IEEE SA
STANDARDS
ASSOCIATION

IEEE Standard for Application Technical Specification of Blockchain-based E-Commerce Transaction Evidence Collecting

STANDARDS

IEEE Consumer Technology Society

Developed by the
Digital Finance and Economy Standards Committee

IEEE Std 3802™-2022

IEEE

IEEE Standard for Application Technical Specification of Blockchain-based E-Commerce Transaction Evidence Collecting

Developed by the

Digital Finance and Economy Standards Committee
of the
IEEE Consumer Technology Society

Approved 9 February 2022

IEEE SA Standards Board

Abstract: This standard specifies the terminology, technical reference framework, basic functional requirements, and technical indicators for the platform of blockchain-based e-commerce transaction evidence collecting, which is the foundation of digital business interactions.

Keywords: blockchain, evidence collecting, evidence management, IEEE 3802™

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-1-5044-8474-9 STD25262
Print: ISBN 978-1-5044-8475-6 STDPD25262

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[2]

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

---

[1] Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.

[2] Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.[5]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are

---

[3] Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.

[4] Available at: https://standards.ieee.org/standard/index.html.

[5] Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this IEEE standard was completed, the Evidence Collecting Working Group had the following membership:

Xiaofeng Chen, *Chair*
Yi Sun, *Vice Chair*
Baixue Yang, *Secretary*

Organization Represented	*Name of Representative*
0xSenses Corporation	Daozhuang Lin
1stCycle Corporation	Huafeng Lei
Chaincomp Technology Co., Ltd.	Hui Ding
China Academy of Information and Communications Technology	Baixue Yang
China Zheshang Bank Co., Ltd.	Guozheng Yang
HangZhou CChC Digital Technology Co., Ltd.	Yong Jiang
Hangzhou Qulian Technology Co., Ltd.	Xiaofeng Chen
Huochain Technology	Wenqi Zhao
Institute of Computing Technology, Chinese Academy of Sciences	Yi Sun
Institute of Information Engineering, Chinese Academy of Sciences	Jingyuan Hu
Hangzhou Echaincity Technology Co., Ltd.	Keting Yin
Ontology Foundation Co., Ltd.	Ning Hu
PetroChina Planning and Engineering Institute (CPPEI)	Xi Zhang
Shanghai Distributed Technologies Co. Ltd	Le Ju
Sichuan Changhong Electric Co., Ltd.	Bo Tang
State Grid Blockchain Technology (Beijing) Co., Ltd.	Liangliang Zhi
Tencent	Chao Huang
Zhejiang University	Liang Cai

The Evidence Collecting Working Group gratefully acknowledges the contributions of the following participants. Without their assistance and dedication, this standard would not have been completed:

Wei An
Jiajun Chen
Yufeng Chen
Dejun Huang
Xiangjuan Jia
Wei Li
Jie Liu
Zhenjun Ma
Weiwei Qiu
Cheng Zang
Jingzhi Zhang
Shuai Zhang
Peiyu Zheng
Tianchen Wang

The following members of the entity Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

0xSenses Corporation
Beckhoff Automation
Chaincomp Technologies Co., Ltd.
China Academy of Information and Communications Technology (China Academy of TeleCommunication Research, MIIT) CAICT (CATR)
China Jiliang University
China National Electric Apparatus Research Institute Co., Ltd.
China Zheshang Bank Co., Ltd.
HangZhou CChC Digital Technology Co., Ltd.
Hangzhou echaincity technology Co., Ltd.
Hangzhou Qulian Technology Co., Ltd.
Huochain Technology
Institute of Computing Technology, Chinese Academy of Sciences
Institute of information Engineering, Chinese Academy of Sciences
Ontology Foundation, Ltd.
Shanghai Distributed Technologies Co., Ltd.
Sichuan Changhong Electric Co., Ltd.
State Grid Corporation of China (SGCC)
Tencent
Zhejiang University

When the IEEE SA Standards Board approved this standard on 8 February 2022, it had the following membership:

David J. Law, *Chair*
Vacant Position, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy
Ted Burse
Ramy Ahmed Fathy
J. Travis Griffith
Guido R. Hiertz
Yousef Kimiagar
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick
Johnny Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Andrew Myles
Damir Novosel
Annette D. Reilly
Robby Robson
Jon Walter Rosdahl
Mark Siira
Dorothy V. Stanley
Lei Wang
F. Keith Waters
Karl Weber
Sha Wei
Philip B. Winston
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 3802-2022, IEEE Standard for Application Technical Specification of Blockchain-based E-Commerce Transaction Evidence Collecting.

