Blockchain Standards for Compliance and Trust

Ashiq Anjum
University of Derby

Manu Sporny
Digital Bazaar

Alan Sill
Texas Tech University

Cryptocurrency applications of distributed ledger methods such as blockchains are now well established, but their implications for more general topics are just beginning to be appreciated. Beyond applications in finance and banking, new applications are emerging in supply chain management, manufacturing, agricultural product tracking, advertising verification, Internet of Things, healthcare, and the pharmaceutical industry, among others.

This column will explore current and open topics for trust, verification, compliance, and security in distributed environments with a specific focus on the current status of standards efforts related to blockchain technologies.

Distributed Trust

The idea of a completely stand-alone, autonomous, self-contained, self-validating application that does not depend on either immediate or eventual network communication is becoming nearly unthinkable. In the past, keeping something secure usually depended on providing it with isolated defenses, such as placing it in a physical safe or otherwise isolating it from external access. This approach is still a component of some forms of electronic security, such as offline hardware cryptographic modules for certificate authorities, but blockchain methods depend, in contrast, on the idea of independent open verification rather than isolated operation.

Distributed methods carry the advantage of being useful in multiple, physically separated settings, but require the existence of methods to determine that a given transaction is complete. Blockchains have become popular precisely because they provide noncentralized, independently verifiable capabilities to ensure the integrity and consistency of distributed ledgers and the associated transactions.

EDITOR
ALAN SILL
Texas Tech University
alan.sill@standards-now.org

Key Success Factors

One factor that drives the interest in distributed ledger-based methods is the ease with which they can be added to existing workflows and data processing lifecycles. This consideration may be more important, in the long run, than the current emphasis on inventing entirely new business models based on such methods.

Key success factors, in this view, for the use of distributed ledger technologies basically boil down

2325-6095/17/$33.00 © 2017 IEEE

Many Different Types of Blockchains

Principle	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
Confidentiality	None	None	None	Hash-based content addresses	None	None
Information availability	Block mirroring	Block mirroring	Ledger mirroring	Graph and file mirroring	Block mirroring/ DHT mirroring	Hashgraph/ mirroring; Optional Event History
Integrity	Multiple block verifications	Multiple block verifications	Latest block verification	Hash-based content addressing	Multiple block verifications	Consensus with probability one
Non repudiation	Digital signatures	Digital signatures	Digital signatures	Digital signatures	Digital signatures	Digital signatures
Provenance	Transaction inputs/outputs	Ethereum state machine and transition functions	Digitaly signed ledger transition instructions	Digital signatures and versioning	Transaction inputs & outputs and virtual chain references	Hashgraph/ mirroring; Optional Event History
Pseudonymity	Public keys	Public keys and contract addresses	Public keys	Public keys	Public keys, but public information encouraged	Not supported; could be layered
Selective disclosure	None	None	None	None	Selective access to encrypted storage	Not supported; could be layered

FIGURE 1. Blockchain information security principle analysis.

to whether the introduction of such methods will solve particular problems without requiring the addition of entirely new business models and can be incorporated into existing processes.

