Read-Ahead for NIST Workshop on Blockchain and DLT

April 7, 2026

On April 16, 2026, NIST is convening a public workshop to examine technical considerations at the technology layer of blockchain and DLT. The workshop will focus on technical architectures, interoperability, risk management practices, and security risks in real-world blockchain and DLT deployments. Discussions will be technically focused, and attendees would benefit from prior familiarity with the technical design, deployment, security, or standardization of blockchain and DLT systems. **Feedback on this document, including any responses to the questions noted under Next Steps (p. 2), is requested by April 21, 2026 and may be sent by email to blockchain@list.nist.gov.**

1. Background

Distributed ledger technologies (DLT), namely blockchains, continue to attract significant interest for their potential to support new forms of digital infrastructure, recordkeeping, and digital assets across a range of sectors. The recent White House report *Strengthening American Leadership in Digital Financial Technology* highlights the importance of blockchains and related technologies to innovation and U.S. leadership, including and beyond the financial services sector. It also underscores NIST's role in standards development through pre-standardization research and participation in standards-setting activities.

2. Workshop Goals and Audience

The objective of the workshop is to:

- Identify existing technical resources, standards, and ongoing efforts relevant to blockchain and DLT
- Highlight key challenges and areas that may warrant further attention by industry, standards organizations, or the research community
- Support improved coordination across existing technical workstreams
- Inform NIST's understanding of the current cybersecurity, interoperability, and privacy landscape for blockchain and DLT technologies

This workshop is intended for:

- DLT platform and infrastructure developers
- Security engineers and system architects
- Standards developers and technical contributors
- Practitioners with experience designing, deploying, or assessing DLT systems
- Policymakers and regulators interested in DLT/blockchain technologies, digital assets, and the suite of critical and emerging technologies that enable this ecosystem, including post-quantum cryptography, digital identity, digital wallets, smart contracts, and privacy-enhancing technologies

3. Next Steps

From this workshop, NIST will develop a public report that synthesizes the technical input received, identifies key findings and gaps, and describes potential next steps and areas for further work by NIST, industry, and standards organizations. The public report will reflect attendee feedback in response to the following questions:

Standards and Common Practices Driving Interoperability

- What are the primary technical barriers to interoperability between DLT systems?
- What existing widely adopted practices, specifications, or standards are being used to support interoperable and secure DLT deployments?
- Which approaches have seen significant industry adoption, and what has contributed to their uptake?
- Where have community specifications, processes, and practices emerged in the absence of formal standards?
- What existing standards, practices, and technologies are being used to support regulatory and risk management outcomes, for example, those relating to data governance, digital identity or privacy-enhancing technologies?

Gaps and Technical Challenges

- Where do gaps exist in current standards, guidance, or shared technical practices?
- Which challenges appear to be primarily technical in nature, and which arise from system integration, lifecycle management, or operational complexity?
- What are the obstacles to adopting standards and practices supporting interoperability and cybersecurity?
- Do current architectures support both individual privacy and compliance obligations like AML/CFT?

Cybersecurity and Privacy Risks

- What attack paths are top of mind – including those that directly target managed systems, as well as those whose aim is to leverage managed systems as part of a supply chain attack?
- What security and privacy risks are most relevant for deployed DLT systems?
- What classes of failures, vulnerabilities, and attacks recur across different platforms, architectures, and use cases and how do they arise at the protocol, implementation, and operational layers?
- How do failures and attacks propagate across systems and affect other participants, partners, and stakeholders?

Ongoing Efforts to Develop Standards and Improve Coordination

- Where are industry, open-source communities, and standards organizations already coordinating effectively on DLT security and privacy topics?
- What existing technical workstreams or forums could be leveraged or better aligned?
- Where might additional collaboration be beneficial?

Appendix: Distributed Ledger Technologies, Threat Landscape Overview, and Relevant Standards

Section 1: Introduction to Blockchain and DLT

Distributed Ledger Technologies (DLTs) are systems for recording and sharing data (often value transfers) across a network of participants without the need for a centralized entity. A common type of DLT is a blockchain.[1, 2] Blockchains are tamper-evident and tamper-resistant digital ledgers implemented in a distributed fashion that enable a community of users to record transactions in a shared ledger, such that under ideal operation of the blockchain network no transaction can be changed without detection once recorded in the ledger.

Blockchains can be implemented as permissionless systems or as permissioned systems. They can be open for participation by all or closed to a private group of participants. Communities and organizations across various sectors have adopted or piloted the use of private, permissioned blockchain systems – for example, as a means of providing supply chain provenance, digital record integrity, or auditability of transactions. Additionally, an ecosystem of blockchain networks has emerged, built largely on the same stack of shared infrastructure that much of the connected world relies upon, such as web servers and cloud infrastructure. The growth of these networks has resulted in the development of subsequent layers of technology, demonstrated in the graphic below and described in Table 1.