There are many fake and shoddy commodities in the processes of e-commerce transactions that result in transaction conflicts and disputes. It is difficult for users to provide effective legal evidence after the fact and the data on the e-commerce platform itself may be tampered with. Through blockchain technology, judicial institutions with regulatory functions are introduced to reduce the risk of tampering with forensic data and make evidence collecting legally effective to provide a basis for resolving commodity trading disputes.

This standard provides references and guidelines for a blockchain-based e-commerce evidence collecting platform, this standard describes the technical reference framework, basic functional requirements, and technical indicators of blockchain-based e-commerce evidence collecting. This standard serves as a guide for blockchain service providers to integrate blockchain into a traditional e-commerce transaction platform in order to develop and design a tamper-proof, full-process traceable blockchain-based e-commerce evidence collecting platform.

Contents

IEEE Standard for Application Technical Specification of Blockchain-based E-Commerce Transaction Evidence Collecting

1. Overview

1.1 Scope

This standard specifies the terminology, technical reference framework, basic functional requirements, and technical indicators for the application of blockchain in e-commerce transaction evidence collecting, which is the foundation of digital business interactions.

1.2 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).[6,7]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

---

[6] The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

[7] The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

IEEE Std 1609.2™-2016, IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages.[8,9]

IEEE Std 3801™, IEEE Standard for Blockchain-based Electronic Contracts.

ITU-T X.1400 (10/2020), Terms and definitions for distributed ledger technology.[10]

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [11]

blockchain-based e-commerce transaction evidence collecting (BETEC): The process of putting the identity, information, assets, and behaviors in the process of e-commerce transactions on-chain as electronic evidence when disputes arise.

cleanability: The condition where the software, hardware, and network environment are safe and controllable and there is no contextual data pollution, network hijacking, virus injection, or other risks.

evidence collector: The user(s) who use the blockchain evidence collecting service to collect evidence.

evidence: Electronic data evidence information is stored in a safe and stable database so that it can be called up when needed. At the same time, it also uses a specific technology to record this process through data to prove the status of the electronic data at a specific time to prove that the electronic data has not been tampered with after storage.

hash: The "fingerprint" of the data, the output of the data through the hash algorithm. Through the hash algorithm, an input of any length can be calculated into a fixed-length output, and the output is unique and irreversible in the engineering sense.

on-chain: When the business-related direction initiates a request to the blockchain system and the blockchain node writes the relevant data into the blockchain system.

Practical Byzantine Fault Tolerance (PBFT): A distributed system consensus algorithm that can tolerate byzantine errors.

private key signature: The private key provided by the user is matched with the public key stored in the system. After matching, the private key is used to sign the transaction data and the corresponding public key is used by the system to verify the signature.

process witness: One who collects evidence of the user's operation process. Technically, it refers to providing remote desktops of virtual machines for users to use and record the user's operation process.

signature: See IEEE Std 1609.2™-2016.[12]

webpage witness: See ITU-T X.1400 (October 2020).

---

[8] The IEEE standards or products referred to in this annex are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

[9] IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://standards.ieee.org/).

[10] ITU-T publications are available from the International Telecommunications Union (https://www.itu.int/).

[11] *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

[12] Information on references can be found in Clause 2.

3.2 Acronyms and abbreviations

BETEC	blockchain-based e-commerce transaction evidence collecting
GUI	graphical user interface
ID	identification
PBFT	Practical Byzantine Fault Tolerance

4. Technical reference framework

The platform uses blockchain to effectively store evidence and help reduce evidence repudiation. Platform use cases are provided in Annex A. The technical reference framework of a blockchain-based e-commerce transaction evidence collecting (BETEC) platform is shown in Figure 1.

