



IEEE Standard for a Framework for Use of Distributed Ledger Technology in Security of Electronic Voting (e-Voting) Systems

IEEE Industrial Electronics Society

Developed by the
Industrial Electronics Society Standards Committee

IEEE Std 2418.11™-2023

IEEE Standard for a Framework for Use of Distributed Ledger Technology in Security of Electronic Voting (e-Voting) Systems

Developed by the

Industrial Electronics Society Standards Committee
of the
IEEE Industrial Electronics Society

Approved 8 November 2023

IEEE SA Standards Board

Abstract: e-Voting is an application of modern Web 3 and distributed ledger technology (DLT) for more choices and security in registration and voting. Choices range from voting with anonymous paper ballots and postal mail, to online voting where an electronic ballot can be authenticated that it was received and recorded as intended. For security, DLT-enabled systems: validate sources with cryptographic methods, secure communications with digital signatures, and confirm valid transaction with a transparent ledger. Suspicious transactions are recorded as part of a private real-time audit and database, and e-Voting can be tailored for the local needs and methods of a country or administrative sub-division.

Keywords: adjudicate, administration, anonymous, application, archival, area, audit, authenticated, ballot, blockchain, certification, chain of custody, choices, classify, clear, code, communications, compliance, confirm, council, cryptocurrency, cryptography, database, digital signature, digital wallet, directed acyclic graph, distributed ledger technology, e-Voting, efficient, electronic, error, flexible, framework, fraud, fungible token, genesis, hash, IEEE 2418.11™, level, location, methods, mint, modern, non-fungible token, on-site, online, optional, paper, performance, pillars, polling, postal mail, private key, provenance, pseudo-anonymous, public address, public key, quantum, quick response code, real-time, receive, record, registered ballot, registered voter, registration, registration area, scalable, security, send, settle, source, storage, sub-divisions, supervisor of elections, suspicious, sustainable, system, tailored, timeline, token, transaction, transparent, unique, validate, validation node, verify, voter identification card, voting, Web 3

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

Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 7 February 2024. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 979-8-8557-0423-5 STD26711
Print: ISBN 979-8-8557-0424-2 STDPD26711

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

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 IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. 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. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s).

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 subcommittees of the IEEE SA Board of Governors 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 & 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.

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>.

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, neither IEEE nor its licensors waive any rights in copyright to the documents.

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.

³ Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴ Available at: <https://standards.ieee.org/standard/index.html>.

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 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.

⁵ Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

Participants

At the time this standard was completed, the Electronic Voting Systems Working Group had the following membership:

John Wnuk, *Chair*
Saif Aldeen Saad Obayes Al-Kadhim, *Vice Chair*

Allen C. Chen
Jinguang Han

Lakshya Nahar
Vicente Alonso Navarro Valencia

Victor K. Huang
Weili Liu

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

Saif Aldeen Saad Obayes Al-
Kadhim
Boon Chong Ang
Steven Bezner
Cheng-Jen Chen
Xiaofeng Chen
Diego Chiozzi
Abhinav Chopra
Jie Guan
Marco Hernandez

Werner Hoelzl
Victor K. Huang
Piotr Karocki
Weili Liu
M. Sabarimalai Manikandan
Rajesh Murthy
Vicente Alonso Navarro
Valencia
Mfanasibili Nkonyane
Howard Penrose

R. K. Rannow
Cole Scott
Diana Shi
Inga Urbina
Alexandru Vulpe
Stephen Webb
Karl Weber
John Wnuk
Yu Yuan
Bingsheng Zhang

When the IEEE SA Standards Board approved this standard on 8 November 2023, it had the following membership:

David J. Law, *Chair*
Ted Burse, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Sara R. Biyabani
Doug Edwards
Ramy Ahmed Fathy
Guido R. Hiertz
Yousef Kimiagar
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick

Joseph S. Levy
Howard Li
Johnny Daozhuang Lin
Gui Lin
Xiaohui Liu
Kevin W. Lu
Daleep C. Mohla
Andrew Myles

Paul Nikolich
Annette D. Reilly
Robby Robson
Lei Wang
F. Keith Waters
Karl Weber
Philip B. Winston
Don Wright

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2418.11-2023, IEEE Standard for Framework for Use of Distributed Ledger Technology in Security of Electronic Voting (e-Voting) Systems.

