

# Blockchain Standardization in Practice: Contrasting European Union and U.S. Approaches

**Nir Kshetri**, The University of North Carolina at Greensboro

*This article categorizes blockchain standards by their functional focus and by how they are established. It also contrasts the European Union's and the United States' regulatory approaches in blockchain standardization in key areas.*

The 2024 valuation of the global blockchain market at US$31 billion[1] underscores its potential, yet the lack of standardization continues to hinder its broader adoption. For instance, by 2025, the sectoral visibility of blockchain initiatives in Canada, particularly those extending beyond cryptocurrency applications, has experienced a measurable decline in prominence relative to prepandemic levels. Efforts by firms like Walmart Canada and major banks to implement blockchain in payments and supply chains have faced delays, primarily due to challenges in achieving the necessary standardization.[2]

Standards are essential for global interoperability and market flexibility, facilitating seamless cross-blockchain data exchange. However, persistent fragmentation in standardization efforts remains a barrier.[3] The inherent complexity of blockchain and related technologies, spanning diverse technical, regulatory, and operational domains, requires collaboration among diverse stakeholders, complicating both the development of unified standards and the evolution of current standardization ecosystems.[4]

The role of standards in distributed ledger technology (DLT) and blockchain is thus widely acknowledged. However, views vary on specific areas for standardization and implementation timelines.[5]

*Digital Object Identifier 10.1109/MC.2025.3563736*
*Date of current version: 27 June 2025*

EDITOR **NIR KSHETRI**
The University of North Carolina at Greensboro;
nbkshetr@uncg.edu

Blockchain requires standards for various key areas, including interoperability for seamless communication among platforms, governance to manage decentralized projects, identity frameworks for consistent identity protocols, security to protect networks and nodes, and best practices for ensuring the safety of smart contracts. These standards are crucial for creating a robust, secure, and cohesive blockchain ecosystem.[6]

Interoperability is challenging due to variations in technology, standards, and legislation. The absence of a global standard for blockchain-based digital identification leads to interoperability issues, hindering system integration and slowing adoption.[7]

The development of technological standards is shaped by a confluence of technical, commercial, political, and moral imperatives.[8] While market dynamics and regulatory interventions influence their adoption, scholarly analysis underscores the pivotal role of state actors: standards backed by governmental mandates exhibit a higher likelihood of market dominance.[9] Governments, leveraging regulatory authority, strategically steer standardization processes to align with national economic and technological objectives.[10]

Government regulation can play a pivotal role in unifying fragmented blockchain standards. By leveraging their authority, policy makers can drive the development of consistent frameworks that enhance interoperability, close regulatory and technical gaps, and improve data security across blockchain networks. In the absence of such coordination, developers may continue to adopt divergent or incomplete standards, exacerbating fragmentation. A unified regulatory approach, requiring intergovernmental collaboration, clear leadership, and dedicated resources, can promote more secure and interoperable blockchain ecosystems across sectors.[11]

This article examines blockchain standards by their functional focus and by the processes through which they are established. It also compares the regulatory roles in key standardization areas between the European Union (EU) and the United States.

## TAXONOMY OF BLOCKCHAIN STANDARDS: TYPES AND CATEGORIES SHAPING INDUSTRY PRACTICES

Standards exist in various types and categories, each serving distinct purposes in blockchain systems. They ensure consistency, reliability, and interoperability, guiding the design, implementation, and evaluation of blockchain applications across industries. This section categorizes standards based on their functional focus and how they are developed and adopted.

### Types of standards based on their functional focus

Standards can be classified based on their functional focus, what they aim to define, measure, or enable. In the blockchain ecosystem, these include measure or metric standards, process-oriented or prescriptive standards, performance-based standards, and interoperability standards (Table 1). Each type plays a distinct role in promoting consistency, reliability, and compatibility across blockchain systems and applications, supporting the technology's

**TABLE 1.** Types of standards and their applications in blockchain systems.

| Type | Definition and characteristics | Examples/applications in blockchain |
|---|---|---|
| Measure or metric | Reference points used to quantify and compare attributes. These standards enable consistency in measurement and facilitate informed decision making. | Ethereum's "gas" for computational effort in smart contracts, priced in gwei and fluctuating based on network demand. |
| Process oriented | Provide structured procedures and best practices to ensure repeatability and consistency. These are often regulatory or compliance oriented. | Financial Action Task Force standards for virtual assets and virtual asset service providers (for example, anti-money-laundering/countering the financing of terrorism compliance, licensing requirements). |
| Performance tased | Focus on the outcomes rather than specific methods, offering flexibility in how results are achieved. These standards prioritize final objectives like security, control, and privacy. | EU Digital Identity Framework (eIDAS 2) supports blockchain-based IDs for security and cross-border recognition. |
| Interoperability | Ensure systems can communicate and operate together by using common formats, without dictating internal processes or performance levels. These standards promote compatibility across platforms and services. | Chainlink's corporate actions data standardization project in Europe: the use of artificial intelligence and oracles (ChatGPT, Gemini, and Claude) to create structured Golden Records compliant with ISO. |

scalability and integration across industries.