NOTE—Basic DLT Reference Framework of BEC reference from ITU-T F.751.2 (08/2020) [B1][13,14]

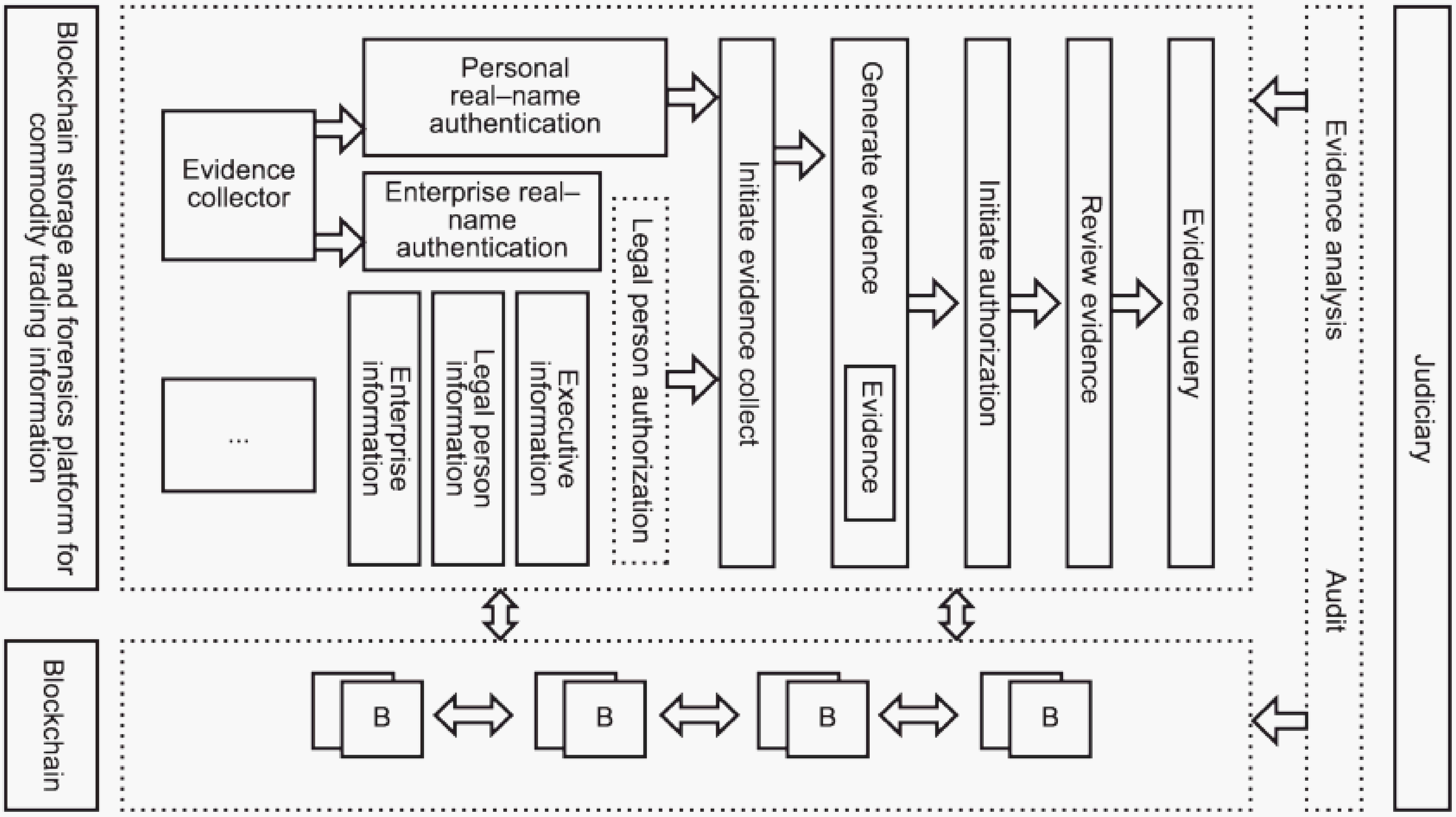

Figure 1—Technical reference framework of the BETEC platform

The specific process design is as follows: The evidence collector first conducts personal real-name authentication and enterprise real-name authentication, initiates an access certificate on the platform, generates evidence, and then initiates authorization. The evidence can be viewed and queried on the platform. Similarly, the enterprise information, legal person information, and information on agents participating in the access card are successfully uploaded to the chain after authorization. The evidence certification process is to hash and secure and credibly collect such documents such as PDF, Word, graphics, audio files, etc., through the blockchain to achieve data confirmation. The evidence collecting process is to obtain real-time evidence and solidification of information such as webpages, clients, chat records, etc., through web page collecting, screen

---

[13] The numbers in brackets correspond to those of the bibliography in Annex B.
[14] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

recording, and video evidence collecting. The platform supports evidence management and judicial services as well as the authorization, query, verification, and download of the evidence.

5. Functional requirements

5.1 Blockchain management

5.1.1 Data management

The BETEC platform shall support block data management, block information display, and transaction information display.

5.1.2 Blockchain node management

The BETEC platform shall support blockchain node management. The functions of blockchain node management include the following:

- Support platform managers to add new blockchain nodes
- Support platform managers to delete blockchain nodes

5.1.3 Blockchain operation monitoring

The BETEC platform shall support blockchain operation status monitoring. The functions of blockchain operation management include the following:

- Display the running status of each node of the blockchain, including real-time running status of the node and usage of the server resources.
- Display block height and block transaction information, so that users can intuitively see block information and transaction information through the graphical user interface (GUI).

5.2 User identity management

5.2.1 Registration

The BETEC platform shall support the user identity registration and the registration record shall be stored on blockchain. The functions of user identity registration include the following:

- Support evidence collector identity registration.
- Provide a review mechanism to verify the integrity and legality of the identity registration after the evidence collector submits an identity registration application.
- Support on-chain for all information in the identity registration process. On-chain shall be signed with a user's private key and the user will be notified with the block number where the information is stored.