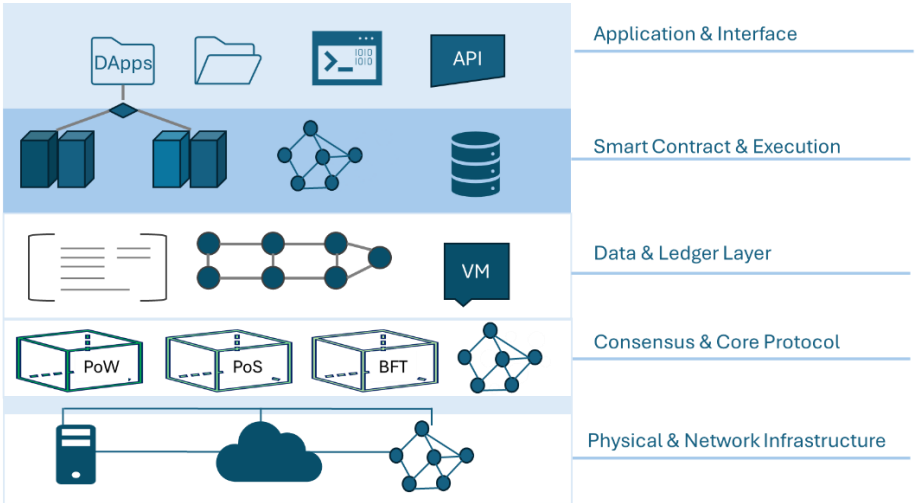

Figure 1. Key components of the blockchain technology stack

Table 1. Blockchain Ecosystem Layers & Components

Application and Interface Layer	
Identity and access management	Mechanisms that bind actions on-chain to entities and control who can participate in a network or permissioned ledger.
Decentralized Apps (dApps)	Applications that use smart contracts and the blockchain as a backend, typically combining on-chain logic with off-chain UI and services.
Wallets	Software or hardware that stores private keys, derives addresses, presents balances, and signs transactions on behalf of users.
Off-chain scalers	Protocols and services that enable external computation or transaction processing with periodic main chain reconciliation.
Smart Contract and Execution Layer	
Oracles	External services or mechanisms that feed off-chain data into smart contracts so that on-chain logic can react to real-world events.
Smart contracts	Programs deployed on the blockchain that execute when triggered by transactions, updating ledger state according to pre-set rules.
Data and Ledger Layer	
Tokens	Digital representations of value or rights tracked on the ledger, moved by transactions and often governed by smart contract logic.
Transactions	Signed data structures that describe state changes and are collected into blocks and validated.
Distributed ledger	Append-only record of cryptographically linked blocks replicated across many nodes so all participants share a consistent transaction history.
Consensus and Core Protocol Layer	
Cryptography	Various cryptographic techniques can be used to encrypt or sign data, link blocks, derive addresses, and verify transaction authenticity.
Consensus mechanisms	Protocols that let mutually distrusting nodes agree on the contents of a distributed ledger
Physical and Network Infrastructure Layer	
Network nodes	Computers participating in the peer-to-peer network that relay transactions, validate blocks, and maintain copies of the ledger.
Compute	Processing resources of network nodes used to validate transactions, execute smart contracts, and run consensus algorithms.
Storage	Mechanism for holding and accessing blockchain data, state databases, and often auxiliary indexes or archives on network nodes.

Section 1A. Permissionless vs. Permissioned Systems

The blockchain technology stack is designed to implement a distributed, append-only ledger that records a sequence of validated transactions. Requests for new transactions to be added to the ledger, are typically cryptographically validated using digital signatures. Blockchains must solve the problem of allowing a distributed set of users to agree on which block(s) of data should be part of the chain and in what order. This leads to different architectural implementations of blockchain solutions (permissioned and permissionless).

In permissionless blockchains, where anybody can propose a new block of transactions to add, Proof of Work[3] or Proof of Stake[4] are common ways to establish this consensus. Alternatively, permissionless blockchains can restrict which users can read from or write to the chain and may consequently use other consensus methods such as Proof of Authority.[5] These consensus protocols help to enforce the append-only property, creating long-term stability for the contents of past blocks. The blocks themselves are then connected through a chain of cryptographic hashes to ensure all past data is represented in subsequent blocks. Outside of this primary distinction on governance and consensus, additional differences between permissioned and permissionless ledgers are summarized below.

Table 2. Comparison of Permissionless vs. Permissioned Blockchains

Dimension	Permissionless Blockchain	Permissioned Blockchain
Network access	Open to anyone with internet access; no prior approval to publish blocks of transactions.	Restricted to approved participants; access controlled by an organization or consortium.
Control and governance	Decentralized; protocol changes and operations governed by broad community and open-source processes.	Centralized or consortium-led; a governing entity manages membership, rules, and upgrades.
Identity model	Typically pseudonymous; identities not strongly bound to real-world entities.	Users that participate in consensus are known or verifiable entities; often integrated with enterprise identity and compliance. Note that users who

Dimension	Permissionless Blockchain	Permissioned Blockchain
		submit transactions to the validators might not be verified.
Data visibility	Ledger and transactions are publicly visible and auditable by anyone.	Data visibility limited to network members; fine-grained controls can restrict who sees what.
Consensus mechanisms	Resource-based, highly decentralized mechanisms (e.g., PoW, PoS, proof of space/time) designed for open participation.	Identity-based, configurable mechanisms (e.g., PoA, PBFT variants, Raft, PoET) optimized for known validators.
Performance and scalability	Lower throughput, higher latency, and variable fees due to global, adversarial consensus assumptions.	Higher throughput, low latency, and predictable costs because there are fewer, permissioned nodes.
Security and trust model	Security from large, diverse validator sets and economic incentives; minimizes need to trust any single operator.	Security relies more on access control, governance, and trust in the operating organization(s).
Censorship resistance	Strong: difficult for any single actor to censor transactions or rewrite history.	Weaker: controlling entities can, in principle, block transactions or alter policies.
Privacy characteristics	Weak transactional privacy by default; requires add-on techniques (mixers, zero-knowledge, etc.).	Stronger privacy; data and participation can be limited to specific entities, with selective disclosure.
Compliance alignment	Harder to align directly with strict KYC/AML and data localization without additional layers.	Easier to embed KYC/AML, role-based access, and regulatory controls into the network design.

