

IEEE Guide for Blockchain in Power and Energy Systems

IEEE Power and Energy Society

Developed by the
Smart Buildings, Loads, and Customer Systems
Committee

IEEE Std 2418.5™-2025

STANDARDS

IEEE Guide for Blockchain in Power and Energy Systems

Developed by the

Smart Buildings, Loads, and Customer Systems Committee
of the
IEEE Power and Energy Society

Approved 19 June 2025

IEEE SA Standards Board

Abstract: Blockchain/distributed ledger technology, referred to as blockchain/DLT, is a proven technology in industry and, though newer to applications in the energy industry, is well-positioned to become a critical component of this evolving electrical system. blockchain/DLT can provide transparency and traceability within energy markets and distributed system operations, reduce error and processing inefficiencies between the multiple parties engaged in interconnected grid management, and offer a path to automation of the grid through the use of smart contracts. This guide provides an open, common, and interoperable reference framework model for distributed ledger technology (DLT) such as blockchain in the energy sector. This guide also serves as a guideline for blockchain/DLT use cases in the electrical power industry, creating a guide for a reference architecture framework, including interoperability, terminology, functionality, and system interfaces.

Keywords: blockchain, distributed ledger technology, DLT, electric power system, energy markets, energy system management, IEEE 2418.5™, smart contracts

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

Copyright © 2025 by The Institute of Electrical and Electronics Engineers, Inc. All rights reserved.
Published 15 December 2025. 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 979-8-8557-2615-2 STD28254
Print: ISBN 979-8-8557-2616-9 STDPD28254

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 IEEE 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 involved in technical working groups 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 all standards, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or compliance with law, or guarantee against interference with or from other devices or networks. 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 their 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 balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English language version published by IEEE is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. “Artificial intelligence” refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual is not, and 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, or be relied upon as, a formal position of IEEE or IEEE SA. 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). News releases about IEEE standards issued by entities other than IEEE SA should be considered the view of the entity issuing the release rather than the formal position of IEEE or IEEE SA.

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 revisions to an IEEE standard is welcome to join the relevant IEEE SA 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

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

² Available at: <https://standards.ieee.org/about/contact/>.

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, 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

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

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

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 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

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. 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, data privacy, 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 IEEE guide was completed, the Energy Blockchain Working Group had the following membership:

Claudio Lima, *Chair*
Unit Cali, *Vice Chair*
Johnny Lin, *Secretary*
Shawn Chandler, *Chair TF Interoperability*
Sri Nikhil Gupta Gourisetti, *CoChair TF Cybersecurity*
Tamara Hughes, *Co-Chair TF Smart Contracts*
Jonathan Sebastian David Sebastian-Cardenas, *CoChair TF Smart Contracts*
Annabelle Lee, *Co-Chair TF Cybersecurity*
Puica Nitu, *Chair TF Industry Use Cases*

Kalaiarasan A.
Mohamed Aathil
Kashif Abbas
Farihal Abedin
Shivani Abrol
Hannes Agabus
Ayushi Agarwal
Praveen Kumar Agarwal
Sarveakash Aggarwal
Saad Ahmed
Felix Akpagloh
Maher Al-Badri
Aslaha Ali
Mohammed Ali
Mahdieh Aliaslkhiani
Sarah Almajid
Carlos Frederico
Meschini Almeida
Abdullah Alobaidi
Merlinda Andoni
Manuel Andrade
Amjad Anvari-
Moghaddam
Madalina Arhip
Alejandro Arias
Aru Arunasalam
Miguel Aybar
Krishna Sandeep
Ayyagari
Koti Reddy B.
Sruthi S. B.
Parupkar Singh
Badhesha
Linquan Bai
Thushankgi
Balachandran
Saifullah Baloch
Sayanta Banerjee
Dinesh Baradi
Mike Barker
Alan Bartos
Alan Bax

Abhisek Bedant
Mike Bennett
Sameh Betamony
Rohit Bhakar
Milan Biswal
Sara Biyabani
Ayodele Boglo
Peter Boglo
Hanumantha Rao
Bokkisam
Mehrdad Boroushaki
Anastasia Boutzious
Ebou
M. Boye Muniraj C.
Tommaso Caldognetto
Kevin Cameron
Taylor Cardin
Gerry Cauley
César Andrés Cazal
Mongkon Chaiongsin
Bo Chen
Haoyong Chen
Xiaofeng Chen
Xinzhi Chen
Long Cheng
Ravi Sankar
Chittavarjula
Abhinav Chopra
James Clark
Christopher Conley
Cletus John Crasta
Jonah Crespo
Marcio Ribeiro da Cruz
Curtis Cryer
Luis Ernesto Cárdenas
Shitikantha Dash
Nimalanjana Piyumal
Dassanayake
Stuti S. Datta
Vincent David
Carlos Delgado
Surekha Deshmukh

Jael Diana
Hui Ding
Michael Dixon
Shashwat Dwivedi
Oliver Dzobo
Miriam Eduful
Murray Eitzmann
Shyamali Ekanayaka
Elizabeth Escobar
Liz Escobar
Jay Fallah
Zhenyu Fan
Amro Farid
Fernando Figliolo
Constantin Filote
Jonathan Fleming
Fernando Flores
Victor Francisco
Monsoon Fu
Rao Fu
Shubhanker Garg
Michael Geocariss
Soham Ghosh
Sreekesh Giri
Satya Prasad R. K. D.
Gollakota
Ajith Gopi
Anna Gorbacheva
Chris Gorog
Saibal Gosh
Gerald Gray
Cihan Guldorum
Swapnil Gupta
Yaren İlayda Gürkan
Santoshkumar
Hampannavar
Ahteshamul Haque
David Hardin
V. S. K. V. Harish
Naveed Ul Hassan
Barry Hayes
Paul Heitmann