- Support the evidence collector to query blockchain identity information.

5.2.2 Authentication

The BETEC platform shall support the registered evidence collector to conduct identity authentication, the results of which can be stored on blockchain. The functions of identity authentication include the following:

- Support real-name authentication of individual users by validating their identification (ID) information.

- Support real-name authentication of enterprises by validating their unified social security codes, business licenses, and other identity information.
- Support automatic examination for authentication information's integrity and correctness and confirm the file format of uploaded attachments along with the authentication. Users shall be notified with the examination result.
- Notify the evidence collector about identity authentication by means of in-site letter or email.
- Support on-chain authentication results and notify users of the block number where the information is stored.
- Support the evidence collector to query identity authentication results stored on blockchain.

5.2.3 Private key issuance

The BETEC platform shall support the private key's issuance by an authenticated evidence collector. The functions of private key issuance include the following:

- Support blockchain private key issuance by an authenticated evidence collector.
- Support the user in downloading blockchain private keys after download permission verification to help improve that the download is performed by the forensic person itself.
- Reliable encryption measures shall be applied to help improve the security of private key transmission during private key download.

5.2.4 Digital signature

The BETEC platform shall support an authenticated evidence collector with a downloaded private key to upload a private key. The uploaded private key shall match the public key saved on the platform. After a successful match, the system signs the transaction with the private key and the system uses the corresponding public key to verify the signature and on-chain after validation.

5.2.5 Authentication information modification

The BETEC platform shall support an authenticated evidence collector to modify authentication information. The functions of authentication information modification include the following:

- Any modification by the evidence collector shall be reviewed.
- Modify the authentication information of the evidence collector.
- Support the user in uploading supporting documents in the process, and the upload module shall support common file storage formats.
- Notify users about their authentication results by means of in-site letter or email.
- Support on-chain of change application records, uploaded certification documents, and review results, and notify users about transaction information and the block number where this storage is located.
- Display modification application records uploaded, supporting documents, and the review results on the blockchain.