In the 1970s, ARPAnet evolved to the Internet. With the Internet came “email” with an easy-to-use “To:name@server.com.” (For context, that was Web 1.). Decades In the 1990s, “client/server” and “https” technologies enabled “web browsing” and secure applications such as online banking (i.e., Web 2).

Decades later in the 2010s, cryptocurrency and blockchain-based distributed ledger technology (DLT) with miners (or validator nodes) enhanced security for financial transactions by

- a) Validating sources with cryptographic methods
- b) Securing communications with digital signatures
- c) Confirming valid transactions with a transparent ledger

This was the beginning of Web 3.

One of the first Web 3 applications was genesis or creation of a cryptocurrency. Cryptocurrencies can be referred to as “crypto” or “coins” and are fungible tokens (FTs). That means an FT can be interchanged with a peer FT. Transfer of cryptocurrencies between peer digital wallets is performed with a secure electronic transaction that is recorded on a blockchain. Those digital wallets have public addresses that can be represented by scannable quick response (QR) codes.

Minting is another type of Web 3 application. Typically, a smart contract is used to “mint” a non-fungible token (NFT). An NFT is a one-of-a-kind creation such as art or unique tangible asset such as a deed or copyright. An NFT is not fungible. That means an NFT cannot be interchanged, replaced, or swapped with another NFT that may be similar. However, for more security, NFT ownership and transfer of ownership can be recorded on a DLT.

Coins and tokens are part of the world of Web 3. Coins are the cryptocurrency FTs for financial applications. Tokens are the NFTs in non-financial applications. NFTs may also have financial value as determined by their owner or minter. Web 3 non-financial applications may be labeled as Web 3A, 3B, and so on, where Web 3V may be the label for security in a non-financial voting application.

e-Voting is an application of DLT for improved security in registrations and voting. Voters may have the choice to vote online or on-site at a polling location, or with the traditional paper ballot and postal mail. Voters may also have the choice to authenticate that their ballot was received and recorded as intended. e-Voting includes a real-time audit for early detection and resolution of suspicious activity, and a database to summarize results of a local, regional, or national voting event.

The four pillars of e-Voting are registration, voting, audit, and database. Security results from those pillars are interconnected by a DLT, digital wallets, QR codes, and validation nodes. That interconnection can result in validation of sources or provenance, a record of the chain of custody of registration and ballot materials—from genesis (i.e., FT creation, or NFT minting) to clearing (i.e., recording on a DLT) to settlement (i.e., confirmation as valid or suspicious with adjudication).

As part of that security, two important terms in this standard are “Supervisor of Elections” and “registration area.” A Supervisor of Elections would be responsible for coordinating all activities in one or more registrations areas. That may include production or acquisition of registration and voting materials, equipment, and facilities; voter education about candidates, propositions, process, and schedules; and services and assistance for challenged voters.

A registration area can be a precinct, ward, neighborhood, quadrant in the US or similar administrative subdivision in other countries (with elections) with common candidates and propositions that appear on a voting ballot. An example of e-Voting follows for a DLT-enabled registration area with responsibilities of a Supervisor of Elections. Registration and voting transactions include genesis, mint, send, mail, authentication, and adjudication. Records for a voting event are included in the DLT, audit, and database.

Registration:

- The Supervisor of Elections is responsible for the genesis of Voter Identification Card (ID card) FTs, each with unique registered card ID, for potential voters in a registration area (RgA).
- If ID cards are appropriate for the RgA and using registration data, the Supervisor of Elections is responsible for the minting of a unique ID card NFT for each registered voter.
- If appropriate and depending on voter choices at registration, the Supervisor of Elections is responsible for sending or postal mailing a unique ID card NFT to each registered voter.

Voting:

- The Supervisor of Elections is responsible for the genesis of ballot FTs, each with a unique registered ballot ID as a public ID or in a private part of an optional secure QR code, for registered voters in a RgA.
- Depending on voter choices at registration, the Supervisor of Elections is responsible for sending an electronic ballot or postal mailing a paper ballot to each registered voter.
- The voter mints a unique ballot NFT by marking their voting choices on that ballot.
- The voter sends or postal mails their marked ballot NFT to a RgA return address.
- Depending on choices at registration, the voter can authenticate that their marked ballot was received and recorded as intended.

