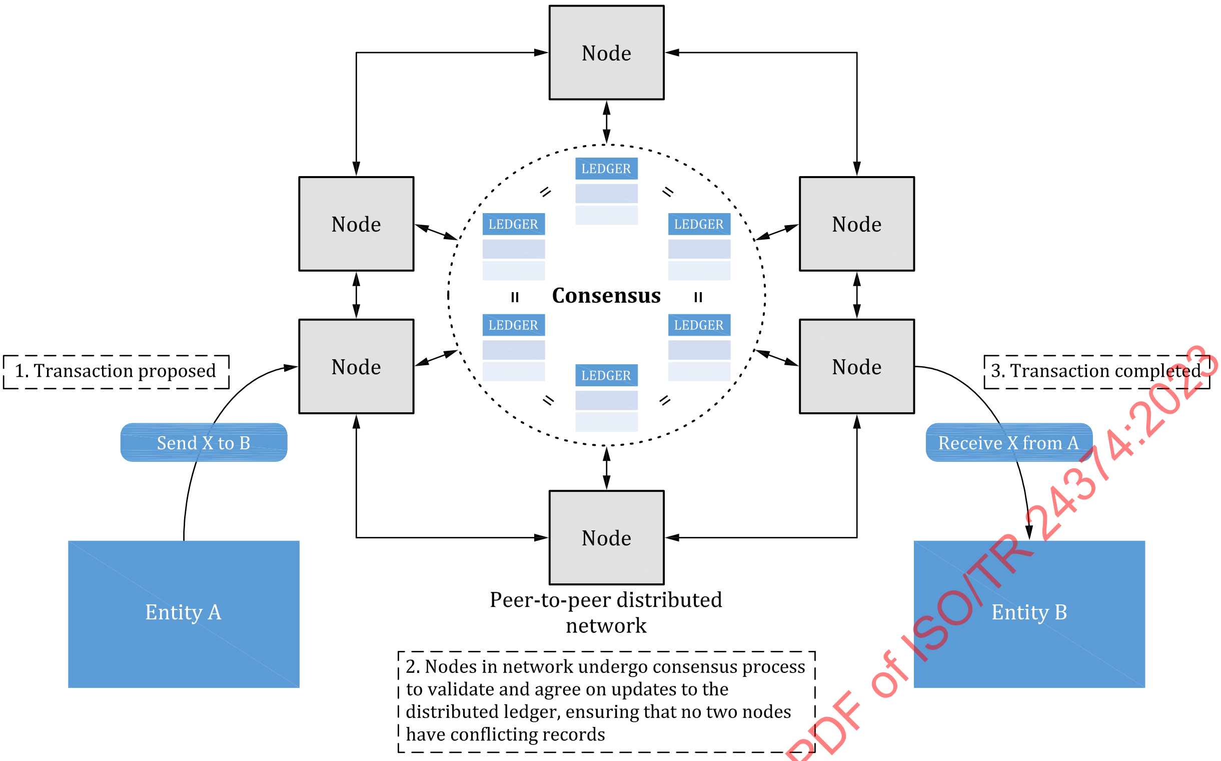
Node
Node
Node
Node
Node
Node
LEDGER
LEDGER
LEDGER
LEDGER
LEDGER
LEDGER
Consensus
1. Transaction proposed
Send X to B
Entity A
3. Transaction completed
Receive X from A
Entity B
Peer-to-peer distributed network
2. Nodes in network undergo consensus process to validate and agree on updates to the distributed ledger, ensuring that no two nodes have conflicting records

**Figure A.1 — - Stylised process flow of a DLT-based payment system**

## A.2 BCP with PKI

In solutions involving PKI, BCP involves ensuring the technical integrity of the key generation mechanisms (certificate authorities, hardware security modules), the business processes involved in the secure transportation of the private keys, and the authorisation layer around these mechanisms.

In addition, business recovery plans need to deal with issues such as redundancy and avoiding data loss or service outage without increasing the attack surface area and reducing operational security.

BCP needs to involve internal security teams, with possible validation from external specialists, to ensure that best practices are adhered to during setup, implementation, and testing.

Blockchain has yet to be tested on a wide scale in a highly regulated environment. Exchanges, banks, and fund managers have all been impacted by cyber-crime and regulators require these financial institutions to ensure both their own cyber protections are fully robust band the cyber-protection measures at their service providers meet appropriate standards.

## A.3 The implementation of Public Key Infrastructure (PKI) and Blockchain.

While the outcome is yet to be determined, it is thought that Blockchain technology benefits from PKI and other identity technologies, rather than replacing them.

Blockchain at its core is a shared ledger, the technology provides a mechanism for multiple participants to agree upon the contents of the ledger, in a decentralized manner. These participants make up what often called as the Blockchain network. Having to use Public Key or "asymmetric" cryptography system with Blockchain requires the private key to be protected to the highest level, which is because if you lose your private key with Bitcoin that essentially means losing your money. With all this information, there's no question that Blockchain stands significance in certain applications. The experiments made by the banking industry are a good example how Blockchain can secure bank transfers. However, because Blockchain is new technology, it has lots of room to develop and improve.