A measure or metric standard is a reference against which comparable quantities are measured. Examples include the kilogram for mass, the meter for length, and the liter for volume. These standards are particularly beneficial for consumers as they facilitate comparison shopping for price, function, or features.[12] Ethereum uses gas to measure the computational effort for executing smart contract operations. Gas costs depend on the complexity and resource usage of the operation. Prices are denominated in gwei (a fraction of Ether) and fluctuate based on network demand.[13]

Process-oriented standards provide structured guidelines for executing tasks in a consistent and reproducible manner.[12] The Financial Action Task Force (FATF) is an intergovernmental body established in 1989 by the G7 to set global standards for combating money laundering. Since 2001, its mandate has expanded to include countering terrorist financing. In 2019, FATF updated its standards on virtual assets (VAs) and virtual asset service providers (VASPs), followed by a comprehensive review in 2020. The FATF standards involve a number of recommendations that provide a comprehensive framework for combating money laundering and terrorist financing in the cryptocurrency sector. For instance, under the amended FATF Recommendation 15, VASPs must be regulated, licensed, or registered and implement anti-money-laundering (AML)/countering the financing of terrorism (CFT) measures similar to traditional financial institutions. VASPs are required to gather and transmit sender and recipient details for transactions exceeding a specified threshold to maintain traceability and regulatory compliance. Countries must regulate and monitor VASPs to enforce AML/CFT measures and ensure compliance with FATF recommendations, mitigating money laundering and terrorism financing risks.[14] This type of standard is process oriented or prescriptive, standardizing activities and methodologies to ensure consistency and repeatability in testing and operations.

Performance-based standards focus on the final outcome rather than the processes involved. They specify the desired end result but leave flexibility in how to achieve it.[12] For instance, blockchain-based digital identities use a variety of performance measures related to security, privacy, and control. The EU Digital Identity Framework is built on three key pillars designed to enhance security, accessibility, and user control. The first pillar strengthens national electronic identification systems under electronic identification, authentication, and trust services (eIDAS), ensuring cross-border recognition across EU member states for smoother identity verification. The second pillar involves the private sector, enabling companies to provide identity-linked services while adhering to eID regulations. The third pillar introduces the EU Digital Identity Wallet, a secure app that allows users to manage and control their identity data, ensuring privacy and portability. Blockchain plays a crucial role in supporting the framework, linking credentials to decentralized identifiers on the blockchain to ensure security and authenticity. The wallet employs biometric authentication for access, securely stores data, and provides users with full control over their information, enabling them to share only necessary details. Additionally, the wallet is designed for interoperability, ensuring seamless use across different services and EU member states.[15]

The final type of standard focuses on interoperability, where systems are required to work together seamlessly. These standards do not explicitly define processes or performance metrics but specify a fixed format to ensure smooth operation among systems using the same physical entity or data. The goal is to enable compatibility and coordination across different systems without dictating how each should perform or function.[12] In the financial sector, Chainlink has launched an initiative to standardize and improve access to corporate actions data through artificial intelligence (AI) and blockchain, addressing the issue of fragmented information, especially in Europe. Corporate action data, such as dividends, mergers, and stock splits, often come in inconsistent formats, leading to errors and financial losses. Despite efforts by organizations like the Depository Trust & Clearing Corporation, standardizing these data has been an ongoing challenge. The initial phase of Chainlink's project focuses on equity and fixed-income securities in six European countries. It will use decentralized oracles and advanced AI models like OpenAI's ChatGPT, Google's Gemini, and Anthropic's Claude to extract and structure corporate actions data into standardized "Golden Records" that comply with international standards, such as ISO 20022. These structured data will be shared across multiple blockchains using Chainlink's Cross-Chain Interoperability Protocol (CCIP). This initiative is expected to reduce manual processes, improve operational efficiency, and cut costs.

### Categories of standards based on establishment processes

Standards can also be categorized based on how they are developed and adopted, whether through market dynamics, regulatory mandates, or formalized collaboration. In the blockchain domain, all three categories, de facto, regulatory, and consensus standards, play critical roles in shaping the technology's evolution (Table 2). These standards not only guide blockchain development and deployment but also influence how ecosystems interoperate, gain legitimacy, and achieve mass adoption.