Section 1B. Blockchain Use Cases

There are several use cases enabled by blockchain technologies that allow for public or private recording of information in the distributed ledger as well as validation and consensus of that information across a wide variety of sectors from healthcare to real estate.

In the area of **healthcare**, blockchains have been demonstrated as a supporting technology for electronic health records management,[6] pharmaceutical and blood bank supply chain integrity,[7] smart contracts for insurance claim processing,[8] patient identity,[9] medical data ownership,[10] internet of medical things,[11] and for clinical trial/research data sharing.[12]

In the area of **manufacturing**, DLTs are being used for managing and tracing supply chain properties including integrity and traceability,[13] smart contracts for automation,[14] asset tracking in manufacturing-as-a-service (MaaS),[15] compliance and auditing of provenance of manufactured products,[16] and digital twin integrity.[17]

In the **energy** sector, DLTs are being used for peer-to-peer trading of energy from renewable sources based on demand,[18] keep track of energy credits for tracking origin of "green" energy,[19] and grid modernization for coordination of millions of IoT devices on energy usage.[20]

In the **financial** sector, other than cryptocurrencies, DLTs are being used for managing intraday liquidity to facilitate internal transfers outside regular banking hours,[21] accounting/audit,[22] trading, clearing, settlement,[23] custody of assets,[24] grant funding,[25] and automating payments.[26]

In the **real estate** sector, DLTs are being utilized for fractional ownership using tokenized assets,[27] smart contracts for leasing,[28] and immutable title records.[29]

Section 2: Trends in the Blockchain and DLT Threat Landscape

Stakeholder engagement and research to-date conducted by NIST has revealed that DLTs aren't immune to cyber risk, and they still depend on much of the same underlying infrastructure as traditional IT architectures do, for instance, web servers, APIs, and commercial cloud platforms. Many incidents involving public blockchains look like familiar compromises but with higher stakes: funds can move faster, transactions are difficult to reverse, and the most valuable targets are the keys, signing workflows, and smart contract code that control access to assets.

Beyond the threats detailed below, common issues contributing to the ecosystem's challenges include inconsistent cybersecurity hygiene; key loss and theft; social engineering and scams that present as new investment opportunities; and unmanaged vulnerabilities or bugs in underpinning IT infrastructure, smart contracts, or zero knowledge proofs. These are exacerbated by (1) the lack of a consistent vetting process prior to a project being launched or token being offered; and (2) mass adoption of AI by project participants that do not employ secure development practices, leading to flawed or insecure production code.

AI-generated code may pull in outdated or vulnerable libraries, reuse insecure patterns, or create silent failures that look correct but hide exploitable logic bugs. Models often lack full system context, producing code that breaks architectural rules or is hard to maintain. These issues are particularly risky for blockchain and DLT systems because small coding mistakes can have outsized and often irreversible consequences: a small bug in a smart contract (e.g. access control, reentrancy, upgrade logic) can enable unauthorized transfers or lock funds. Limited expert review further increases the chance that insecure dependencies, overly broad privileges, or misconfigurations make it into production code, where fixing these issues may require downtime across multiple systems or complex governance.

This section provides an overview of the trends in this rapidly evolving threat landscape, underscoring the need for stronger implementation of controls across the ecosystem and impacted sectors, not just at a single point in the technology stack.

Trend 1: Attackers are increasingly shifting toward tactics that target people and operational workflows, not just smart contract bugs. One clear signal is the rise in personal wallet compromises, with threat actors targeting more individuals as adoption increases. In parallel, centralized services are seeing larger losses as adversaries focus on private key infrastructure and the signing process, often attacking the systems and people involved in preparing and approving transactions. Even cold wallet controls can be bypassed by advanced threats if they can compromise the surrounding environment or manipulate the human steps in the process. To that end, social engineering remains[30] a major threat to blockchain and DLT users, administrators, and developers.

Trend 2: Connections between services are being exploited. Attackers are taking advantage of third-party wallet integrations and increasingly trying to trick legitimate signers into authorizing malicious transactions. Supply chain compromises [30] remain a major risk as well, where a breach at a vendor or upstream dependency can cascade across multiple targets. In particular, DPRK-linked actors have been dominant, applying an approach that blends technical intrusion with insider access through embedded IT workers at cryptocurrency firms who gain privileged access and enable high-impact thefts. Another tactic involves the use of sophisticated social engineering campaigns, including impersonating recruiters from prominent Web3 and AI firms and conducting fake hiring processes that end in "technical screens" designed to steal credentials, source code, and VPN or SSO access to the victim's current employer.[31] The $1.4 billion ByBit[32] compromise in February 2025, attributed to a sophisticated social engineering and supply-chain campaign by North Korean threat actors, highlights both the relevance and the severity of these threats to the blockchain and broader DLT ecosystem.