Audit and database:

- a) The DLT, audit, and database are updated for each registration and ballot transaction from creation and valid sources (i.e., provenance) to settlement and vote counts (i.e., chain of custody).
- b) Depending on sources and methods, each transaction can be classified as valid or suspicious.
- c) Valid transactions can be recorded in the transparent and public part of the DLT, audit, and database.
- d) Valid data is not available to the public until after a voting event is completed.
- e) Suspicious transactions can be recorded in the private part of the DLT, audit, and database, and is not available to the public.
- f) Suspicious transactions can be adjudicated and confirmed as unintentional errors or intentional fraud.
- g) Confirmed unintentional errors may be repaired if possible, such as adding a registration ID to a registered ballot, and then repeat the registration and/or voting process.
- h) Confirmed intentional fraud can be referred to law enforcement, consistent with all applicable legal requirements.

- i) Status of investigations, adjudication, and law enforcement actions can be recorded as in item c) and item e).
- j) Audit and database process can include registration of voters, ID cards, ballots, and certification that products and services comply with the e-Voting standard.

Contents

1. Overview	13
1.1 Scope	13
1.2 Purpose	13
1.3 Word usage	14
1.4 Registrations and voting	14
2. Normative references	17
3. Definitions, acronyms, and abbreviations	17
3.1 Definitions	17
3.2 Acronyms and abbreviations	18
4. Registration methods	19
4.1 Preferred voting method	20
4.2 Preferred voting type	20
5. Timelines for registration	21
6. Electronic voting	21
6.1 Anonymous	21
6.2 Authenticated	22
7. Timelines for electronic voting	23
8. Postal mail voting	23
8.1 Anonymous	23
8.2 Authenticated	24
9. Timelines for postal mail voting	25
10. Scalability and sizing estimates	25
11. Technology applications and assistance	26
11.1 Distributed ledger technology	26
11.2 Digital wallet, QR codes, and tokens	27
11.3 Electronic systems	27
11.4 Real-time audits	27
11.5 Special suspicious conditions	28
11.6 Voter assistance	28
11.7 Phase-in and education	28
11.8 Optional private QR data	28
11.9 DLT template and features	29
Annex A (normative) Registration	30
A.1 First step	30
A.2 Voter identification card	31
A.3 Tokens	32
A.4 Creation and validation of ID cards	33
Annex B (normative) Ballots	34
B.1 Creation and validation of ballots	34

B.2 Online or on-site electronic ballots	34
B.3 Postal mail paper ballots	34
Annex C (normative) Voting.....	35
C.1 e-Voting concept.....	35
C.2 e-Voting applications and websites.....	38
C.3 Authenticating ballots	39
C.4 On-site voting at polling location.....	39
C.5 e-Voting equipment	40
Annex D (normative) Audits	41
D.1 Objective.....	41
D.2 Maps	41
D.3 Census data	41
D.4 New audits for e-Voting	42
D.5 Public e-Voting audit data	42
D.6 Private e-Voting audit data	43
Annex E (normative) Databases	45
E.1 Public database of valid ballots.....	45
E.2 Private database of suspicious activity	45
E.3 Database structure	46
E.4 Database and address capacity	47
E.5 Digital wallet public address formats.....	47
E.6 Optional secure QR codes on ballot.....	48
E.7 DLT in operation.....	49
E.8 Registration area data	50
Annex F (normative) Digital signature.....	52
Annex G (normative) Open system interconnection	54
Annex H (normative) Digital wallet application	55
Annex I (normative) Paper ballot phase-in.....	59
Annex J (normative) Quantum security.....	62
Annex K (informative) Bibliography	63

IEEE Standard for a Framework for Use of Distributed Ledger Technology in Security of Electronic Voting (e-Voting) Systems

1. Overview

1.1 Scope

The standard specifies the process and requirements for the framework of e-Voting systems. The process includes the following:

- a) Distributed ledger technology (DLT) to enhance security of registrations and voting with electronic or paper ballots
- b) Real-time audits to detect and resolve suspicious activity
- c) A database to summarize validated and suspicious results

1.2 Purpose

The purpose of the standard is to provide procedures and protocols for DLT-enabled registrations and voting that can help secure the voting process. Secure voting is more than a signature on a voting log or voting envelope. It includes the following:

- a) A registration process that verifies authorized voters
- b) Registered voters who can authenticate that their marked ballot was received and recorded as intended without malicious changes
- c) A real-time audit that can detect suspicious activity
- d) Suspicious voting activity is recorded and investigated, but is not counted with valid votes

1.3 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*).

1.4 Registrations and voting

The objective of e-Voting is to apply modern technology to registrations and voting, so that it is easy to use and as popular as IEEE 802.11™ technology [B4].⁸ The intent is reduction of controversial results in voting and elections by assuring that every counted vote was from a registered ballot and registered voter.

A voting event can be for a local, regional, or national election. The voting event shall include Registration Areas (RgAs), where each area has the same candidates, propositions, or other voting topics or matters. An RgA can be one or more precinct(s), ward(s) and the like in the United States (US), or similar areas in other countries.

Each RgA enabled with DLT shall have general attributes including: X potential voters, y valid registrations, z suspicious registrations, x of X that do not register or vote, or Z more that register or vote than the X potential voters.

As appropriate, an RgA shall have common and registered unmarked Voter Identification Card (ID card) fungible tokens (FTs) and unmarked ballot FTs. When unique voter data is added to an ID card, that card shall become a one-of-a-kind non-fungible token (NFT). When a ballot is marked with unique voter choices, that ballot shall become a one-of-a-kind NFT.

The Supervisor of Elections for an RgA shall a) determine options for voting by electronic or postal mail methods, and b) define the templates for the unmarked ID card FTs and unmarked ballot FTs. Unless otherwise specified, there shall be (X + Z) unmarked ID card FTs and unmarked ballot FTs for an RgA's voting event.

For postal mail voting, there shall be a Supervisor of Elections that represents postal offices in the RgA.

Real-time audits for an RgA shall be able to classify registration and voting activity as valid or suspicious. Suspicious activity shall be adjudicated as a) unintentional error for possible repair and reprocessing, or b) intentional fraud, or c) remain as suspicious in archival storage for continued investigation.

A database for a RgA shall include records of: a) valid ID card and ballot FTs and NFTs, b) suspicious ID card and ballot FTs and NFTs for investigation, c) confirmed registration and voting errors and repair status, d) confirmed registration and voting fraud and status of referrals to law enforcement, and e)

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.

⁸ The numbers in brackets correspond to those of the bibliography in Annex K.

suspicious FTs and NFTs that cannot be adjudicated and remain in archival storage for continued investigation.

The following includes more on blockchain and DLT, validating sources, securing communications, confirming transactions, and transparent ledgers.

1.4.1 Blockchain and DLT

A blockchain is a DLT, but a DLT includes more than blockchains. Another type of DLT is based in directed acyclic graph (DAG) technology. In the beginning, blockchain was the only type of cryptocurrency DLT. More recently, DAG has become popular as a more efficient DLT than blockchain.

A DLT records transactions between peer digital wallets. In e-Voting, Supervisor of Elections and voters shall have digital wallets for storage and processing of electronic FTs and NFTs, and folders for storage of paper FTs and NFTs. More on blockchain and DLT is in Clause 11 (see also Digital Wallet [B10], Blockchain [B11], and DAG [B17]).

1.4.2 Validating sources

ID cards and ballots can be electronic or paper. Validating a source (i.e., provenance) depends on the type of transaction such as genesis, mint, send, mail, or authenticate. An invalid source is one of several reasons why a transaction can be classified as suspicious.

Genesis shall be the creation of FTs from an identifiable source (i.e., software code or printer) with output that goes to a receive FT wallet or folder. A suspicious transaction shall be an electronic or paper ID card or ballot with an invalid source or invalid or missing voter registration ID or registered ballot ID.