Lin Herenčić
Dayna Herling
Rafael Hernandez-Millan
Christopher Hicks
Amer Hijazi
Xuwei Huang
Yuping Huang
Philip Huff
Stefan Häselbarth
Naveed Ihsanullah
Faiz Ikramulla
Ahzan Musnath Ilahi
Vassileios Iliadis
Kateryna Isirova
Onwuzuruike Jessica
Xiangjuan Jia
Kevin Joshi
Ananthanarayanan K.
Uwe Kaltenborn
Yi Kang
James Kempf
Komal Khan
Prince Waqas Khan
Chul Kim
Zan Kiparizoski
Stanley C. Koski
Akshaya Krishna
Amit Kumar
Anil Kumar
Arun Kumar
Bipul Kumar
Murat Kuzlu
Haobo Lai
Kent Lambert
Faouzi Laouej
Andres Laso
Fernando Lezama
Canbing Li
Kang Li
Canbing Li
Xiangming Li
Jason Lin
Jason Lin
Weijia Liu
Anthony Locker
Tony Locker
Andres Lopez
Timothy Lu
Doug Lucas
Zhihan Lv
Cheng Lyu
Zheng Ma
Anand Madhavan
Carlos Maestre
Rupeekshan
Maheswaran
Nitika Mahiya
Rasel Mahmud

Abhilash Manjunath
Luis Gabriel Marin
Tony Markel
Ryan May
Padraic McFreen
Raveendra Reddy
Medam
Raveena Meena
Manan Mehta
Cristian Melendez
Fernando Cardoso Melo
Fernando Melo
Ron Melton
Johannes Menzel
Girish Babu Meruva
Nancy Min
Amir Miragha
Sambeet Mishra
Moein Moeini-Aghtaie
Ahmed Mohamed
Fazel Mohammadi
Pooria Mohammadi
Manish Mohanpurkar
Sushree Shataroopa
Mohapatra
Hamed Mohseni
Juan Molina-Castro
Marissa Morales
Matthew Moroney
David Mueller
Aaditya Muley
Leslie Munanura
Ali Nabavi
Neha Nandagaoli
Vicente Navarro
Bogdan Neagu
Steven Nelson
Kanchit Ngamsanroaj
Young Ngo
Tran Huynh Ngoc
Mahsa Nicknam
Nawaz Nimmagallu
Brian Noel
Mike Nolte
Anggoro Yudho
Nuswantoro
Brian O'Regan
Yasuhiko Ogushi
Pattharaphon Ongmee
Charles Onyango
James Orenstein
Eduardo Ortiz-Rivera
Sivaraman P.
John Packwood
Pavan Padghan
Yash Pal
Nikitha petcy Panditi
Marco Pasetti
Bansi Patel

Chris Peoples
Daniel Perez
Saeed Peyghami
Scott Placide
Radu Porumb
Masoud Pourali
Soheil Pouraltafi-Kheljan
Akshara V. Prabhath
Shalini Prasad
Rizwana Nazar R.
Maria Raboaca
E. Thirshal Ragav
Farrokh Rahimi
Ashkan Rahimi-Kian
Gerber Ramos
Md Juel Rana
Kumudhini Ravindra
Ali Razban
Ramesh Reddi
Amal Reji
Kathy Render
Kenneth Reyes
Carol Rivas
Shayan Rizvi
Laurence Robitaille
Luiz Henrique Leite
Rosa
Simon Round
Crystle Ryland
Biju S. S.
Rohan Damodar S.
Sreelakshmi B. S.
Shammya Saha
Lou Sahlou
Asvika Saibalaji
Syed Mostasim Hasnain
Saif
Rajashekhar Sammeta
Hugo Sanchez-Reategui
Kumari Sandhya
Yuanrui Sang
Abubakar Sadiq Sani
Ray Schilling
Kai Schmied
Jonathan Sebastian
David Sebastian-Cardenas
Kwami Senam Sedzro
Moin Shaikh
Xingyu Shang
Abhishek Sharma
Divya Sharma
Priyansha Sharma
Mohamed Shihab
Shahab Shokrzadeh
Prasad Shrawane
Sandeep Shukla
Stuti Shukladatt

Iony de Siqueira
P. Sanjana Kavindi
Siriwardhana
Glenn Skutt
Joao Soares
Tirupati Solanke
Bhawana Solanki
Clayton Stice
Aravinth Subramaniam
Cahyo Subroto
Pruthiraj Swain
Elroy Switlshoff
Pradeep T.
Jinrui Tang
Adhinarayanan
Theerthamalai
Andreas Theocharis
Kaung Thu
Patiphan Thupphae
Leonard Tillaman
Shubham Tiwari

Marie Torres
Sawa Toshiyuki
Mohamed Toub
Ahsan Upal
Luis Valdivia
Jaber Valinejad
Harsh Vardhan
Salvin Antony Varghese
Eduardo Vega-Fuentes
Ioannis Vlachos
Yash Vyas
Qiushi Wang
Xiaonan Wang
Preethy V. Warriier
Jianguo Wei
Fushuan Wen
Joshua Wepman
Gabby Whitman
Robert Wilson
Sam Wynn
Hao Xiao