5.3 Smart phone techniques

5.3.1 Audio

The BETEC platform shall support adding new evidence collecting in the form of audio evidence collecting. The functions of audio evidence collecting include the following:

- Support the evidence collector in recording and collecting evidence through mobile terminal applications to form relevant evidence.
- Support audio evidence collecting information on-chain through the private key signature and feedback the transaction information and the block on which they are stored to the user.
- Support users in querying the corresponding information on the blockchain.

5.3.2 Video

The BETEC platform shall support adding new evidence collecting in the form of video evidence collecting. The functions of video evidence collecting include the following:

- Support the evidence collector in recording video evidence collected through mobile terminal applications to form relevant evidence.
- Support audio evidence collecting on-chain through the private key signature and feedback the transaction information and the block where the storage is located to the user.
- Support users in querying the corresponding information on the blockchain.

5.3.3 Photo

The BETEC platform shall support adding new evidence collecting in the form of photo evidence. The functions of photo evidence collecting include the following:

- Support the evidence collector in taking photos and collecting evidence through mobile terminal applications to form relevant evidence.
- Support photo evidence collecting information on-chain through the private key signature and feedback the transaction information and the block where the storage is located to the user.
- Support users in querying the corresponding information on the blockchain.

5.3.4 Recording screen

The BETEC platform shall support adding new evidence collecting in the form of recording screen evidence collecting. The functions of recording screen evidence collecting include the following:

- Support the evidence collector in using the recording screen to collect relevent evidence through mobile terminal applications.
- Support recording screen evidence collecting information on-chain through the private key signature and feedback the transaction information and the block which stored to the user.
- Support users in querying the corresponding information on the blockchain.

5.4 Computer techniques

5.4.1 Webpage

The BETEC platform shall support adding new evidence collecting in the form of webpage evidence collecting. The functions of webpage evidence collecting include the following:

- Support for the evidence collector to capture webpage information through webpage scraping tools and to request webpage evidence collecting to generate relevant evidence, including evidence packages and screenshot files.
- Support for evidence collecting information of the webpage on-chain through the private key signature and feedback the transaction information and block where the storage is located to the user.
- Support users in querying the corresponding information on the blockchain.

5.4.2 Process

The BETEC platform shall support adding new evidence collecting in the form of process evidence collecting. The functions of process evidence collecting include the following:

- Support for the evidence collector to connect to the virtual machine remotely and perform related operations through the virtual machine desktop. The BETEC application shall record the screen of the entire process and is required to generate screen recording documents and other relevant evidence.
- Support for the process of evidence collecting information on-chain through the private key signature and feedback the transaction information and the block which stored to the user.
- Support users to query the corresponding information on the blockchain.

5.4.3 Automatic sample

The BETEC platform shall support adding new evidence collecting in the form of automatic sample evidence collecting. The functions of automatic evidence collecting include the following:

- Supports the evidence collector in submitting related purchase sample requests after the system executes an automated procedure to automatically purchase the target goods. The purchase process is recorded and forms relevant evidence.
- Support on-chain automatic sample evidence collecting information through the private key signature and feedback the transaction information and block of the storage to the user.
- Support users in querying the corresponding information on the blockchain.

5.5 Blockchain-based evidence management

5.5.1 Query

BETEC platform collecting shall support evidence query. The functions of query include the following:

- Support for users to query evidence previously stored on the blockchain.
- The contents shall include, but are not limited to, the amount of user evidence stored, the time of evidence storage, the contents of evidence storage, and the record of evidence collection.

5.5.2 Verification

The BETEC platform shall support evidence verification to verify the authenticity of the evidence. The functions of verification include the following:

- Support the evidence collector in using the certificate hash to verify, check whether the evidence is consistent with the data on the blockchain, and inform the evidence collector whether the evidence is true.
- Support the evidence collector in using evidence files to verify and check whether the evidence is consistent with the data on the blockchain by comparing the original text and inform the evidence collector whether the evidence files are true.

5.5.3 Authorization

The BETEC platform shall support the authorization of user evidence to others to facilitate others to view it.