Mint shall be the creation of a new electronic or paper NFT from an electronic or paper FT with output that goes to a receive NFT wallet or folder, respectively. A suspicious transaction shall be an electronic or paper ID card or ballot that has an invalid FT source.

Send shall be an electronic FT or NFT transaction from a send wallet to a receive wallet. A suspicious transaction shall be a send wallet that has an invalid FT or NFT source.

Mail shall be a paper FT or NFT transaction from a mailing postal mail address to a receiving postal mail address. A suspicious transaction shall be a mailing address that has an invalid FT or NFT source.

Authenticate shall be an indirect method to determine if the original marked ballot from a voter was received and recorded as intended. When a marked electronic or paper ballot is received at an RgA the following shall occur:

- a) A copy shall be made in electronic form
- b) A digital representation shall be made in comma separated value (CSV) or other format
- c) A cryptographic “hash” shall be made of the digital representation
- d) When authentication is requested, a hash of the received and recorded ballot shall be returned to the voter as receipts

Based on processing of the hash receipts, the e-Voting application shall classify the ballot as authenticated or suspicious as shown in Annex H. Authenticated ballots shall be counted, and recorded in the public audit and database. Otherwise, suspicious ballots shall be handled as follows:

- Suspicious ballots shall not be counted.
- Suspicious ballots shall be recorded in the private audit and database.
- Suspicious ballots shall cause an alert to the Supervisor of Elections to investigate the source of suspicion.

1.4.3 Securing communications

Secure communications shall be used for electronic and postal mail transactions. For electronic transactions, digital signatures shall provide a first level of security, with more details in Annex F. Another level of security for electronic transactions shall be provided with Transport Layer Security (TLS) and Advanced Encryption Standard (AES) as described in Annex G and Annex J.

For postal mail (and paper ballot) transactions, secure communications shall be provided with cryptographic hash receipts. More details are in Clause 8, Clause 9, and Annex I.

1.4.4 Confirming transactions

Transactions shall be confirmed with a clearing and settlement process. A transaction shall be cleared when the following occurs:

- The send and receive wallets are peered
- They have valid formats and addresses
- The transaction is entered to a DLT for settlement

A transaction shall be settled when there is consensus by the validator nodes that the transaction is valid, the data or value in the send wallet has been withdrawn, and the withdrawn data or value has been deposited in the receive wallet.

1.4.5 Transparent ledgers

A ledger shall be transparent when a DLT explorer can access and display transaction details given a send or receive digital wallet public address, a Transaction ID (TxID), or a Postal Mail Transaction ID (MxID).

TxID, with symbol “-->” in a graphical representation, shall be an electronic “send” transaction identification number for a transaction between two peered digital wallets. The Supervisor for Elections shall be responsible for payment of any TxID fees, with funds that come from election assistance or equivalent.

MxID, with symbol “==>” in a graphical representation, shall be a postal “mail” transaction identification number for a transaction between valid postal addresses. Coding may be similar to “Informed Delivery,” or a TxID for electronic communications. The Supervisor of Elections representing postal offices in the RgA shall be responsible for payment of any MxID fees with funds that come from election assistance or election mail or equivalent.

Each DLT transaction record should include several items, not necessarily limited to the following:

- a) TxID or MxID
- b) Sending digital wallet public address or postal mail address

- c) Receiving digital wallet public address or postal mail address
- d) Message or data
- e) Voting method (i.e., online, on-site, or postal mail)
- f) Voting type (i.e., anonymous or authenticated)—Anonymous transactions shall not reveal a voter's identity or postal mail address

2. Normative references

Normative references are referenced documents that 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).

Currently there are no normative references in this standard. Sources referenced in this document are listed in Annex K.

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.⁹

Curve25519: With a 32-byte secret key, Curve25519 computes a 32-byte public key. With a 32-byte secret key and a 32-byte public key from another user, Curve25519 computes a 32-byte secret key shared by the two users to enable encryption and decryption of a digital signature.

e-Voting: An application of Web 3 technology for security in registrations and voting.

ECDH with p384: Elliptic curve specified in NSA Suite B Cryptography. *See also:* **Elliptic Curve Diffie-Hellman (ECDH).**

Ed25519: Digital signing with EdDSA encryption and Curve25519 elliptic curve.

elliptic curve: Plot points on a graph defined by equation $y^2 = x^3 + a \times x + b$.