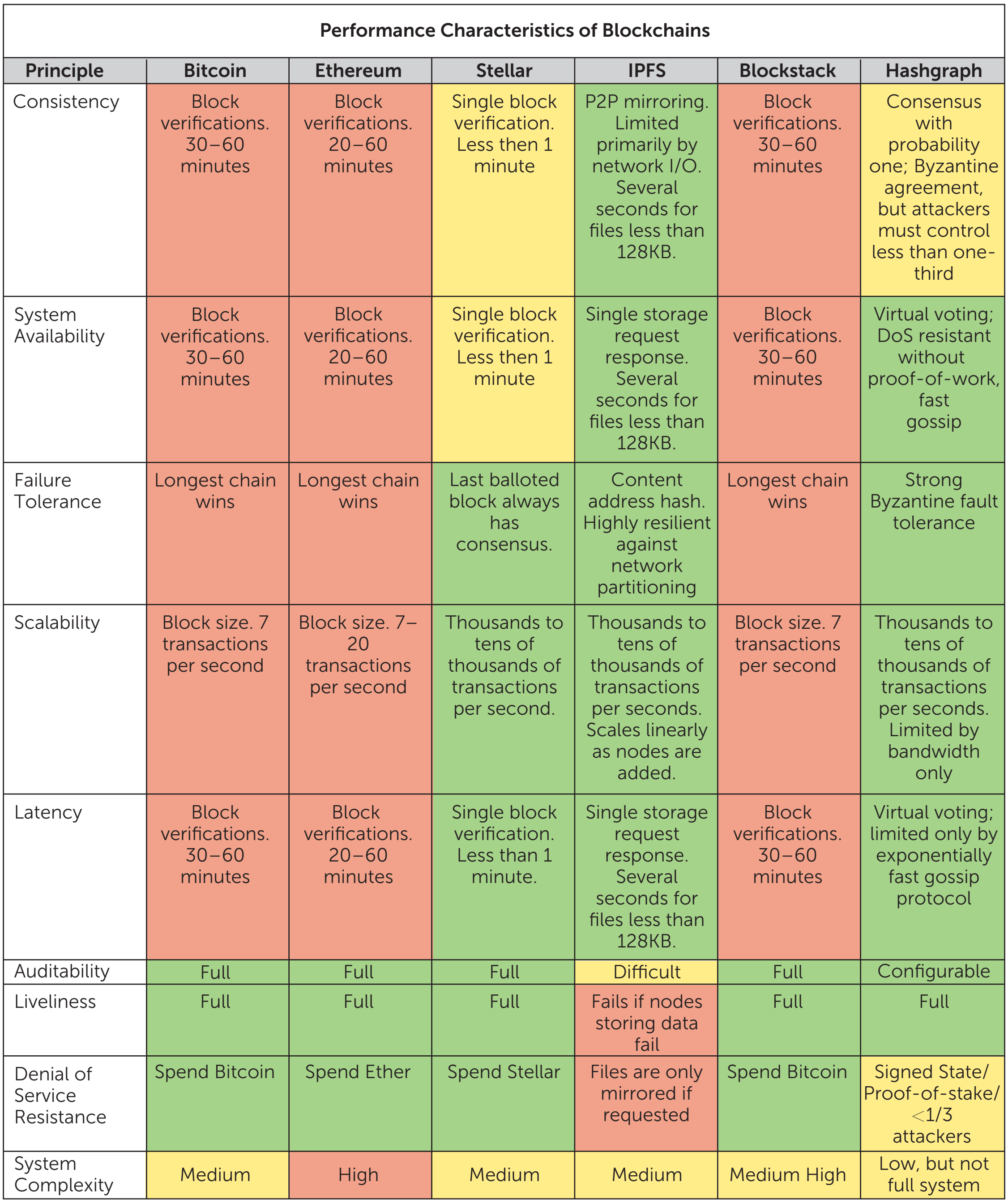
Blockchain Types and Performance Characteristics

By now, many different blockchain approaches have been documented, and an increasing number of them are beginning to receive significant use. Figure 1 documents different blockchain approaches and how capable they are at achieving traditional information security principles.[1]

Not all of these perform in the same way on a given usage pattern. Some are more suited to particular types of operation than others. Figure 2 highlights some of the primary performance characteristics of several different types of blockchains.[1]

Beyond the generally-applicable types of blockchains explored in these figures, an increasingly wide range of specialized distributed ledger technologies has emerged focused on specialized fields of application. Although some have argued that this represents a foundational shift in technology, our belief is that, just like the web itself, this represents the applicability of blockchain techniques to solve problems in a way that adds to, rather than replaces, existing business, scientific, record-keeping, and audit trail logging use cases.[2]

To make a true leap to a status that could in fact be revolutionary, international standards will have to be developed simultaneously across a wide range of needs, as outlined in these tables; or alternatively, developed in a way that will allow their characteristics to be mixed and matched seamlessly depending on the application area. Much work is going on in pursuit of such approaches.