Trend 3: Ransomware is another key ecosystem-wide issue that continues to grow with ramifications that cross sector boundaries.[33] Cryptocurrency has become a preferred payment method for ransomware attacks inflicted upon organizations of all types. Unfortunately, the gains in speed and scalability of the current architectures that underpin most public blockchain and DeFi networks have also made it easier for attackers to receive funds at any time, from anywhere, and then rapidly shift or fragment proceeds across wallets and services to avoid detection and interception. In the context of the blockchain ecosystem, ransomware attacks on other sectors can be conceptualized as a supply chain attack that starts with the compromise of a primary victim's system or data and that is further supported by deceptive use of the blockchain stack to move ransom proceeds.

Trend 4: Illicit finance (AML/CFT) risks remain central to the ecosystem's shared challenges.[34] Similar to the movement of ransom proceeds, threat actors often use DeFi services as part of the process for transferring and laundering funds, stitching together swaps, bridges, and other protocols to obscure where funds came from and where they end up. Compared with many traditional payment architectures, this can be faster and less dependent on regulated intermediaries, especially when services don't consistently implement technical and management controls intended to mitigate these risks, making it easier for bad actors to exploit gaps in oversight.

Trend 5: Threat trends in private, permissioned blockchains are increasingly shaped by operational weaknesses, such as node compromises, availability attacks, and flaws in smart contract implementations. Denial-of-Service (DoS) attacks on core components can increase latency, reduce throughput, and in extreme cases make the ledger inaccessible.[35] At the application layer, issues like smart contract endorser identity exposure can make it easier to target specific participants for disruption. Another notable risk for private blockchains, which tend to involve fewer participants, is insider collusion or

corruption, or single points of failure if a controlling entity or privileged account is compromised.

Looking ahead, **one of the most significant emerging threats to blockchain and DLT systems is quantum computing.** Quantum algorithms could solve certain hard computational problems much faster than today's computers, and a sufficiently powerful quantum machine could undermine public-key cryptography by deriving private keys from public keys, enabling attackers to impersonate users, drain wallets, and interfere with smart-contract activity.[36] As quantum capabilities mature, blockchains and DeFi protocols will need clear migration paths to quantum-resistant cryptography and stronger key management practices to preserve long-term security.

Additionally, while AI offers the opportunity for greater participation in blockchain networks, it also may exacerbate the risk of insecure or buggy code being contributed. Currently, limited expert review processes are in place, which further increases the chance that insecure dependencies, overly broad privileges, or misconfigurations make it into production code, where fixing these issues may require downtime across multiple systems or complex governance.

Section 3: Blockchain and DLT Standards Landscape

Given the distributed technology architecture of this ecosystem there are a variety of standards and protocols that support specific functions ranging from identity and access controls, token issuance and management, data exchange/messaging and privacy and security. This section summarizes a few prominent standards organizations and efforts at various stages of maturity as they relate to the blockchain and DLT technology stack. The focus is on standards that could be applied across various blockchains and not on network-specific standards. Below is a non-exhaustive list of various standardization efforts taking place to normalize language and practices across the technology ecosystem, including efforts that are specific to blockchain systems.

NIST maintains and is developing numerous resources that offer guidance and best practices that can apply directly to various parts of the DLT technology stack. Resources such as NIST Cybersecurity Framework (CSF) 2.0,[37] Secure Software Development Framework Version 1.2,[38] and NIST Call for Multi-Party Threshold Schemes[39] are relevant for the lowest layers of the technology stack. Other resources, including NIST Digital Identity Guidelines, Revision 4,[40] Zero Trust Architecture,[41] and Ransomware Risk Management: A CSF 2.0 Community Profile[42] would apply to higher layers. NIST's Post-Quantum Cryptography project[43] directly addresses potential future threats to core underlying cryptographic mechanisms of DLT. NIST is also actively developing technical resources to help financial institutions use mobile driver's licenses (mDLs) for customer identification.[44]

The **International Organization for Standardization (ISO)** has established a Technical Committee (ISO TC 307 *Blockchain and distributed ledger technologies*) to develop a series of resources applicable to or scoped specifically for blockchain implementations. These include resources such as Blockchain and distributed ledger technologies - Vocabulary[45] and Taxonomy and Ontology,[46] focus on standardizing common terms and concepts. ISO maintains a reference blockchain architecture[47] in addition to other efforts that exist at various stages of maturity to address smart contract security (ISO24875 series),[48] privacy (ISO/WD 24876.6, ISO/DIS 24946), digital assets management (ISO/WD 25316), decentralized identity systems (ISO/WD 23042),[49, 50] governance (ISO/TS 23635:2022, ISO/AWI TS 25481), interoperability (ISO/TS 23516),[51,52] wallet interoperability,[53] and information sharing.[54] ISO also maintains the standard for Mobile driving licenses, including add-on functions for online presentation of credentials (ISO/IEC 18013).[55]

The **International Telecommunication Union Telecommunication Standardization Sector (ITU-T)** is actively pursuing work relevant for blockchain and distributed ledger technologies through SG17 (Security), SG16 (Multimedia), SG13 (Future Networks), and SG20 (IoT/Smart Cities).

AICPA SOC 2 (Trust Services Criteria)[56] has become a common expectation for exchanges, custodians, and infrastructure platforms to demonstrate operational security and privacy controls.

IEEE P2145 develops standards for framework and definitions for blockchain governance, addressing decision-making structures and upgrade mechanisms. IEEE 3205-2023[57] establishes the Standard for Blockchain Interoperability Data Authentication and Communication Protocol, enabling cross-chain data verification.