Elliptic Curve Diffie-Hellman (ECDH): Scheme for two parties to derive a shared secret.

ephemeral keys: Symmetric key generation by sender and receiver without transfer of a public key.

genesis: The origin or source of something of value. Creation of fungible tokens.

Keccak-256: A family of hash functions.

⁹*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.

mining: Cryptocurrency service that verifies transactions and creates value by solving a mathematics challenge.

mint: Creation of fungible fiat coins or a non-fungible token.

private key: A cryptographic key, used for key exchange, decryption, and/or signature generation, that has a corresponding *public key* such that the private key cannot feasibly be derived from the public key using public information.

public key: A cryptographic key, used for key exchange, encryption, and/or signature verification, that has a corresponding *private key* such that the private key cannot feasibly be derived from the public key using public information.

qubit: A basic unit of information in a quantum computer vs. a bit as a basic unit of information in a conventional digital computer.

registration area (RgA): Can be a precinct or ward, or other area as defined by the Supervisor of Elections with the same candidates, propositions, or other voting topics or matters.

secp256k1: Elliptic curve parameters associated with Koblitz curve $y^2 = x^3 + a \times x + b$.

SHA-256: Secure Hash Algorithm 256. Cryptographic hash that generates a 256-bit (32 byte) signature for a message of arbitrary length.

SHA-384: Secure Hash Algorithm 384 has the same encryption as SHA-512, with output truncated to 384 bits (48 bytes).

SHA-512: Secure Hash Algorithm 512 generates a 512-bit (64 byte) signature for arbitrary length message.

sustainable: The ability to endure a variety of controllable and uncontrollable conditions.

validation node: Receives transactions from clients, can charge transaction fees, and can settle a transaction. *Syn:* **consensus node**.

Web 3V: Web 3 technology applied to a non-financial voting application.

Winternitz: Algorithm with speed and storage tradeoffs to meet security objectives in digital signatures.

x.y.z: shard.realm.account: Digital wallet public address format where x, y, and z are numbers.

x.y.z-abcde: Digital wallet public address checksum abcde that is computed using the DLT ID and x.y.z address.

3.2 Acronyms and abbreviations

A-PKC	Asynchronous Public Key Cryptography
ABFT	asynchronous byzantine fault tolerance
AC	account code
AES	Advanced Encryption Standard
CITY	City District
CON	Congressional District
CSV	comma separated values
DAG	directed acyclic graph

DLT	distributed ledger technology
DOR	date of record
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-curve Digital Signature Algorithm
EKC	Ephemeral Key Cryptography
EPS	encapsulated postscript
FT	fungible token
HD Wallet	Hierarchical Deterministic Wallet
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol (non-secure)
HTTPS	HTTP Secure
ID	identification
IP	Internet Protocol or Intellectual Property
ISP	Internet Service Provider
JP	Justice of Peace Precinct
LEG	Legislative District
MAC	Media Access Control
NFT	non-fungible token
OSI	Open Systems Interconnection
PDF	Portable Document Format
PKC	Public Key Cryptography
PRC	Precinct
QR	quick response
RgA	registration area
S-EKC	Synchronous Ephemeral Key Cryptography
S-PKC	Synchronous Public Key Cryptography
SHA-3	Secure Hash Algorithm 3
SHA-256	Secure Hash Algorithm 256
SHA-384	Secure Hash Algorithm 384
SHA-512	Secure Hash Algorithm 512
SSL	Secure Socket Layer
SUP	County Supervisors District
TCP	Transmission Control Protocol
TLS	Transport Layer Security
tps	transactions per second
UDP	User Datagram Protocol, Unreliable Datagram Protocol
WebP	Web Picture
x.y.z	shard.realm.account
x.y.z-abcde	shard.realm.account-checksum

4. Registration methods

Registration shall be the collection of data from potential voters and if appropriate for the registration area (RgA) for the production of valid ID cards for qualified voters. An ID card shall be an unmarked FT, or NFT that is marked with unique voter registration data. The back of each ID card NFT shall include a prefix and address as defined in Annex A.