A de facto standard is widely accepted and used without formal approval, emerging through market consensus. Examples include the

QWERTY keyboard, PC architecture, and the UNIX operating system.[12] Ethereum can be viewed as a de facto standard in the blockchain industry, especially for smart contracts and decentralized applications (dApps). Flipside's "EVM Smart Contract Deployment Snapshot" report indicates that 637.9 million Ethereum Virtual Machine smart contracts have been deployed from January 2022, within a little over two years.[16] Likewise, as the largest blockchain oracle platform, Chainlink is focused on creating standards for blockchain oracles.[17]

Regulatory standards are established by agencies to ensure uniformity in processes independent of market forces.[12] As blockchain gains recognition, regulatory standards are evolving, with governments, international organizations, and regulators addressing its growing significance. The EU's Markets in Crypto Assets (MiCA) Regulation is focused on creating clear rules for crypto assets, protecting investors, and ensuring that crypto service providers comply with consumer protection requirements. The European Blockchain Services Infrastructure (EBSI) initiative seeks to create technical standards that facilitate cross-border interoperability for blockchain applications in public services across the European Union.

Consensus standards are voluntary standards developed by domestic or international bodies using agreed-upon procedures. These standards are created by organizations that plan, develop, and coordinate voluntary standards.[12] As of 2023, at least 30 organizations, including IEEE and GS1, were developing separate or overlapping standards.[3]

For instance, IEEE P3222.01, *Standard for Blockchain-Based Digital Identity Systems*, defines requirements for blockchain-based digital identity systems, covering identity creation, authentication, credentials (for example, ID cards or work cards), and data circulation protocols. It has been active since May 2020.[18]

## STANDARDIZING THE FUTURE: A TRANSATLANTIC PERSPECTIVE ON BLOCKCHAIN REGULATION

Europe and North America are key regions where standards-setting activities are predominantly concentrated,[19] reflecting their strategic roles in shaping global blockchain interoperability, governance, and regulatory frameworks. In this regard, Table 3 outlines the key areas where the European Commission (EC) considers blockchain standardization essential[6] and compares the regulatory roles in these areas between the EU and the United States.

### Interoperability

Blockchain interoperability is referred to as "the ability of blockchain networks to communicate with each other, sending and receiving messages, data, and tokens."[20] Key challenges in blockchain include the systematic benchmarking of interoperability solutions. This involves a structured evaluation of various blockchain solutions to measure their performance, efficiency, and compatibility across different networks, helping to identify the most effective solutions and areas for improvement. Additionally, there is a lack of standardized terminology as academia and industry often use different language, especially in rollups research.[21]

The EU drives blockchain interoperability through government-led infrastructure and regulatory alignment, while the United States relies on industry-driven pilots and sector-specific standards. The commission collaborates with the private sector, academia, and the blockchain community through the International Association of Trusted Blockchain Applications, a public/private partnership that promotes blockchain interoperability and governance and serves as a liaison with governments and international bodies.[22] The European public sector is creating its own blockchain infrastructure, which will soon be interoperable with private sector platforms. The EBSI is a peer-to-peer network of nodes run by the 27 EU countries, Norway, Liechtenstein, and the EC. It includes a base layer for infrastructure and storage, a core services layer for EBSI applications, and additional layers for specific use cases. The infrastructure will enable public organizations to develop applications, with plans to extend it to private organizations.[23] EBSI aims to provide a shared, secure, and interoperable infrastructure for EU-wide cross-border public sector digital services, reflecting European values like data sovereignty and sustainability. It will address global issues such as climate change and supply

**TABLE 2.** Categories of standards and their applications in the blockchain ecosystem.

| Category | Definition | Blockchain example |
|---|---|---|
| De facto standard | Widely adopted through market consensus without formal approval. | Ethereum for smart contracts and dApps; Chainlink as the leading oracle network. |
| Regulatory standard | Set by governmental or intergovernmental agencies to ensure legal compliance. | EU's MiCA Regulation for crypto asset oversight; EBSI for public service blockchain interoperability. |
| Consensus standard | Voluntary standards developed through collaborative, agreed-upon processes. | IEEE P3222.01 for blockchain-based digital identity systems. |

chain corruption, while ensuring high standards of scalability, security, and privacy. The infrastructure should be deployed within three years. Built as a "public permissioned" blockchain, EBSI's interoperable peer-to-peer network consists of 36 live nodes, with 11 more in setup, managed by the EC and EU member states.[24]

U.S. federal government initiatives, led by agencies such as the Department of Homeland Security (DHS), the U.S. Customs and Border Protection (CBP), the Department of the Treasury, and the Government Accountability Office, have aimed to advance blockchain interoperability, emphasizing operational applications, interagency collaboration, and the development of common standards. Pilot projects have tested blockchain's ability to streamline data sharing and verification processes across agencies. For example, the CBP within the DHS explored blockchain's potential to improve trade documentation and verify import legality, highlighting benefits such as enhanced interoperability and data integrity.[25] The Treasury and GAO expanded a blockchain prototype to a two-agency network under the JFMIP, emphasizing the importance of shared services and interoperability testing.[3] DHS's S&T Directorate, through its Silicon Valley Innovation Program, has worked with startups to develop interoperable standards for supply chain security and digital credentialing.[26]