Tao Xu
Nobuyuki Yamaguchi
Shixing Yan
Chao Yang
Wentao Yang
Xiaofeng Yang
Xiaochun Yi
Jiang Yu
Jiangshan Yu
Yunjun Yu
Vahraz Zamani
Jiangfeng Zhang
Qianchuan Zhao
Yue Zhou
Zou Zhou
Mengmeng Emily
Zhuang
Weiwei Zhuang
Danish Zia
Muhammad Fahad Zia
Guy Zito

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

P. K. Agarwal
Boon Chong Ang
Sara Biyabani
Koti Reddy Butukuri
Umit Cali
Shawn Chandler
Haoyong Chen
Xiaofeng Chen
Xinzhi Chen
Zhiman Chen
Sharmeela Chenniappan
Diego Chiozzi
Kurniawan Diharja
Donald Dunn
Shubhanker Garg
Sri Nikhil Gupta

Gourisetti
Brook Hagen
David Hardin
Werner Hoelzl
Xuwei Huang
Uwe Kaltenborn
Piotr Karocki
Haobo Lai
Annabelle Lee
Claudio Lima
Daozhuang Lin
Weili Liu
Greg Luri
Vicente Alonso Navarro
Valencia

Tran Ngoc
James Orenstein
Sivaraman P.
Marco Pasetti
Bansi Patel
Howard Penrose
Radu Porumb
Simon Round
Daniel Sabin
David Sebastian
Cardenas
Jhony Sembiring
James Simko
Wayne Stec
Kaung Thu
Janusz Zalewski

When the IEEE SA Standards Board approved this guide on 19 June 2025, it had the following membership:

Lei Wang, *Chair*
John Walter Rosdahl, *Vice Chair*
David J. Law, *Past Chair*
Alpesh Shah, *Secretary*

Edward Au
Ted Burse
Xiaofeng (Alfred) Chen
Doug Edwards
Nehad El-Sherif
J. Travis Griffith
Deborah R. Hagar

Guido R. Hiertz
Ronald W. Hotchkiss
Tyler L. Jaynes
Thomas Koshy
Howard Li
Xiaohui Liu
Kevin W. Lu
Hiroshi Mano

Daleep C. Mohla
Annette D. Reilly
Robby Robson
Daniel Sabin
F. Keith Waters
Sha Wei
Luyang (Eric) Zhang

Introduction

This introduction is not part of IEEE Std 2418.5-2025, IEEE Guide for Blockchain in Power and Energy Systems.

This guide provides an open, common, and interoperable reference framework model for blockchain applications in the energy sector.

This guide provides the following:

- Serves as a guideline for blockchain use cases in the electrical power industry, renewable energy industry, and their related services;
- Create subsequent standards on reference architecture, interoperability, terminology, and system interfaces for blockchain applications in the energy sector by building an open protocol and technology agnostic layered framework; and
- Evaluate and provide guidelines on scalability, performance, security, and interoperability through evaluation of consensus algorithms, smart contracts, and types of blockchain implementation, etc., for the energy sector.

This standard provides a unifying framework to the processes, functionalities, and use cases of a changing power grid supported by innovative, high-impact blockchain applications.

Clause 1 provides an overview, positioning blockchain and distributed ledger technology (DLT) as a key enabler of the evolving electrical system, enhancing transparency, efficiency, and decentralized energy transactions. The grid is evolving toward a more decentralized network, or a network of networks with dynamic energy as a service and internet of things, all supported by DLT blockchain technology. As the grid of the future will have new operational flexibilities, the blockchain applications should provide flexible and secure solutions.

Clause 5 describes the smart contracts as self-executing agreements with terms written in code, typically running on blockchains to automate transactions without intermediaries. This should ensure transparency, efficiency, and trust. Legal considerations are considered as well as cybersecurity risks and mitigating best practices.

Clause 6 presents key principles in the blockchain/DLT technology and its related cybersecurity applications. The multiple layers should protect against potential cyber threats. These layers are the “application layer” supporting applications built on the blockchain; “execution and consensus layers” that manage consensus and transaction validation; the underlying “data, network, and infrastructure layers” that govern data modeling and transmission across the network; and the “physical layer” with hardware and physical devices throughout the network.

Clause 7 presents the blockchain and DLT interoperability, examining the IT/OT functional segmentation to describe how different blockchain networks communicate and exchange data through cross-chain transactions, scalability, and standardization.

Clause 8 presents real-world use cases of blockchain/DLT technology in energy markets, focusing on managing real-time data, operational flexibility, and digital assets such as carbon credits and renewable energy certificates. This clause presents each use case in a standardized format to include challenges, stakeholders, actors, agents, interoperability and inter-blockchain communications, transaction types, domains, cybersecurity, privacy, standards, regulations, and gaps. This approach outlines the functional requirements and key interfaces between blockchain/DLT networks and transactive energy agents to facilitate secure peer-to-peer (P2P) trading, enhance market transparency, ensure data integrity, and enable seamless transactions between energy producers, consumers, and grid operators.