IETF RFC 8578 (DetNet Use Cases)[58] addresses deterministic networking requirements including point-to-multipoint and low-latency transport suitable for blockchain traffic in production environments.

W3C WebAuthn (Levels 2[59] & 3[60]) and **FIDO**2[61] specify strong, cryptographic, phishing-resistant credentials essential for securing access to Web3 accounts and identity wallets. W3C also manages the Verifiable Credentials Data Model v2.0.[62]

OpenID Connect (OIDC) provides authentication layers critical for "sign-in with X" flows that bridge Web2 identities into Web3 ecosystems. OpenID for Verifiable Presentation 1.0[63] and Verifiable Credential Issuance 1.0[64] enable standardized, privacy-preserving credential exchange between wallets, issuers, and verifiers.

The **Government Blockchain Association** has developed a Blockchain Maturity Model.[65]

The **Blockchain Security Standards Council** has undertaken several efforts to define best practices, notably:

- Node Operation Standard[66]
- Token Integration Standard[67]
- Key Management Standard[68]
- General Privacy and Security Guidelines[69]

The **Global Blockchain Business Council** maintains a comprehensive mapping of technical and legal standards, as well as blockchain network-specific protocols across the blockchain technology stack through their Global Standards Mapping Initiative 6.0 report[70] organized into four layers:

1. **Infrastructure and Protocol Layer**: The foundational layer encompasses consensus mechanisms, blockchain interoperability, and core protocol specifications.
2. **Data and Token Standards**: This layer governs how digital assets are represented, structured, and transferred across networks.
3. **Digital Identity and Access Control**: This layer outlines identity standards, which form the critical trust layer enabling compliant, secure interactions.
4. **Application and Use Case**: Standards at this layer address specific implementations and regulatory compliance.

References

1. Baron J, O'Mahony A, Manheim D, Dion-Schwarz C (2015) *National Security Implications of Virtual Currency*. Available at: https://www.rand.org/pubs/research_reports/RR1231.html
2. Bayer D, Haber S, Stornetta WS (1993) Improving the Efficiency and Reliability of Digital Time-Stamping. *Sequences II*, Capocelli R, De Santis A, Vaccaro U (Springer, New York, NY), pp. 329-334. https://doi.org/10.1007/978-1-4613-9323-8_24
3. Behnke R (2025) *EXPLAINED: THE BIGONE HACK (JULY 2025)*. Available at: https://www.halborn.com/blog/post/explained-the-big-one-hack-july-2025
4. Buterin, V (2014). A Next-Generation Smart Contract and Decentralized Application Platform. Available at: https://ethereum.org/en/whitepaper
5. Chainalysis (2026) *Chinese Language Money Laundering Networks Emerge as Major Facilitators of the Illicit Crypto Economy, Now Driving 20% of Laundering Activity*. Available at: https://www.chainalysis.com/blog/2026-crypto-money-laundering/
6. Chainalysis (2026) *Total Ransomware Payments Stagnate for Second Consecutive Year, While Attacks Escalate*. Available at: https://www.chainalysis.com/blog/crypto-ransomware-2026/
7. Fast-Track Action Committee on Digital Assets Research and Development (2023) National Objectives for Digital Assets Research and Development. (White House National Science and Technology Council, Washington, DC). https://www.nitrd.gov/pubs/National-Objectives-for-Digital-Assets-RD-2023.pdf
8. Global Blockchain Business Council (2025) *101 Real-World Blockchain Use Cases Handbook: 2025 Edition*. Available at: https://downloads.ctfassets.net/so75yocayyva/1QeBFAtvDyoHK6pJgG5ITU/91f891937e91c20dc430d8eb6ef66c5b/GBBC-s_101_Real-World_Blockchain_Use_Cases_Handbook_digital.pdf
9. Global Blockchain Business Council (2024) *Global Standards Mapping Initiative 5.0: The Future of Global Supply Chains: December 2024 Edition*. Available at: https://www.gbbc.io/uploads/reports/gsmi50/Supply-Chain-Stand-Alone.pdf
10. Haber S and Stornetta WS (1991) How to time-stamp a digital document. Journal of Cryptology. 3 (2): 99–111. https://link.springer.com/article/10.1007/BF00196791
11. Haber S and Stornetta WS (1997) Secure names for bit-strings. *In Proceedings of the 4th ACM conference on Computer and communications security (CCS '97)* (Association for Computing Machinery, New York, NY, USA), pp. 28–35. https://doi.org/10.1145/266420.266430
12. Marikyan D, Papagiannidis S, Rana OF, Ranjan R (2022) Blockchain adoption: A study of cognitive factors underpinning decision making. *Computers in Human Behavior* 131(2022):107207. https://www.sciencedirect.com/science/article/pii/S0747563222000292
13. Nakamoto S (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf

14. Padalkar N (2023) Unveiling the Digital Shadows: Exploring the Role of Technology in Illicit Finance Flows. *11th IMF Statistical Forum*. https://www.imf.org/-/media/files/news/seminars/2023/11th-stats-forum/session-iii-nakul-r-padalkar.pdf
15. Salam A (2023) Blockchain Revolutionizing Healthcare Industry: A Systematic Review of Blockchain Technology Benefits and Threats. *Perspectives in Health Information Manag*ement 20(3):1b. https://pmc.ncbi.nlm.nih.gov/articles/PMC10701638/
16. Strengthening American Leadership in Digital Financial Technology, Executive Order 14178 (2025).
17. The MITRE Corporation (2025) *Adversarial Actions in Digital Asset Payment Technologies (AADAPT) Framework*. Available at: https://aadapt.mitre.org/
18. Tripathi G, Ahad MA, Casalino G (2023) *A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges*. Decision Analytics Journal, Volume 9, 2023, 100344, ISSN 2772-6622. https://www.sciencedirect.com/science/article/pii/S2772662223001844
19. United States Department of the Treasury (2023). *Illicit Finance Risk Assessment of Decentralized Finance*. Available at: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf
20. United States Senate Committee on Homeland Security and Governmental Affairs (2022). *Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns*. Available at: https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf

Endnotes

[1] Yaga D, Mell P, Roby N, Scarfone K (2018) Blockchain Technology Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal Report (NISTIR) 8202. https://doi.org/10.6028/NIST.IR.8202

[2] Davidson M (2023) State Machine Replication and Consensus with Byzantine Adversaries. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal Report (NISTIR) 8460. https://csrc.nist.gov/pubs/ir/8460/ipd.

[3] Alzoubi YI, Mishra A, Aljaafreh A (2025) Blockchain based on proof-of-work consensus algorithm: Evolution and future potential. *Energy Nexus* 20:100577. https://doi.org/10.1016/j.nexus.2025.100577

[4] Saleh F (2021) Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies* 34(3):1156–1190. https://doi.org/10.1093/rfs/hhaa075

[5] Manolache MA, Manolache S, Tapus N (2022) Decision Making using the Blockchain Proof of Authority Consensus. *Procedia Computer Science* 199:580-588. https://doi.org/10.1016/j.procs.2022.01.071

[6] Haddad A, Habaebi MH, Islam MR, Hasbullah NF, Zabidi SA (2022) Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems. *IEEE Access* 10: 94583-94615. https://doi.org/10.1109/ACCESS.2022.3201878

[7] Kutybayeva, Razaque A, Rai HM (2025) Enhancing Pharmaceutical Supply Chain Transparency and Security with Blockchain and Big Data Integration. *Procedia Computer Science* 259:1511-1522. https://doi.org/10.1016/j.procs.2025.04.106

[8] Wang Q, Lau RYK, Si YW, Xie H, Tao X (2023) Blockchain-enhanced smart contract for Cost-Effective insurance claims processing. *Journal of Global Information Management (JGIM) 31*(7):1-21. https://doi.org/10.4018/JGIM.329927

[9] Houtan B, Hafid AS, Makrakis D (2020) A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access*, 8:90478-90494. https://doi.org/10.1109/ACCESS.2020.2994090

[10] Azaria A, Ekblaw A, Vieira T, Lippman A (2016) MedRec: Using blockchain for medical data access and permission management. Permission Management. *2nd International Conference on Open and Big Data (OBD),* (IEEE, Vienna, Austria), pp. 25-30). IEEE. https://doi.org/10.1109/OBD.2016.11

[11] Ellouze F, Fersi G, Jmaiel M (2020) Blockchain for Internet of Medical Things: A Technical Review. *The Impact of Digital Technologies on Smart Homes and Public Health Telematics* (*in Developed and Developing Countries (ICOST),* (Springer, Hammamet, Tunisia), pp. 259-267. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-51517-1_22

[12] Hang L, Chen C, Zhang L, Yang J (2022) Blockchain for applications of clinical trials: Taxonomy, challenges, and future directions. *IET Communications*, *16*(20):2371-2393. https://doi.org/10.1049/cmu2.12488

[13] Alkaabi N, Salah K, Jayaraman R, Arshad J, Omar M (2020) Blockchain-based traceability and management for additive manufacturing. *IEEE Access* 8:188363-188377. https://doi.org/10.1109/ACCESS.2020.3031536

[14] Afanasev MY, Fedosov YV, Krylova A, Shorokhov AA, (2018) An application of blockchain and smart contracts for machine-to-machine communications in cyber-physical production systems. *2018 IEEE Industrial Cyber-Physical Systems (ICPS),* (IEEE, St. Petersburg, Russia), pp. 13-19. IEEE. https://doi.org/10.1109/ICPHYS.2018.8387630

[15] Hasan M, Starly B (2020) Decentralized cloud manufacturing-as-a-service (CMaaS) platform architecture with configurable digital assets. *Journal of manufacturing systems*, *56*:157-174. https://doi.org/10.1016/j.jmsy.2020.05.017

[16] Tuladhar A, Rogerson M, Engelhart J, Parry GC, Altrichter B (2024) Blockchain for compliance: an information processing case study of mandatory supply chain transparency in conflict minerals sourcing. *Supply Chain Management: An International Journal*, *29*(4):755-777. https://doi.org/10.1108/SCM-11-2023-0585

[17] Suhail S, Hussain R, Jurdak R, Oracevic A, Salah K, Hong CS, Matulevičius R (2022) Blockchain-Based Digital Twins: Research Trends, Issues, and Future Challenges. *ACM Computing Surveys (CSUR)*, *54*(11s):1-34. https://doi.org/10.1145/3517189

[18] Vishwakarma AK, Patro PK, Acquaye A, Jayaraman R, Salah K (2026) Blockchain-based peer-to-peer renewable energy trading and traceability of transmission and distribution losses. *Journal of the Operational Research Society*, 77(1):85-107. https://doi.org/10.1080/01605682.2024.2441224