U.S. federal agencies are collaborating with the private sector to improve blockchain interoperability, particularly in complex pharmaceutical supply chains. Current blockchain solutions, while industry specific, lack interoperability, creating challenges for firms adopting different systems to conduct business. As part of the FDA's program to evaluate the use of blockchain to protect pharmaceutical product integrity, Merck and Walmart partnered with IBM and KPMG in the DSCSA Pilot Project Program under section 582(j) of the FD&C Act in March 2019. The initiative aimed to assess blockchain's potential in ensuring interoperability among trading partners and meeting DSCSA 2023 compliance requirements. The project also explored blockchain's value beyond compliance, particularly in improving the medication recall process.[27]

### Governance

Countries are revising regulatory frameworks to attract crypto businesses,

**TABLE 3.** Key areas in blockchain standardization.

| Area | Explanation | EU | United States |
|---|---|---|---|
| Interoperability | Enabling seamless data exchange and communication among different blockchain and DLT platforms. | The public sector is creating its blockchain infrastructure, which will be interoperable with private sector platforms | Federal agencies' initiatives to advance interoperability, emphasizing operational applications, interagency collaboration, and the development of common standards. Federal agencies collaborating with the private sector to improve blockchain interoperability. |
| Governance | Setting rules, processes, and guidelines for managing blockchain projects and consortia on decentralized platforms. | MiCA aims to provide regulatory clarity for crypto assets and consumer/investor protection. No specific regulations for decentralized autonomous organizations (DAOs). | Federal regulation of cryptocurrencies and DAOs pending. States like Wyoming have recognized DAOs. |
| Identity | Establishing a unified or compatible identity system across various blockchain protocols and platforms. | eIDAS 2 explicitly recognizes DLT-based electronic trust services, granting them the same legal status as traditional services. | No national standard for digital identity: Utah was the first state to integrate blockchain into digital identity management. |
| Security | Maintaining the safety and reliability of nodes, networks, and services. | MiCA sets out requirements for blockchain nodes to reduce transaction risks and protect network participants. | The CETU's focus on dark web investigations, cryptocurrency fraud, and blockchain-related crimes. |
| Smart contract | Establishing guidelines and standards to enhance the security and reliability of smart contract technology. | MiCA regulation lacks full smart contract provisions. 2024: France's Autorité de contrôle prudentiel et de résolution collaborating with industry to mandate the certification of smart contracts before use. | The United States relies on varying state laws without a unified federal approach. |

with a focus on governance standards and investor protection.[28] The EU's MiCA Regulation establishes uniform rules for unregulated crypto assets, emphasizing governance through transparency, disclosure, authorization, and oversight to enhance market integrity, financial stability, and consumer protection.[29]

In the United States, regulatory uncertainty persists as lawmakers and industry stakeholders debate whether the Securities and Exchange Commission (SEC) or the Commodity Futures Trading Commission (CFTC) should oversee the crypto market. This ongoing disagreement, rooted in whether crypto assets are classified as securities or commodities, reflects broader governance challenges in establishing a clear and consistent regulatory framework.[30] The SEC is taking a stricter stance on proof-of-stake (PoS) tokens than proof-of-work assets. Chair Gary Gensler has suggested PoS tokens may be securities under the Howey test as they involve profit expectations based on others' efforts.[31]

One key area of blockchain governance is decentralized autonomous organizations (DAOs), which rely on smart contracts and token-based participation to enable decentralized decision making. In the EU, while MiCA provides regulatory clarity for crypto assets and enhances consumer and investor protection, it does not specifically address the distinctive governance structures and legal status of DAOs.[32] In the United States, while federal regulation of cryptocurrencies and DAOs remains pending, states like Wyoming have proactively recognized DAOs as a form of limited liability company, providing a legal framework for their operation.[32]

### Identity frameworks

Blockchain identity systems rely on advanced technologies and standards to ensure security, privacy, and user control. They incorporate key components that form a robust and reliable framework for managing digital identities.[33]

The EU's eIDAS 2 regulation establishes legal standards for DLT-based electronic trust services, enabling interoperability and removing key barriers to blockchain adoption.[34] By granting blockchain-based services the same legal status as traditional ones, it promotes integration into regulated sectors; supports smart contract enforceability; and encourages innovation across industries such as finance, real estate, and energy.[35]