In the Bitcoin Blockchain, the ledger contains transactions involving the exchange of currency, but in the more general case, the contents of the ledger can be almost anything. When it comes to Public Key Infrastructure, it is thought that the basic setup will remain the same. That means that CA will issue and manage certificates needed for the trusted digital identities to implement strong authentication, digital signatures, and data encryption. But instead of running the infrastructure on a computer which requires a lot of maintenance, the CA would be running on the Blockchain instead. It would replace the single computer by a group of connected computers where the ledger content is accessible to anyone and that would make PKI even more trustworthy and vigorous.

There are several advantages on implementing PKI on Blockchain that are beneficial over traditional PKI. These include:

— The certificates are not signed, resulting in them being shorter which would reduce the time it takes to transmit a certificate backed by CA certificate chain.

— Validation of a certificate and its CA certificate chain is critical. But because Blockchain is a “distributed ledger”, the verifier has a local copy of the entire blockchain and can look up the hashes of certificates in the blockchain stores therefore no signatures need to be verified. Note this design approach requires further explanation.

— Lastly, in Blockchain PKI the use of certificate revocation list (CRLs) or responses to online certificate status protocol (OCSP) queries would no longer be required. Blockchain based PKI [6] solves a longstanding problem of traditional PKIs by not requiring the use of a service that issues certificate revocation lists (CRLs) thanks to blockchain synchronization between network’s nodes where any modification to the state of a certificate will be instantaneously notified to all nodes. [11] This is an advantage because these lists can consume a lot of data, resulting in a slower overall process.

## A.4 How Blockchain Addresses Public Key Infrastructure Shortcomings

Traditional PKI has its limitations –including the fact that it works on an outdated design and comes with complexity for any enterprise to manage.[14] Blockchain is emerging as the foundation for the next generation of applications, delivering a modern foundation for businesses so that their PKI performs more effectively.

Application design has changed dramatically since PKI emerged. With cloud and mobility, employees are no longer tied to their desks when they access computer services.

A new foundation is needed to secure such applications because there is no simple, centralized connection from endpoint to server. Blockchain was built to meet today’s business needs. The architecture [3] is based on a distributed database that maintains a continuously growing list of ordered records, called blocks. Since Blockchain runs on tens of thousands of computers simultaneously, its design eliminates the risks found with old school PKI systems.

Blockchain has an open, transparent, secure architecture. Authenticated users on a Blockchain can read all its contents. This feature eliminates the potential problems stemming from relying on a third-party CA’s actions. Companies no longer need to put their trust in CAs that can be duplicitous or error-prone in creating public and private keys. Everything that happens on a Blockchain can be available to anyone using it. So, if a CA issues keys in someone else’s name, that information is seen by everyone on the chain.

Information is time stamped, and a record is created each time an update occurs. Consequently, it is clear who did what when. Altering the transaction record on the ledger becomes impossible. A hacker needs to change every item in the Blockchain rather than just one record. The solution protects information in a secure distributed fashion and is more in tune with current needs than traditional PKI systems.

Solutions running PKI on Blockchain are emerging from vendors. PKI emerged as a viable option when applications were processed on centralized servers. As the industry has moved to distributed processing, the need for a new approach became clear. Blockchain offers a sound foundation to build a distributed security solution, while attention of organizations to the technology has been constantly growing.

## A.5 Example solutions

Existing solutions to the listed problems in 5.2.1 can be grouped in three main classes, as shown in the following.

In the first class, there is a group of solutions based on the creation of one or more servers that operate in parallel to already existing servers (for example, OCSP servers). Their task is to answer questions about the validity of a certificate. They have to be efficient, fast, secure, and simple. In this class falls the so-called log-based PKI schema, where highly available public log servers monitor and publish a log of the certificates issued by the CAs, ensuring that only the certificates listed in the published logs are to be accepted and trusted by end-customers. Proposals have been produced to extend the log also to the revoked certificates, without reaching widely adoptable solutions. This class also includes OCSP solutions that try to support CRLs or other error handling solutions supporting certificate revocation. The idea here is to create a super-CA that coordinates and supports the tasks of the other CAs. However, these solutions suffer from the same fragilities of standard, traditional PKIs because the underlying architecture is essentially the same.

In the second class, there is a group of solutions that come from decentralized networks of peer-to-peer certification, known as the web of trust (WoT). This is where a trust function built on a social network replaces the concept of authority and the classical CA. This trust function can be used to enforce a certificate in its link between a subject and a public key. A user accumulates a certificate containing his public key and digital signatures from entities that have deemed him trustworthy.

In the third class, a DLT is used to build a new implementation for blockchain based management of X.509 certificates that can address the trust management problem while maintaining most of the existing PKI infrastructure.

The solution requires:

- A community of independent peers where everyone checks the certificates;
- The results of the checking phase are shared in the community, by approval;
- The obtained results are kept unchanged and tamper-proof.

With this approach, a precise detection of any misbehaviour of PKI actors can be achieved. Errors can be distinguished from attacks and the previously mentioned attacks can be mitigated.

For more information see [10]