[19] Danish SM, Zhang K, Amara F, Cepeda JCO, Vasquez LFR, Marynowski T (2024) Blockchain for Energy Credits and Certificates: A Comprehensive Review. *IEEE Transactions on Sustainable Computing*, *9*(5):727-739. https://doi.org/10.1109/TSUSC.2024.3366502

[20] Waseem M, Adnan Khan M, Goudarzi A, Fahad S, Sajjad IA, Siano P (2023) Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. *Energies*, *16*(2):820. https://doi.org/10.3390/en16020820

[21] Milne A, Ransome O (2024) Payment 'Tokens': A Route to Optimizing Liquidity Management? *SWIFT Institute Working Paper* 2024-001. http://dx.doi.org/10.2139/ssrn.4823807http://doi.org/10.2139/ssrn.4823807

[22] de Andrade Simões MP, Cavalcanti JA, de Melo JFM, Reis CQ (2021) Benefits of Using Blockchain Technology as an Accounting Auditing Instrument. REVISTA AMBIENTE CONTÁBIL-Universidade Federal do Rio Grande do Norte-ISSN 2176-9036, *Revista Ambiente Contábil* 13(1):39-53. https://doi.org/10.21680/2176-9036.2021v13n1ID23626

[23] Abdennadher S, Cheffi W, Amin AHM, Naveed M (2024) Performance analysis of a blockchain process modeling: Application of distributed ledger technology in trading, clearing and settlement processes. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(3):100348. https://doi.org/10.1016/j.joitmc.2024.100348

[24] Cyrus R (2023) Custody, Provenance, and Reporting of Blockchain and Cryptoassets. *The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges*, eds. Baker HK, Benedetti H, Nikbakht E, Stein Smith S (Emerald Publishing Limited, Bingley, UK), Chapter 16, pp. 233-248. https://doi.org/10.1108/978-1-80455-320-620221016

[25] The MITRE Corporation (2019) Assessing the Potential to Improve Grants Management Using Blockchain Technology. Available at https://www.mitre.org/sites/default/files/2021-11/prs-19-1654-MITRE-grants-mgt-blockchain-study-report.pdf

[26] Nwangele CR, Adewuyi A, Ajuwon A, Akintobi A (2021) Advancements in real-time payment systems: Advancements in Real-Time Payment Systems: A Review of Blockchain and AI Integration for Financial Operations. *IRE Journals*, *4*(8):206-221. Available at https://www.irejournals.com/paper-details/1708928

[27] Kim S (2020) Fractional ownership, democratization and bubble formation-the impact of blockchain enabled asset tokenization. *Press, Journal Pre-Proof*. https://doi.org/10.1016/j.knosys.2026.115631

[28] Qi-Long C, Rong-Hua Y, Fei-Long L (2019) A blockchain-based housing rental system. *Proceedings of the International Conference on Advances in Computer Technology, Information Science and Communications (CTISC)*, pp. 184-190. https://doi.org/10.5220/0008097201840190

[29] Stančić H, Bralić V (2021) Digital Archives Relying on Blockchain: Overcoming the Limitations of Data Immutability. *Computers*, *10*(8):91. https://doi.org/10.3390/computers10080091

[30] CertiK (2025) *Skynet Hak3d: The Web3 Security Report 2025*. Available at https://www.certik.com/blog/hack3d-the-web3-security-report-2025

[31] Chainalysis (2025) *North Korea Drives Record $2 Billion Crypto Theft Year, Pushing All-Time Total to $6.75 Billion*. Available at https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/

[32] Benke R (2026) *Year in Review: The Biggest DeFi Hacks of 2025*. Available at https://www.halborn.com/blog/post/year-in-review-the-biggest-defi-hacks-of-2025

[33] Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens, Executive Order 14390 (2026)

[34] United States Department of the Treasury (2026). *Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets*. Available at: https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf

[35] Mohammad P, Yixing L, Harfoush K, Jawad M (2025) Denial-of-Service Attacks on Permissioned Blockchains: A Practical Study. *Journal of Cybersecurity and Privacy* 5(3):39. https://doi.org/10.3390/jcp5030039

[36] Coinbase (2026) *Is quantum computing a threat for crypto?* Available at: https://www.coinbase.com/learn/crypto-basics/is-quantum-computing-a-threat-for-crypto

[37] Pascoe C, Quinn S, Scarfone K (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Papers (CSWP) 29. https://doi.org/10.6028/NIST.CSWP.29

[38] Booth H, Ogata M, Kent K, Souppaya M, Dodson D (2025) Secure Software Development Framework (SSDF) Version 1.2: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-218r1 ipd. https://doi.org/10.6028/NIST.SP.800-218r1.ipd

[39] Teixeira D'Aguiar Norton Brandao L, Peralta R (2026) NIST First Call for Multi-Party Threshold Schemes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal Report (NISTIR) 8214C. https://doi.org/10.6028/NIST.IR.8214C

[40] Temoshok D, Choong YY, Galluzzo R, LaSalle M, Regenscheid A, Proud-Madruga D, Gupta S, Lefkovitz N (2025) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-4. https://doi.org/10.6028/NIST.SP.800-63-4

[41] Rose S, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207

[42] Souppaya M, Barker WC, Fisher W, Scarfone K (2025) Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal Report (NISTIR) 8374r1 ipd. https://doi.org/10.6028/NIST.IR.8374r1.ipd