In the United States, the absence of a national digital identity standard has led the federal government to delegate much of the responsibility to individual states.[36] Some states are developing regulatory frameworks for digital identity based on blockchain. These frameworks aim to enhance security, privacy, and control over personal data, offering a more transparent and decentralized approach to managing digital identities. Utah Governor Spencer Cox recently signed HB 470, mandating the state's Division of Technology Services (DTS) to launch a pilot program for digital verifiable credentials using blockchain. The bill requires DTS to provide recommendations on issuing digital IDs or records through DLT, as well as policies to protect personal privacy.[37] Utah was the first state to integrate blockchain technology into digital identity management.[38] Utah demonstrated its crypto ambitions by becoming one of the first states to accept digital assets for certain payments, including local and state taxes, placing it among a select few states taking this step.[39]

### Cybersecurity

Regulators in the EU and the United States are taking measures to enhance blockchain security by focusing on maintaining the safety and reliability of nodes, networks, and services. This includes implementing stricter compliance requirements, oversight, and security standards to ensure that blockchain systems operate securely and are resilient against potential threats.

The European Securities and Markets Authority (ESMA) has recommended that MiCA include mandatory third-party cybersecurity assessments for crypto firms and establish consistent security protocols across the EU. ESMA contends that FTX's collapse underscores the need for rigorous cybersecurity audits to strengthen crypto company resilience, although the EC cautions that such measures might exceed MiCA's intended scope.[40] MiCA sets out requirements for blockchain nodes to reduce transaction risks and protect network participants. Node operators offering commercial services must register with EU regulators and disclose details about their operations, infrastructure, and risks to enhance transparency. Nodes must implement strong data security measures, including encryption and backup, especially when handling sensitive data or high transaction volumes. Additionally, operators must follow AML and know-your-customer procedures to prevent illegal activities. Node operators are legally responsible for complying with these regulations and may face sanctions or fines for noncompliance.[41]

In the United States, the SEC is focusing on cybersecurity involving crypto assets to address risks posed to investors. Focused on cybersecurity and innovation oversight, the SEC's Cyber and Emerging Technologies Unit (CETU) investigates bad actors exploiting emerging technologies to deceive retail investors.[42] The SEC has also replaced its Crypto Assets and Cyber Unit with the new CETU. The CETU will focus on dark web investigations, cryptocurrency fraud, and blockchain-related crimes, reflecting the growing government and public attention on cryptocurrency.[43]

### Smart contracts

Smart contracts are computer programs that produce sequences of bits but do not define their meaning or

correct interpretation. For instance, a sequence like "e, s, t, a, t, e" could represent "estate," but it might also be random data, and the term "estate" has different meanings in different languages. Thus, smart contracts require external standards to properly encode/decode data and guide interpretation. These rules cannot be stored on the blockchain itself, as that would create a circular problem.[44] For smart contracts to function effectively, standards are thus key, particularly given the presence of users in multiple jurisdictions with different languages.

Smart contracts run exactly as coded, leaving no room for error; once deployed, they cannot be fixed, only replaced with a new version, which is costly and time consuming. Smart contract auditors are essential for ensuring the code's safety and security.[45] Therefore, establishing robust standards for smart contract development and auditing is crucial to ensure their reliability, security, and efficiency throughout their lifecycle.

Both government agencies and the private sector play vital roles in the implementation of auditing standards, ensuring compliance, promoting best practices, and enhancing the overall security of smart contracts. The Cardano Smart Contract Certification program sets standards for auditing and certifying smart contracts on Cardano, enhancing security and reliability through formal verification and building confidence among users and developers.[46]

The EU's MiCA regulation provides a broad blockchain framework but lacks full smart contract provisions.[47] Individual EU countries are also advancing smart contract regulation. In 2024, France's Autorité de contrôle prudentiel et de résolution (Prudential Supervision and Resolution Authority), with support from the Banque de France, proposed certifying smart contracts before deployment to ensure security and consumer protection. The initiative, which includes regulating decentralized finance platforms and blockchain infrastructure, reflects France's broader influence on EU-level crypto policy and aims to balance innovation with risk mitigation.[48]

The United States relies on varying state laws without a unified federal approach.[47] In 2017, Arizona became the first U.S. state to recognize smart contracts by passing legislation that included blockchain-based signatures and records. Tennessee followed in 2018, amending its statutes on electronic forms and signatures to incorporate blockchain.[49] In 2020, Illinois enacted the Blockchain Technology Act, which defines and enforces smart contracts under specified conditions. New York also introduced a bill that recognizes the use of smart contracts, although it is limited to commercial transactions.[50]

The contrasting approaches to blockchain standardization between the EU and the United States underscore the critical role of regulatory frameworks and collaborative governance in overcoming fragmentation and fostering global adoption. While the EU has leveraged centralized, principle-based initiatives like MiCA and EBSI to drive interoperability, security, and legal clarity across member states, the United States has adopted a decentralized model reliant on industry innovation and state-level experimentation. Both regions face persistent challenges, such as reconciling blockchain's decentralized nature with compliance requirements, addressing interoperability gaps, and harmonizing technical standards, that demand robust frameworks spanning metric- and performance-based paradigms. Moving forward, bridging transatlantic disparities through international collaboration on consensus standards, shared security protocols, and interoperable identity systems will be essential to unlocking blockchain's full potential as a scalable, secure, and globally integrated technology.