5.5.4 Demonstration

The BETEC platform shall support evidence demonstration. The functions of evidence demonstration include the following:

- Support to locally download the original evidence stored in the blockchain for demonstration.
- During the downloading of evidence, a reliable encryption method shall be provided to help improve the security of evidence transmission.

5.5.5 Audit

The BETEC platform shall support regulatory auditing, and the regulatory and judicial departments can access various information stored on the blockchain within their scope of authority, including evidence information, evidence collection records, etc.

5.6 System maintenance

5.6.1 User management

The users of the platform shall be managed uniformly. The functions of user management include the following:

- Support the creation, modification, deletion, and query of personnel information.
- Support the on-chain creation, modification, and deletion of personnel information records.

5.6.2 Authority management

Authority management refers to controlling the access of system function users to ensure the normal use of valid users and to prevent illegal users and unauthorized users from using system functions and accessing user data. The functions of authority management include the following:

- Supporting the addition, modification, deletion, and query of evidence collector authority.
- Support setting the access and operation permissions for different evidence collectors.

6. Technical indicators

6.1 Ledger data

The requirements that the ledger data of the BETEC platform shall reference IEEE Std 3801.[15]

6.2 Consensus mechanism

The requirements that the consensus mechanism of the BETEC platform shall reference IEEE Std 3801.

6.3 Cryptology system

The requirements that the cryptology system of the BETEC platform shall reference IEEE Std 3801.

6.4 Smart contract

The requirements that the smart contract of the BETEC platform shall reference IEEE Std 3801.

6.5 Communications network

The requirements that the communications network of the BETEC platform shall reference IEEE Std 3801.

6.6 Integrity

The BETEC platform shall include the functions of evidence collection and evidence management of commodity information and provide on-chain support and blockchain data query support for the data of each evidence collecting process as well as detailed functional support.

6.7 Security

The BETEC platform shall provide a security mechanism covering storage and transmission of commodity information data to help improve the privacy and security of user data. Privacy data, sensitive data, and confidentiality data in the system shall be strictly encrypted.

6.8 Availability

The BETEC platform shall have complete functionality, scientific process, easy operation, etc.

6.9 Effectiveness

The BETEC platform shall be effective to help ensure that the evidence collecting information obtained is accurate, effective, complete, and not distorted.

6.10 Scalability

The BETEC platform shall have easy scalability, including easy expansion of functional modules and the underlying blockchain platform.

---

[15] Information on references can be found in Clause 2.

6.11 Cleanliness

The BETEC platform shall have a clean environment with a safe, stable network connection and no contextual influence for each evidence collecting.

Annex A

(informative)

Application scenario

A.1 Copyright protection

Blockchain is used to pre-register and deposit information of goods such as copyrights involved in e-commerce platforms in advance to provide copyright protection for merchants. After a dispute occurs, the cause shall be determined, and the dispute shall be resolved by checking the deposited evidence.

A.2 Evidence of infringement

Merchants use blockchain forensic tools to forensically examine the goods involved in infringement in the e-commerce platform and use this evidence as the main evidence of infringement to apply for rights protection.

Buyers use blockchain evidence collecting tools to obtain relevant evidence on disputes arising during the purchase process and use this evidence as the main evidence of merchants' infringements to apply for rights protection.

A.3 Market supervision/supervision reporting

For a series of illegal behaviors by merchants on the e-commerce platform, such as illegal prices, sale of prohibited items, false propaganda, etc., evidence collection is carried out through the blockchain evidence collecting tools. The collected evidence serves as the evidence basis for market supervision and public reporting, and targeted management and punishment are carried out based on relevant inherent evidence.

Annex B

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] ITU-T F.751.2 (08/2020), Reference framework for distributed ledger technologies.

RAISING THE WORLD'S STANDARDS

Connect with us on:

Twitter: twitter.com/ieeesa

Facebook: facebook.com/ieeesa

LinkedIn: linkedin.com/groups/1791118

Beyond Standards blog: beyondstandards.ieee.org

YouTube: youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060