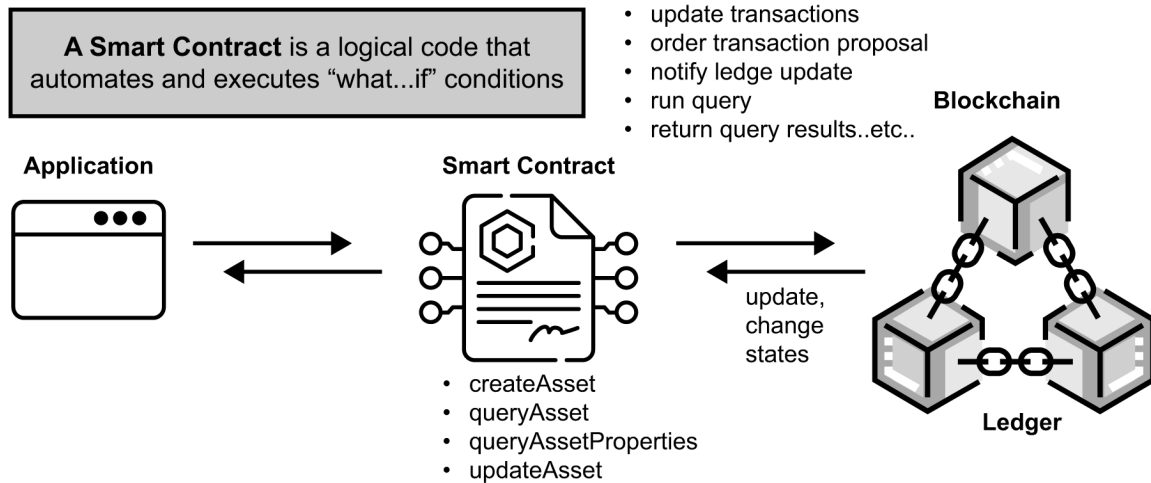


Figure 1—Framework for IEEE 2418.5 Blockchain Energy Standard

Contents

1. Overview	15
1.1 General	15
1.2 Scope	16
1.3 Word usage	17
2. Normative references	17
3. Definitions, acronyms, and abbreviations	17
3.1 Definitions	17
3.2 Acronyms and abbreviations	19
4. Common categories of blockchain/DLT	19
4.1 General	19
4.2 Consensus mechanisms	23
5. Smart contracts	26
5.1 General	26
5.2 Taxonomy	27
5.3 Legal aspects of smart contracts	28
5.4 Smart legal energy contract framework	29
6. Blockchain/DLT and cybersecurity	31
6.1 General	31
6.2 Secure design and development	32
6.3 Privacy	33
6.4 Blockchain/DLT cybersecurity	35
6.5 Blockchain/DLT engineering and cybersecurity stack	36
6.6 Cybersecurity mapping to P2418.5 DLT stack	38
6.7 Cryptographic key management and performance impacts	40
6.8 Smart contract cybersecurity and privacy	40
7. Blockchain/DLT interoperability	41
7.1 Blockchain/DLT interoperability framework	41
7.2 Segmentation and interoperability	43
8. Blockchain/DLT in the electric power Industry	52
8.1 Industry benefits	52
8.2 Blockchain/DLT energy application overview	55
8.3 Use case applications	59
8.4 Blockchain/DLT challenges	81
8.5 Regulation, policy, and standards of blockchain/DLT in the electric power industry	82
Annex A (informative) Bibliography	84

List of Figures

Figure 1—Framework for IEEE 2418.5 Blockchain Energy Standard.....	11
Figure 2—Smart contract.....	27
Figure 3—Reference blockchain/DLT implementation attributes.....	28
Figure 4—Various smart contracts and pertinent objects for transactive energy markets.....	30
Figure 5—Smart legal energy contracts	30
Figure 6—Cybersecurity and energy components pertaining to blockchain/DLT in power and energy use-cases	32
Figure 7—Blockchain/DLT engineering and cybersecurity stack: Layer definitions with examples	36
Figure 8—Blockchain/DLT stack layer with cybersecurity attributes.....	39
Figure 9—Blockchain/DLT interoperability framework.....	44
Figure 10—Blockchain/DLT-CIL interoperability framework example	45
Figure 11—Blockchain/DLT semantic interfaces and technology domains.....	46
Figure 12—Grid segmentation examples with blockchain/DLT types.....	48
Figure 13—Industry domain interoperability mapped to syntactic interface types	49
Figure 14—DLT engineering and cybersecurity stack mapping with the OSI model and TCP/IP model.....	50
Figure 15—Transformation of GridWise to SGAM interoperability layers	51
Figure 16—Blockchain/DLT stack mapping with SGAM.....	52
Figure 17—General applications of blockchain/DLT.....	56

List of Tables

Table 1—Evolution of the electric power system	16
Table 2—Key differences and features comparison between permissionless and permissioned blockchain/DLT.....	20
Table 3—Blockchain/DLT use case applications	57
Table 4—Use case application key features	57
Table 5—Wholesale energy markets	60
Table 6—Local and regional energy markets	62
Table 7—Retail electricity markets	64
Table 8—Energy trading platform.....	65
Table 9—Tokenization of energy and ancillary products	67
Table 10—Flexibility services in the short term	70
Table 11—Flexibility services in the long term	72
Table 12—Electric vehicle (EV) mobility charging	73
Table 13—Recording energy data for billing and other purposes	75
Table 14—Substation and operations digitalization	77
Table 15—Energy traceability and certificates	78
Table 16—Funding and revenue allocation/remuneration.....	80

IEEE Guide for Blockchain in Power and Energy Systems

1. Overview

1.1 General

The electric power industry is a foundation of modern society and is comprised of all entities participating in the production, management, and sale of electricity. Modern operation of the grid, services, and markets involves bi-directional sharing of information between many grid participants and stakeholders. Driven by innovation in many adjacent industries, the electrical system is evolving toward a distributed architecture with emerging requirements to support increased deployments of renewable resources, electrification of transportation, two-way power flows, resilient islanding systems and as a result, a new generation of integrated systems to maintain the safety, security, reliability, and operational excellence that is expected by customers, aggregators, system operators, regulators, and third-party stakeholders. distributed ledger technology, referred to as blockchain/DLT, is a proven technology in the financial industry and, though newer to applications in the energy industry, is well-positioned to become a critical component of this evolving electrical system.