## REFERENCES


1. "Blockchain technology market size, share & trends analysis report," Grand View Res., San Francisco, CA, USA, Rep. ID: GVR-1-68038-329-4, Jan. 2025. Accessed: Apr. 19, 2025. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market
2. K. Stiff, "From real estate to identity standards, momentum rebuilds in Canada's blockchain industry," *The Globe and Mail*, Feb. 15, 2025. Accessed: Apr. 19, 2025. [Online]. Available: https://www.theglobeandmail.com/business/article-from-real-estate-to-identity-standards-momentum-rebuilds-in-canadas/
3. "Harnessing blockchain in the federal government: Key considerations for financial management and information systems," Joint Financial Manage. Improvement Program (JFMIP), Dec. 2023. Accessed: Apr. 19, 2025. [Online]. Available: https://www.cfo.gov/assets/files/JFMIP-24-01.pdf
4. C. Koch and K. Blind, "Towards agile standardization: Testbeds in support of standardization for the IIoT," *IEEE Trans. Eng. Manag.*, vol. 68, no. 1, pp. 59–74, Feb. 2021, doi: 10.1109/TEM.2020.2979697.
5. "The potential role of standards in supporting the growth of distributed ledger technologies/blockchain," RAND Europe, Cambridge, U.K. Accessed: Apr. 19, 2025. [Online]. Available: https://www.rand.org/randeurope/research/projects/2017/blockchain-standards.html
6. European Commission. "Blockchain standards." Digital Strategy. Accessed: Feb. 17, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/blockchain-standards
7. "Blockchain-based digital identity: Benefits, risks, and implementation challenges," Finance Magnates, Limassol, Cyprus, 2023. Accessed: Apr. 19, 2025. [Online]. Available: https://www.financemagnates.com/cryptocurrency/education-centre/