[43] National Institute of Standards and Technology (2025) *Post-Quantum Cryptography*. Available at https://csrc.nist.gov/projects/post-quantum-cryptography

[44] Choong Y, Fisher W, Galluzzo R, Ajmo J, Brown C, Umarji S, Nadeau E, Flanagan H (2026). Digital Identities – Mobile Driver's License (mDL): Accelerating Development and Adoption of Digital Identity for Financial Institutions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-42A (IPD). https://www.nccoe.nist.gov/sites/default/files/2026-03/nist-sp-1800-42a-ipd_0.pdf

[45] International Organization for Standardization (2024) *ISO 22739:2024 - Blockchain and distributed ledger technologies - Vocabulary*. Available at https://www.iso.org/standard/82208.html

[46] International Organization for Standardization (2021) *ISO/TS 23258:2021 - Blockchain and distributed ledger technologies - Taxonomy and Ontology*. Available at https://www.iso.org/standard/75094.html

[47] International Organization for Standardization (2022) *ISO 23257:2022 - Blockchain and distributed ledger technologies - Reference architecture*. Available at https://www.iso.org/standard/75093.html

[48] International Organization for Standardization (n.d.) *ISO/WD 24875-1.2 - Smart contract security - Part 1: Secure development*. Available at https://www.iso.org/standard/88313.html

[49] International Organization for Standardization (n.d.) *ISO/WD 24876 - Blockchain and distributed ledger technologies - Privacy protection when involving trust anchors in DLT-based identity management*. Available at https://www.iso.org/standard/88314.html

[50] International Organization for Standardization (n.d.) *ISO/DIS 24946 - Blockchain and distributed ledger technologies - Requirements and guidance for establishing, improving, preserving, and assessing the privacy capability of DLT systems*. Available at https://www.iso.org/standard/88614.html

[51] International Organization for Standardization (2022) *ISO/TS 23635:2022 - Blockchain and distributed ledger technologies - Guidelines for governance*. Available at https://www.iso.org/standard/76480.html

[52] International Organization for Standardization (n.d.) *ISO/AWI TS 25481 - Governance for DAOs in Blockchain and DLT*. Available at https://www.iso.org/standard/90514.html

[53] International Organization for Standardization (n.d.) *ISO/AWI PAS 26347 - Interoperable protocol between digital wallets based on blockchain and DLT*. Available at https://www.iso.org/standard/93265.html

[54] International Organization for Standardization (n.d.*) ISO/CD PAS 26348 - Blockchain and distributed ledger technologies - Cybersecurity Information Sharing and Utilization Framework for the blockchain ecosystem*. Available at https://www.iso.org/standard/93266.html

[55] International Organization for Standardization (2025). *ISO/IEC TS 18013-7:2025 Personal identification — ISO-compliant driving licence Part 7: Mobile driving licence (mDL) add-on functions*. Available at: https://www.iso.org/standard/91154.html

[56] AICPA Assurance Services Executive Committee (2022) *2018 SOC 2® Description Criteria (With Revised Implementation Guidance – 2022)*. Available at

https://www.aicpa-cima.com/resources/download/get-description-criteria-for-your-organizations-soc-2-r-report

[57] Institute of Electrical and Electronics Engineers (2023) *IEEE 3205-2023 – IEEE Standard for Blockchain Interoperability Data Authentication and Communication Protocol*. Available at https://standards.ieee.org/ieee/3205/10237/

[58] Internet Engineering Task Force (2019) *RFC 8578 – Deterministic Networking Use Cases*. Available at https://datatracker.ietf.org/doc/rfc8578/

[59] World Wide Web Consortium (2021) *Web Authentication: An API for Accessing Public Key Credentials Level 2*. Available at https://www.w3.org/TR/webauthn-2/

[60] World Wide Web Consortium (2026) *Web Authentication: An API for Accessing Public Key Credentials Level 3*. Available at https://www.w3.org/TR/webauthn-3/

[61] Fido Alliance (2026) *Specifications*. Available at https://fidoalliance.org/specifications-overview/

[62] World Wide Web Consortium (2025) *Verifiable Credentials Data Model v2.0*. Available at https://www.w3.org/TR/vc-data-model-2.0/

[63] OpenID Foundation (2025) *OpenID for Verifiable Presentation 1.0*. Available at https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[64] OpenID Foundation (2025) *OpenID for Verifiable Credential Issuance 1.0*. Available at https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[65] Government Blockchain Association (2023) *Blockchain Maturity Model*. Available at https://gbaglobal.org/blockchain-maturity-model/

[66] Blockchain Security Standards Council (2025) *Node Operation Standard, version 1*. Available at https://specs.blockchainssc.org/nos/

[67] Blockchain Security Standards Council (2025) *Token Integration Standard, version 1*. Available at https://specs.blockchainssc.org/tis/

[68] Blockchain Security Standards Council (2025) *Key Management Standard, version 1*. Available at https://specs.blockchainssc.org/kms/

[69] Blockchain Security Standards Council (2025) *General Security and Privacy Guidelines, version 1*. Available at https://specs.blockchainssc.org/gsp/

[70]Global Blockchain Business Council (2026) *Global Standards Mapping Initiative 6.0: Technical Standards*. Available at: https://images.ctfassets.net/so75yocayyva/4iJhn03ZUJjsTdcKp4FjHA/186abb11589d68cf3c7e696c2ee6252a/Technical_Standards_-_GSMI_6.0.pdf