Blockchain/DLT can provide transparency and traceability within energy markets and distributed system operations, reduce error and processing inefficiencies between the multiple parties engaged in interconnected grid management, and offer a path to automation of the grid through the use of smart contracts.

[Table 1](#) summarizes the main structural changes expected in the evolution of the electric power industry, along with their respective links to blockchain/DLT.

Table 1—Evolution of the electric power system

Conventional power system	Modern power system	Link to blockchain/DLT
One-way flow of electricity within the bulk electrical system (BES) and distribution grid, from centralized generation to consumers	New services and price formation with multi-path flows of electricity, new grid services, congestion management mechanisms, and grid support from distributed energy resources	Distributed ledger integration with edge computing supports service automation through smart contracts; DLTs are capable of storing distributed energy resource data; DLT may combine operations and economic automation in the same system for third-party market aggregation of distributed energy resources (DERs) in parallel with utility aggregation
Grid operation is accomplished primarily by utility-owned resources and services, including centralized and operator-led activities	Grid operation is supported by increased DERs and behind-the-meter (BtM) resources requiring distributed system transparency, security, and access control	Distributed ledger offering activity transparency, trust of assets and data, data privacy, and immutability of transactions
Retail transactions between utilities and consumers that are managed in a centralized manner	Procurement mechanisms with complex transactions and layered attributions of energy generation, load, and services among prosumer grid participants with decentralized and distributed functions, including settlement	Smart contracts for automation, financial transaction settlement functions for DER-related emerging retail markets
Utility management of grid services and resources with wholesale market participation	Multiple parties are involved in grid activity, including operators, markets, consumers, prosumers/DER owners, and energy service suppliers (ESS), requiring information exchanges, service exchanges, financial exchanges, metering, and billing security	Distributed ledger offering activity transparency, trust of assets and data, data privacy, and immutability of transactions

Note that this guide, at its time of writing, may not fully illustrate all tangible benefits of blockchain/DLT in the electric power industry, as most projects worldwide consist of proof-of-concept (PoC), which test various value hypotheses. Expectations and potential benefits of adopting blockchain/DLT in the electric power industry depend on many factors, including the pace of adoption of digital technology and control systems, changing standards for communications system architecture, the rate of adoption of machine learning and automation, evolving business needs, and regulatory constraints.

1.2 Scope

This guide provides an open, common, and interoperable reference framework model for distributed ledger technology (DLT), such as blockchain, in the energy sector.

It also covers the three following aspects:

- 1) Serve as a guideline for blockchain/DLT use cases in the electrical power industry; energy value industry chain, covering the renewable energy industry and their renewable-related sources of generation.
- 2) Create a guide on reference architecture framework, including interoperability, terminology, functionality, and system interfaces for blockchain/DLT applications in the energy sector by building an open protocol and technology agnostic layered framework.
- 3) Evaluate and provide guidelines on scalability, performance, security, and interoperability through evaluation of consensus algorithms, smart contracts, and types of blockchain/DLT implementation for the energy sector.

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*).

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.

There are no normative references in this standard.

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.⁸

append-only ledger: Blockchain/distributed ledger technology (DLT) is a technology that provides a full transactional history. Unlike traditional databases, transactions and values in a blockchain are not overwritten.

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 *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.

block: A data structure used to record transactions, distributed to all nodes in the distributed ledger network. A block's structure follows Merkle tree architecture, which aids verification of block data integrity. A Merkle tree combines the hash values of transaction data together until there is a root hash. The root hash is an efficient means for fingerprinting all transactions in a block, and the hash tree enables detection of inconsistent transactions within a block. To create a block, a user may submit a candidate transaction to the ledger by sending the transaction to other nodes participating in the blockchain. These transactions are then disseminated to more nodes in the network. These distributed transactions then wait in a queue, or transaction pool, until they are added to the blockchain by a mining or validator node; this occurs when the mining or authorizing nodes publish a block. The block contains a set of validated transactions. After it is created, each block is hashed to generate the digest that represents the block.

Blockchain transaction: A record of information kept in a distributed ledger.

chain: A sequence of blocks linked together by block hashes to maintain a specified order, agreed upon through consensus, and maintained independently by every node in the distributed ledger network.

consensus: An agreement among distributed nodes in the blockchain system that 1) a transaction is validated and 2) that the distributed ledger contains a consistent set and ordering of validated transactions.

distributed database: A database that hosts two or more files located in different locations, where portions of the database are stored in multiple physical servers or locations, and processing happens among multiple database nodes in a distributed manner. A distributed ledger is a distributed database. A blockchain/distributed ledger technology (DLT) is a specific type of distributed ledger.

distributed ledger: The extraction and exchange of data is stored in the ledger on the blockchain. All the extraction and exchange data are digitally signed by the private key, and the data extraction and exchange records under this account are recorded in the ledger.

node: A computer participating in a blockchain architecture maintaining an independent copy of the distributed ledger.