blockchain-based-digital-identity-benefits-risks-and-implementation-challenges/
8. R. Werle and E. Iversen, "Promoting legitimacy in technical standardization," *Sci. Technol. Innov. Stud.*, vol. 2, no. 1, pp. 19–39, 2006.
9. D. J. Teece, "Capturing value from knowledge assets: The new economy, markets, know-how, and intangible assets," *California Manage. Rev.*, vol. 40, no. 3, pp. 55–79, 1998, doi: 10.2307/41165943.
10. I. MacInnes, "A model for standard setting: High definition television," *Contemporary Econ. Policy*, vol. 12, no. 4, pp. 67–78, 1994, doi: 10.1111/j.1465-7287.1994.tb00446.x.
11. "Blockchain: Emerging technology offers benefits for some applications but faces challenges," U.S. Government Accountability Office (GAO), Washington, DC, USA, GAO-22-104625, Mar. 2022. Accessed: Apr. 19, 2025. [Online]. Available: https://www.gao.gov/assets/gao-22-104625.pdf
12. R. H. Allen and R. D. Sriram, "The role of standards in innovation," *Technol. Forecasting Social Change*, vol. 64, nos. 2–3, pp. 171–181, Jun. 2000.
13. Buidly, "Gas costs: EVM & Non-EVM blockchains," *Medium*, Oct. 14, 2024. Accessed: Mar. 18, 2025. [Online]. Available: https://medium.com/@buidly.tech/gas-costs-evm-non-evm-blockchains-f44daf3488d0
14. "12-month review virtual assets and VASPs," FATF, Paris, France, 2020. Accessed: Apr. 19, 2025. [Online]. Available: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html
15. Astrakode, "Digital identity and blockchain: Exploring the EU digital identity framework," *Medium*, Accessed: Apr. 19, 2025. [Online]. Available: https://astrakode.medium.com/digital-identity-and-blockchain-exploring-the-eu-digital-identity-framework-cdec759e03ba
16. G. Matos, "EVM chains see over 637 million smart contracts deployed since Jan 2022: Flipside," *Cryptobriefing*, Mar. 8, 2024. Accessed: Mar. 18, 2025. [Online]. Available: https://cryptobriefing.com/evm-smart-contract-deployment-surge/
17. G. Weston, "Top 10 blockchain oracles," Blockchain Georgia, Feb. 22, 2023. Accessed: Mar. 18, 2025. [Online]. Available: https://101blockchains.com/top-blockchain-oracles/
18. *IEEE Standard for Blockchain-Based Digital Identity Management*, IEEE Standard 3222.01, 2024. Accessed: Apr. 19, 2025. [Online]. Available: https://standards.ieee.org/ieee/3222.01/10242/
19. X. Jia, J. Xu, M. Han, Q. Zhang, L. Zhang, and X. Chen, "International standardization of blockchain and distributed ledger technology: Overlaps, gaps and challenges," *Comput. Model. Eng. Sci.*, vol. 137, no. 2, pp. 1491–1523, Jun. 2023, doi: 10.32604/cmes.2023.026357.
20. "Interoperability report," Eur. Blockchain Observatory and Forum, Nov. 30, 2023. Accessed: Apr. 19, 2025. [Online]. Available: https://blockchain-observatory.ec.europa.eu/document/download/c289f656-052a-4a72-b213-26b307691844_en?filename=EUBOF_Interoperability%20Report-30112023.pdf
21. R. Belchior, J. Süßenguth, Q. Feng, T. Hardjono, A. Vasconcelos, and M. Correia, "A brief history of blockchain interoperability," *Commun. ACM*, Sep. 24, 2024. Accessed: Apr. 19, 2025. [Online]. Available: https://cacm.acm.org/research/a-brief-history-of-blockchain-interoperability/
22. European Commission. "Blockchain strategy: Shaping Europe's digital future." Digital Strategy. Accessed: Apr. 19, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy
23. European Commission. "European blockchain services infrastructure." Digital Strategy. Accessed: Apr. 19, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure
24. C. R. W. De Meijer, "European blockchain services infrastructure (EBSI): The European way to get the most out of blockchain," *Finextra*, Mar. 5, 2024. Accessed: Apr. 19, 2025. [Online]. Available: https://www.finextra.com/blogposting/20963/european-blockchain-services-infrastructure-ebsi-the-european-way-to-get-most-out-of-blockchain
25. "CBP leverages blockchain innovation to protect American business." U.S. Customs and Border Protection (.gov). Accessed: Feb. 28, 2025. [Online]. Available: https://www.cbp.gov/newsroom/national-media-release/cbp-leverages-blockchain-innovation-protect-american-business#:~:text=The%20technology%20is%20critical%20to,rapid%20adoption%20and%20cost%20reduction
26. "Feature article: S&T's Silicon Valley innovation program leverages blockchain interoperability to support DHS," Dept. of Homeland Secur. (DHS), Washington, DC, USA, Oct. 8, 2020. Accessed: Apr. 19, 2025. [Online]. Available: https://www.dhs.gov/science-and-technology/news/2020/10/08/feature-article-st-svip-leverages-blockchain-interoperability-support-dhs
27. "FDA DSCSA: Blockchain interoperability pilot project report," Feb. 2020. Accessed: Oct. 10, 2023. [Online]. Available: https://www.fda.gov/media/169883/download
28. "How regulation will shape key crypto narratives in 2025."Mercuryo. Accessed: Apr. 19, 2025. [Online]. Available: https://mercuryo.io/explore/article/how-regulation-will-shape-key-crypto-narratives-in-2025
29. "Markets in crypto-assets regulation (MiCA)." European Securities and Markets Authority (ESMA). [Online]. Accessed: Oct. 10, 2023. Available: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica
30. A. Kumar. "What is next for crypto regulation in the US?"