Performance Characteristics of Blockchains

Principle	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
Consistency	Block verifications. 30–60 minutes	Block verifications. 20–60 minutes	Single block verification. Less then 1 minute	P2P mirroring. Limited primarily by network I/O. Several seconds for files less than 128KB.	Block verifications. 30–60 minutes	Consensus with probability one; Byzantine agreement, but attackers must control less than one-third
System Availability	Block verifications. 30–60 minutes	Block verifications. 20–60 minutes	Single block verification. Less then 1 minute	Single storage request response. Several seconds for files less than 128KB.	Block verifications. 30–60 minutes	Virtual voting; DoS resistant without proof-of-work, fast gossip
Failure Tolerance	Longest chain wins	Longest chain wins	Last balloted block always has consensus.	Content address hash. Highly resilient against network partitioning	Longest chain wins	Strong Byzantine fault tolerance
Scalability	Block size. 7 transactions per second	Block size. 7–20 transactions per second	Thousands to tens of thousands of transactions per second.	Thousands to tens of thousands of transactions per seconds. Scales linearly as nodes are added.	Block size. 7 transactions per second	Thousands to tens of thousands of transactions per seconds. Limited by bandwidth only
Latency	Block verifications. 30–60 minutes	Block verifications. 20–60 minutes	Single block verification. Less than 1 minute.	Single storage request response. Several seconds for files less than 128KB.	Block verifications. 30–60 minutes	Virtual voting; limited only by exponentially fast gossip protocol
Auditability	Full	Full	Full	Difficult	Full	Configurable
Liveliness	Full	Full	Full	Fails if nodes storing data fail	Full	Full
Denial of Service Resistance	Spend Bitcoin	Spend Ether	Spend Stellar	Files are only mirrored if requested	Spend Bitcoin	Signed State/ Proof-of-stake/ <1/3 attackers
System Complexity	Medium	High	Medium	Medium	Medium High	Low, but not full system

FIGURE 2. Blockchain performance characteristics analysis.

Compliance Using Blockchains

Consider the example of providing RFID tags to parts to enable tracking them through a supply chain. While it is easy to register unique tags to each part, even for items produced at large volumes, nothing prevents a given registry tag from being assigned to more than one such part, or the introduction of other tags that either intentionally or accidentally duplicate such information.

Some might argue that distributed ledgers can entirely replace physical tags and labels, but we believe that there is an overlap between these technologies. There are definitely situations in which human- or machine-readable labels are valuable, or even essential. With the addition of a digital signature and incorporation of that signature into a blockchain, such tags can be checked easily with respect to their authenticity and uniqueness. Counterfeit parts can be excluded, and accidental duplications eliminated, through this method. Such approaches can also be applied to any sort of record management to ensure tamper resistance and authenticity of business records.[3]

Some transactions, however, are too small or otherwise unsuited to affixing physical human- or machine-readable labels, such as bar codes or RFID tags. Furthermore, such physical labels do not themselves permit recording of associated data, such as temperature or shock protection handling records during shipment. Blockchain methods can be added readily to verify the association of such records with food or parts during shipment at extremely low costs once the basic distributed ledger methods are in place.

Advertising verification is another area in which adding trust and compliance to existing business models can enhance value. In addition to the direct use case of allowing billing verification through shared ledgers, blockchain methods can also be applied directly during generation of the advertising impressions to ensure their authenticity and uniqueness. In this way, fake views, spoofed domains, and other mechanisms for advertising fraud can be avoided.[4] The adChain Registry (https://adtoken.com/uploads/white-paper.pdf) provides an example of a decentrally-owned domain whitelist being launched as a collaboration of industry groups. The adChain Registry is a smart contract on the Ethereum blockchain which stores domain names accredited as nonfraudulent by participants.

Blockchains for Recordkeeping

Since many applications of blockchain technology beyond cryptocurrency relate strongly to recordkeeping, existing standards on information and records management are applicable and provide a good basis for extrapolation. A good review of this aspect of blockchain applications is contained in the article by Lemieux, which summarizes previous applicable recordkeeping standards and also points out some limitations inherent in overdependence on distributed ledger technologies for record-keeping.[5]

It is worth remembering that most ledgers function by storing and cryptographically signing hashes associated with information and transactions, and do not necessarily contain the primary information being recorded. While there are ledger standards under development to store information directly in the blockchain, such as the Web Ledger Protocol (https://w3c.github.io/web-ledger/), many existing blockchains require additional layers and long-term repositories to allow blockchain signing to function efficiently as part of recordkeeping systems.