oracle: A digital asset that serves as one or more trusted and agreed-upon sources of data or reference. For example, a temperature oracle could establish a consensus among parties as to the referential temperature at a specific time, date, and GIS location to be used in the execution of a smart contract. In addition, oracles may serve as a gateway or orchestrator between the on-chain infrastructure of a distributed ledger technology (DLT) system and external data that may be used in the execution of the smart contracts, depending on the inputs, conditions, and events originated from external real-world and internal virtual ecosystems.

secure: Blockchain/distributed ledger technology (DLT) helps ensure that the data contained within the ledger has not been tampered with and that the data within the ledger is attestable.

smart contract: A smart contract is a self-executing program that enables agents to execute deterministic functions and to operate and agree upon logical states that can be used to verify and enforce system rules. It allows trusted transactions without third parties that are traceable and irreversible. In addition, computer logic that can be stored or processed on a distributed ledger and executed in response to defined conditions or triggers, automating the execution of conditional statements such as terms of a contract, e.g., "what...if...then", using the blockchain/DLT ecosystem. They contain the digital signatures - the private cryptographic keys - of the parties to the contract and have access to the cryptographic primitives required to participate in a consensus process. Smart contracts are intended to be hosted within each peer computational resource and can create digital assets; read or write (add) transactions, order transaction proposals, and query transactions from the ledger. Results of SC execution are recorded on the blockchain/distributed ledger technology (DLT). Note that the term "contract" in its use here does not specify that it is legally binding.

trustability: A technical feature of a blockchain/distributed ledger technology (DLT) with specific supporting attributes:

- Shared: The ledger is shared among multiple participants, providing transparency across node participants in a blockchain/DLT network.
- Distributed: A blockchain is distributed among nodes, allowing for scaling the number of nodes of a blockchain network to make it more resilient to attacks by bad actors. By increasing the number of nodes, the ability for a bad actor to impact the consensus protocol used by the blockchain/DLT is reduced.
- Immutable: Transactions recorded on a blockchain ledger cannot be altered.

validator: A node or nodes that execute block verification and validation by engaging in a consensus process to publish a new block.

3.2 Acronyms and abbreviations

ADMS	advanced distribution management systems
AMI	advanced metering infrastructure
IoT	Internet of Things
OMS	outage management system
PII	personally identifiable information
SCADA	supervisory control and data acquisition
SGAM	smart grid architecture model
SLEC	smart legal energy contract
WAMS	work and asset management system

4. Common categories of blockchain/DLT

4.1 General

There are two basic classes of blockchain: public (permissionless) and private (permissioned). A hybrid blockchain/DLT combines public and private types for the purposes of controlling specific data or administrative functions via permissions. The intent is to control who has access to specific data stored in the blockchain and the data that is publicly available. Finally, a consortium blockchain is a type of permissioned blockchain, similar to a private blockchain. The difference between a consortium blockchain and a private blockchain is subtle; in a consortium, multiple organizations may participate and agree to administrate the same chain, rather than a private blockchain, which is centrally managed by a single organization.

In a public or permissionless blockchain, accessibility is as follows:

- Anyone in the system can participate
- Read/write access is open to all participants through nodes
- All nodes may participate in the consensus process
- Transactions are visible to all participants

In a public blockchain, the blockchain state (the data, all records) and its transactions are transparent and accessible to everyone. Any node joining a public blockchain network can validate transactions. Notably, in a public blockchain, a node may be a source of malicious behavior. To help prevent attacks from malicious nodes, the blockchain network implements a consensus algorithm.

In a permissioned blockchain, including private and consortium types:

- Only participants with permissions can participate
- Read and write access to publish new blocks requires specific permissions
- Transactions are visible to permissioned participants

Consequently, only authorized and trusted entities can participate in the activities within the permissioned blockchain. By allowing only authorized and trusted entities to participate in activities within the blockchain, a private or consortium blockchain helps ensure the privacy of the chain data. Permissioned blockchain networks have the same traceability of digital assets as they pass through the blockchain, as well as the same distributed, resilient, and redundant data storage system as a permissionless blockchain network.

Permissioned blockchain networks may be used by organizations that need to control and protect their blockchain more tightly. Permissioned blockchain networks may also be used by organizations that wish to work together but may not fully trust one another. They can establish a permissioned blockchain network and invite business partners to record their transactions on a shared distributed ledger. These organizations can determine the consensus model to be used, based on how much they trust one another. Notably, users of the permissioned blockchain will need to have trust in the administrative organization. Beyond trust, permissioned blockchain networks provide transparency and insight that may help better inform business decisions and hold misbehaving parties accountable. This can explicitly include auditing and oversight entities, making audits a constant occurrence versus a periodic event.

Some permissioned blockchain networks support the ability to selectively reveal transaction information based on a blockchain network user's identity or credentials. With this feature, some degree of privacy in transactions may be obtained. For example, it could be that the blockchain records that a transaction between two blockchain network users took place, but the actual contents of transactions are only accessible to the involved parties.

Table 2 describes key differences and applications between permissionless or public blockchain/DLT, and permissioned blockchain/DLT.