CryptoPolicyReview.com. Accessed: Oct. 10, 2023. [Online]. Available: https://www.atlanticcouncil.org/blogs/econographics/what-is-next-for-crypto-regulation-in-the-us/
31. J. Valente, "Clash of consensus: How the SEC's stance on proof of stake tokens challenges Crypto's Green Future," *Georgetown Environmental Law Rev.*, Apr. 17, 2024. Accessed: Apr. 19, 2025. [Online]. Available: https://www.law.georgetown.edu/environmental-law-review/blog/clash-of-consensus-how-the-secs-stance-on-proof-of-stake-tokens-challenges-cryptos-green-future/
32. J. M. de Corral. "DAO legal landscape: An overview of challenges & approaches." *Rif.technology*. Accessed: Apr. 19, 2025. [Online]. Available: https://rif.technology/content-hub/dao-regulations/
33. P. Horbonos, "Introduction to digital identity blockchain," *Blaize Tech Blog*, Aug. 12, 2024. Accessed: Apr. 19, 2025. [Online]. Available: https://blaize.tech/blog/blockchain-digital-identity/
34. Jurisconsul. "EU's digital revolution: How eIDAS 2 could spark a blockchain boom in government and industry." Lexology. Accessed: Apr. 19, 2025. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=af833dbd-f83f-4358-8594-ecaa0e8306a8
35. E. Sotiri. "EU's digital revolution: How EIDAS 2 could spark a blockchain boom in government and industry." Jurisconsul. Accessed: Apr. 19, 2025. Accessed: Apr. 20, 2025. [Online]. Available: https://www.jurisconsul.com/post/eu-s-digital-revolution-how-eidas-2-could-spark-a-blockchain-boom-in-government-and-industry
36. A. Johnson, "The path to digital identity in the United States," Inf. Technol. and Innov. Found., Washington, DC, USA, Sep. 23, 2024, Accessed: Apr. 19, 2025. [Online]. Available: https://itif.org/publications/2024/09/23/path-to-digital-identity-in-the-united-states/
37. K. Quinlan, "Utah governor signs blockchain digital ID pilot into law," *StateScoop*, Apr. 12, 2023. Accessed: Apr. 19, 2025. [Online]. Available: https://statescoop.com/utah-governor-signs-blockchain-digital-id-pilot-into-law/
38. B. Norton, "Navigating the legal framework: Implementing a government-backed digital identity in the United States," *Jurimetrics*, vol. 64, pp. 169–199, Winter 2024. Accessed: Apr. 19, 2025. [Online]. Available: https://www.americanbar.org/content/dam/aba/publications/Jurimetrics/winter-2024/navigating-the-legal-framework-implementing-a-government-backed-.pdf
39. D. Hamilton, "Top 10 pro-crypto states you need to know," *Securities.io*, Sep. 4, 2023. Accessed: Apr. 19, 2025. [Online]. Available: https://www.securities.io/top-10-pro-crypto-states-you-need-to-know/
40. "EU crypto firms face cyber audits and ESMA oversight on security breaches," *CCN*, n.d. Accessed: Apr. 19, 2025. [Online]. Available: https://www.ccn.com/news/crypto/eu-crypto-firms-cyber-audits-esma-security-breaches/
41. K. Quinlan, "MiCA regulation for node operators and its impact on the digital asset ecosystem," *Rue.ee Blog*, 2023. Accessed: Apr. 19, 2025. [Online]. Available: https://rue.ee/blog/mica-regulation-for-node/
42. "Cyber, crypto assets and emerging technology." U.S. Securities and Exchange Commission. Accessed: Apr. 19, 2025. [Online]. Available: https://www.sec.gov/about/divisions-offices/division-enforcement/cyber-crypto-assets-emerging-technology
43. T. Orme-Claye, "US markets watchdog sets up new crypto and cybersecurity unit," *Payment Expert*, Feb. 21, 2025. Accessed: Apr. 19, 2025. [Online]. Available: https://paymentexpert.com/2025/02/21/sec-crypto-and-cyber-security-unit/
44. V. Capocasale and G. Perboli, "Standardizing smart contracts," *IEEE Access*, vol. 10, pp. 91,203–91,212, 2022, doi: 10.1109/ACCESS.2022.3202550. Accessed: Apr. 19, 2025. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9869650
45. "What is a smart contract audit?" Hedera. Accessed: Apr. 19, 2025. [Online]. Available: https://hedera.com/learning/smart-contracts/smart-contract-audit
46. "What is the Cardano smart contract certification program." NMKR. Accessed: Apr. 19, 2025. [Online]. Available: https://www.nmkr.io/glossary/cardano-smart-contract-certification-program
47. A. Krowne, "Legal challenges in defining and regulating smart contracts," Industria Bus. Lawyers LLP, Miami, FL, USA, Nov. 14, 2024. [Online]. Accessed: Apr. 19, 2025. Available: https://ibl.law/legal-challenges-in-defining-and-regulating-smart-contracts/
48. "France's prudential regulator advances work on certification of smart contracts," *Ledger Insights*, Jun. 5, 2024. Accessed: Apr. 19, 2025. [Online]. Available: https://www.ledgerinsights.com/frances-prudential-regulator-advances-work-on-certification-of-smart-contracts/
49. M. Orcutt, "States that are passing laws to govern 'smart contracts' have no idea what they're doing," *MIT Technol. Rev.*, Mar. 29, 2018. Accessed: Apr. 19, 2025. [Online]. Available: https://www.technologyreview.com/2018/03/29/144200/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/
50. "Smart contracts and U.S. state law," Morris, Manning & Martin, LLP, Atlanta, GA, USA, Apr. 5, 2023. Accessed: Apr. 19, 2025. [Online]. Available: https://www.mmmlaw.com/news-resources/102ibtf-smart-contracts-and-u-s-state-law/

**NIR KSHETRI** is a professor of management in the Bryan School of Business and Economics, University of North Carolina at Greensboro, Greensboro, NC 27412 USA. Contact him at nbkshetr@uncg.edu.