Current State of Standards

Applications of blockchain methods are growing rapidly due to the considerations just mentioned. As with any rapidly developing field, there has been a chorus of calls for standardization of associated terminology and technologies to optimize interoperability and usefulness of these methods.

The decision to pursue development of standards depends strongly on whether they will simplify the field by producing an overlap among multiple suppliers, particularly in a way that promotes creation of markets. Conditions under which standards can be expected to contribute usefully to developing areas of technology can be characterized and quantified.[6] Strong bidirectional feedback and communication between application user communities and the organizations developing the standards are also crucial.[7]

Items that could be targets for further standardization include the following:[8]

- Basic data models for Blockchain (Blocks, Events, and State Machine)
- Consensus algorithms (Proof of Work, Stellar Consensus, Hashgraph)
- Storage algorithms (Merkle Trees, MerklePatriciaTries, Linked Lists)
- Signature algorithms (JOSE Web Signing, Linked Data Signatures, Hierarchically Deterministic Keys, Chainpoint)
- Web-based access protocols (Create, Read, Add, Get Status, Query)

The World Wide Web Consortium (W3C; https://www.w3.org) held a workshop in June 2016 to examine aspects of blockchains that relate to Web technologies, and identify specific technologies mature enough to consider for standardization. After issuing a report, it has formed a number of new groups to address these topics including the following:[9]

- Credentials Community Group (https://www.w3.org/community/credentials/)
- Digital Verification Community Group (https://w3c-dvcg.github.io/)
- Blockchain Community Group (https://www.w3.org/community/blockchain/)
- Verifiable Claims Working Group (https://www.w3.org/2017/vc/), and
- Interledger Community Group (https://www.w3.org/community/interledger/)

The W3C's Web Ledger Protocol (https://w3c.github.io/web-ledger/), which is a work in incubation at W3C, was recently the recipient of a Small Business Innovative Research project award from the US Department of Homeland Security's Science and Technology Directorate.[10]

The International Organization for Standardization (ISO; https://www.iso.org/) has also recently launched a technical committee (TC) 307 on blockchain and distributed ledger technologies (https://www.iso.org/committee/6266604.html) with liaisons with several other ISO committees and other relevant standards developing organizations. This effort was originally proposed by Standards Australia, which published a roadmap for blockchain standards in March 2017.[11]

The new ISO TC 307 has established working groups on a reference architecture, taxonomy, and ontology (SG 1), use cases (SG 2), security and privacy (SG 3), identity (SG 4), and smart contracts (SG 5), but has so far deferred the potentially more challenging work on establishing standards for governance, auditing, or interoperability of these technologies.

The standardization sector of the International Telecommunications Union (ITU-T; https://www.itu.int) has established a focus group on distributed ledger technology (FG DLT; https://www.itu.int/en/ITU-T/focusgroups/dlt/). According to its charter, this group will develop a standardization roadmap for interoperable DLT-based services, taking into consideration the activities underway in ITU, other standards developing organizations, forums, and groups.

Other major formal standards developing organizations active in promoting DLT standards include the IEEE, which has formed a blockchain member interest group to coordinate and disseminate information on activities in this area (http://blockchain.ieee.org), and the Society for Worldwide Interbank Financial Telecommunication (SWIFT; https://www.swift.com), which has recently expanded its activities in this area to work with several related industry organizations.

There is already considerable coordination among these efforts. The ISO TC 307 has formal liaisons with ITU-T, SWIFT, and other interested parties, for example, and liaisons from the ISO and W3C Blockchain work recently met at a US Federal Reserve Secure Payments Task Force meeting to discuss aligning the initiatives at each organization as the work progresses.