Table 2—Key differences and features comparison between permissionless and permissioned blockchain/DLT

Permissionless/public	Permissioned/private/consortium
Immutability of the ledger	
Immutability refers to the notion that the content recorded in the ledger cannot be changed or edited due to a hash-based cryptographic linkage. In any blockchain/DLT, this means that any change to previously recorded data is immediately identified by a validator as the cryptographic hash of a previously recorded block would change along with the slightest difference to the content. A ledger can create and read properties, but lacks edit and delete properties.	The immutability aspect of a ledger is maintained in the private/permissioned blockchains. The cryptographic linkage between the blocks of transactions that are recorded in the ledger addresses the integrity security objective. The principle of hash-based cryptographic linkage between the blocks is the same for all blockchains (private, public, hybrid).
Permissionless/public	Permissioned/private/consortium

Table continues

Table 2—Key differences and features comparison between permissionless and permissioned blockchain/DLT (continued)

Permissionless/public	Permissioned/private/consortium
Identity of the participants	
In most cases, there is almost no concept of identity, and the users are anonymous. The node's information (human or a device) is not associated with the transactions or with the data records in the ledger. This may be an undesirable feature in some applications (such as in power and energy applications). Non-repudiation is limited to the individual node addresses, i.e., transactions can be traced to the individual node addresses, but the true entity-based identity (human or device) is unknown.	The philosophy of private blockchains is geared toward solving problems that can use blockchain technology in a restricted multi-organizational facet to facilitate the solution to the entire business network. Therefore, anonymity and transparency are augmented with identity management and permissions. To achieve this, the private blockchain uses a directory of all valid members and their identities pertaining to the network. Some blockchains facilitate access by building upon an organization's or business network's lightweight directory access protocol (LDAP), Active Directory, single-sign-on credentials, and similar technologies. Unlike public blockchain, nonrepudiation can be associated with a particular entity (human or device) in private blockchain architectures since the transaction relationship can be traced to the node (human or device) and not just the node's network address.
Data transparency	
All of the data is expected/assumed to be fully transparent. However, due to the anonymity of the participants, it is extremely difficult (or near impossible) to associate the data record or transaction with an individual/entity. This may be an undesirable feature in some applications (i.e., some power and energy applications).	In most cases, total transparency is replaced with the ability to define access control rules; ultimately, governance policies are placed in the hands of the business network/coalition. The multi-organizational network can collectively define the rules around read- and write-access, as well as transaction initiation access guided by the well-known access control principles such as least privilege and need-to-know to facilitate needed confidentiality and need-based availability. This permits the business network to control who can read what data and who can do what with the data. Access control lists (ACLs) can be used to assign and maintain permissions.
Trust	
Permissionless/public blockchains are designed with the notion of ensuring the secure transaction of digital commodities without the need for reconciliation and trust establishment between transacting entities.	Since enterprise/private blockchain solutions are geared toward applications with well-defined boundaries and business networks, these blockchains are designed to function in a partial or fully trusted environment.
Permissionless/public	Permissioned/private/consortium
High-level functions of a node (decentralization versus quasi-decentralization)	

Table continues

Table 2—Key differences and features comparison between permissionless and permissioned blockchain/DLT (continued)

Permissionless/public	Permissioned/private/consortium
At a high-level, every node in a public blockchain performs three functions: 1) each node is responsible for keeping a copy of the ledger; 2) all nodes would execute any requested smart contract (e.g., if an entity called a function out of a smart contract, that function is executed by all of the nodes in the network); and 3) nodes attempt to keep their copy of the ledger in synchronization with all of the copies of the ledger on the network. The goal is to have the same data in the same order in all of the ledgers on the network. This achieves full decentralization but with the caveat of slow transactional speeds and the lack of centralized control on a node's functions. Public/permissionless blockchains do not control aspects such as who can join the blockchain, who can form consensus, or define the minimum/maximum number of nodes.	Permissioned networks are not fully peer-to-peer given that validator nodes are based on permission/assignment. Permissioned networks retain the needed redundancy, failover, and fault tolerance as a distributed system, and as a result of assigning validation to specific nodes, it increases the scalability factor. Varying types of nodes and administrative roles may be utilized, including but not limited to: 1) Nodes to administrate redundant copies of the ledgers; 2) Nodes to execute smart contracts; 3) Nodes to manage data ordering and ledger synchronization. In a permissioned blockchain/DLT, authority organization(s) can control the number of nodes that would form consensus, conditions and constraints to join the network, and the number of nodes that should be on the blockchain network. In regard to identifying that number, it depends on the nodes that need to transact, and the contractual terms between the organizations that would dictate the number of consensus nodes permitted in a single organization. The key is to have enough consensus-forming nodes to satisfy the network's fault-tolerant parameters.
Consensus mechanisms	
Permissionless ledgers are managed through network consensus. Blockchain nodes attempt to stay in synchronicity with each other using the idea of group consensus. The concept of group consensus is central to the ability of any participating node to participate in the consensus-forming process. Under group consensus, nodes verify if the data was recorded correctly. However, the nodes lack the ability to verify the truth of the data itself.	The concept of a global ledger is replaced with multiple localized ledgers to facilitate need-based availability, with specific consensus nodes assigned. Shards may be fully localized to a business network that can define the security rules and processes in that blockchain/DLT. This concept ties back to the elimination of the group consensus that was described previously. In such a non-global architecture, there may be no one place where all data is stored. In this architecture, an attacker could not obtain all of the data in the network by attacking certain nodes on the network (which addresses a single point of failure).
Permissionless/public	Permissioned/private/consortium
Shared ledger	

Table continues

Table 2—Key differences and features comparison between permissionless and permissioned blockchain/DLT (continued)

Permissionless/public	Permissioned/private/consortium
The ledger is shared with all the nodes, and several redundant copies of the ledger exist on the network (addressing a single point of failure). Therefore, all of the nodes own and maintain a copy of the ledger. The governing rules around the ledger are defined at the overall blockchain network level. This method may have scalability issues for some consensus types. One method to address scalability is referred to as sharding or splitting the workload of transactions in the network into multiple ledgers specific to types of transactions, network locations, or other criteria. Shards may maintain copies of other shards.	The concept of a global ledger is replaced with multiple localized ledgers to facilitate need-based availability, with specific consensus nodes assigned. Shards may be fully localized to a business network that can define the security rules and processes in that blockchain/DLT. This concept ties back to the elimination of the group consensus that was described previously. In such a non-global architecture, there may be no one place where all data is stored. In this architecture, an attacker could not obtain all of the data in the network by attacking certain nodes on the network (which addresses a single point of failure).
Traceability in the ledger	
Cryptocurrency-based blockchains are primarily used to track the history of the cryptocurrency. Recent permissionless blockchain platforms extend that capability to track any feasible digital asset.	Permissioned blockchains have the ability to track any digital asset through the ledger function.

For the electric power industry, entities may utilize the following:

- Private or consortium blockchains are used because of the sensitivity of an application and its data, centralizing control to a single company (private) or a group of organizations (consortium) for a particular business reason.
- Public blockchains where an application and/or data is intended to be public with full transparency.
- Hybrid blockchains, mixing public and private forms to match a business use case application. For private and hybrid type blockchains, entities may require the implementation of identification and authentication security controls for devices and individual participants. Use case applications are presented in [Clause 5](#).

4.2 Consensus mechanisms

Consensus mechanisms are the methods that build trust in a decentralized ledger, such that all the participants in the blockchain/DLT will trust the validity of the system and the data that it contains. It is the method that replaces a centralized authority to verify and validate additions of data and transactions on the blockchain. As data is added to a blockchain, the blockchain version is updated, and nodes accept the updated version through a consensus mechanism. The consensus mechanism confirms the replication of a block record across shared ledgers.

In a distributed ledger system, hashing is a key feature fundamental to consensus as well as other administrative functions of the system. Hashing refers to the digital modification, via an algorithmic, mathematical process, of transforming an input string (i.e., simply the data being recorded into the next block) such that it returns a digital output of a fixed length. Hash functions are designed to be irreversible. Using the same hashing method always produces a hash of the same size, which can be easily compared for the purpose of consensus. Using the same hashing algorithm or function on the same input string always returns the same hash code, no matter how long the input string is, so long as it is the same data.

This feature makes any modification of a blockchain system of record detectable. Finally, using the same hashing method on two different input strings, no matter how small the difference, will always return two different hash codes. This characteristic is what makes blockchain secure, given that any change to any data of any length in any block will change a block's hashed output. In all consensus methods, a computational algorithm is used to compute various hashes. Each block in a distributed ledger stores the hash of the previous block as well as the data being submitted in the current block. Consensus is the process of accepting the same blocks among nodes and at every node participating in the system. This technical feature is what makes distributed ledgers trustworthy, such that information in the distributed ledger may not be altered without changing the hash code of a block. Data in blocks is replicated and distributed throughout all the distributed computing nodes, a technical feature that makes distributed ledgers transparent. Since the process of hashing is repeated for every new block addition to a chain, the blockchain technology makes data stored in the distributed ledger traceable and tamper-evident: a transparent, trustworthy, encrypted record of the data shared by all nodes. This, combined with smart contracts, creates a technical framework to accomplish traceable, trustworthy, transparent automation for the use cases described in [Clause 5](#).

A blockchain/DLT network may be implemented in any computer network, public or private, composed of a set of distributed computing nodes that are connected via a network protocol. A comparison of the network “stack” of web-based applications and blockchain/DLT, and interoperability between systems is provided in [Clause 4](#). A permissioned network uses a host computer to approve new nodes in the network, while a permissionless network permits any node to contribute to the network via a network client. Continuous consensus formation in such a distributed computing framework can be achieved through various methods. Two common consensus types are lottery-based consensus and voting-based consensus.

The following is a summary of the most common lottery-based and voting-based consensus algorithms that are currently in use. This summary is not intended to be an all-inclusive list, particularly as new algorithms are being proposed and developed.

4.2.1 Lottery-based

Lottery-based consensus methods are well-suited for permissionless blockchains. There is no control on the validators, as any node in a permissionless blockchain may be a validator. In a permissioned blockchain, the validators are known and accepted by the network administrator. Each node assigns a probability based on the characteristics of the winner. Lottery reduces the likelihood of an ill-behaved node validating a forged block.

Lottery-based mechanisms are more complex and may be slower than voting-based mechanisms, but can scale well to large dimensions with fewer performance challenges. Good scalability means that a system performs well as it grows in scale. The lottery-based systems may result in multiple chains at different nodes in the network that need to be consolidated and resolved before the chain is concluded, affecting the speed of transactions recorded in the blockchain.

Proof-of-Work (PoW)

PoW consensus requires each network node to validate a bundle of data from the group of current transactions, also called a mempool, competing to add a new block to the blockchain.

Each node randomly solves a cryptographic puzzle (the work is creating a hash) over and over until an output is discovered that sufficiently meets a performance criterion, or level of difficulty, called a “hash target.” The goal for all node participants (frequently called miners) is to achieve a hash output that is lower than a specified hash target. Miners cannot predict nor influence the outcome of a hash algorithm, so the only feasible action is to calculate the hash value over and over through trial and error until success is achieved.

A node is rewarded for correctly solving the puzzle (at the difficulty level of the hash target set in the network, a feature of the specific consensus protocol).