Industry, Trade, and Community Organizations

As has been discussed in several previous Standards Now columns, some of the most effective work in creation, development, and curation of cloud standards continues to be accomplished by the direct formation of industry, trade, and community organizations that are not otherwise based in formal standards developing organizations. These are distinguished from the work of formal standards organizations by the fact that they are often accompanied by repositories of open source implementation code. Bitcoin itself is based on a series of standard specifications developed and maintained by its own community through a process called Bitcoin Improvement Proposals (https://github.com/bitcoin/bips).

Other organizations have emerged to pursue goals for distributed ledger technologies that are independent from the Bitcoin community. The Cloud Standards Customer Council, for example, has produced a document summarizing the exiting needs from a business perspective, and offering a reference architecture that could be used in further standardization efforts.[12]

As an example of community responses to these needs, the HyperLedger collaboration (https://www.hyperledger.org), hosted by The Linux Foundation, currently has more than 120 supporting industry members and a governance model that allows for community participation. It supports projects spanning a range of business blockchain technologies, including distributed ledger frameworks, smart contract engines, client libraries, graphical interfaces, utility libraries, and sample applications. The OpenChain project (https://www.openchain.org) and related Open Assets Protocol (www.openassets.org/) supports specifications available at https://github.com/openchain/docs and https://github.com/OpenAssets/open-assets-protocol that are aimed to support and manage user-created assets. Each of these projects supports both community-based specification development and repositories of open-source implementation code.

Future Directions

Despite initial successful uptake, current blockchain methods exhibit gaps and limitations in areas related to scalability, flexibility, and governance. The architectural choices made by currently available products favor security and data integrity over scalability and flexibility. For example, most Bitcoin-based systems cannot process more than seven transactions per second. These limitations in the technology have led to a number of specialized platforms—we've counted 70 so far—that have emerged to address problems in specific sectors and application domains. Clearly, standardization activity will be required to enable these technologies to be interoperable.

Improvements addressing confidentiality, strong identity, and collaboration between the blockchain network participants will be required in near future. Smart contracts will very likely soon lead to programmable blockchains, and associated standards and tools will be required for developing, debugging, monitoring, and managing smart contract systems.

A recent comparison of the performance of blockchains based on Ethereum, Parity, and Hyperledger has been carried out by researchers at the National University of Singapore.[13] This work introduces a publicly available tool called BlockBench (https://github.com/ooibc88/blockbench/) designed to measure data processing performance at different layers of the blockchain stack using evaluation metrics related to throughput, latency, scalability, and fault tolerance. Such tools and other related work are examples of efforts that can build on the analyses we have presented here.

This discussion only represents our own viewpoints. Given space limitations in this column, it only scratches the surface of a very large field, concentrating on the most recent standards activity. We are open to other opinions and experience in this area and are sure that readers of the magazine would also appreciate any additional article submissions or information on this topic.

The magazine is open to input on this or previous columns. Please include news you think the community should know about in the general areas of cloud standards, compliance, or related topics. Ideas for potential submissions to the magazine or for proposed guest columns can be sent to alan.sill@standards-now.org.

Acknowledgments

Portions of this article are based on work performed with funding from the US National Science Foundation's Cloud and Autonomic Computing Center under award number 1362134. Other portions are based on work that was performed by Digital Bazaar, which has been funded in part by the US Department of Homeland Security's Science and Technology Directorate under contracts HSHQDC-16-C-00058 and HSHQDC-17-C-00019. The content of this article does not necessarily reflect the position or the policy of the US Government and no official endorsement should be inferred.

References

1. M. Sporny, "Building Better Blockchains: Linked Data in Distributed Ledgers," *Proc. 26th Int'l Conf. World Wide Web Companion*, Apr. 3–7, 2017, p. 1429; doi:10.1145/3041021.3053899.
2. M. Iansiti and K. R. Lakhani, "The Truth About Blockchain," *Harvard Business Review*, Jan.–Feb. 2017, pp. 118–127;https://hbr.org/2017/01/the-truth-about-blockchain.
3. K. O'Marah, "Blockchain for Supply Chain: Enormous Potential Down the Road," *Forbes*, Mar. 9, 2017; https://www.forbes.com/sites/kevinomarah/2017/03/09/blockchain-for-supply-chain-enormous-potential-down-the-road/.
4. "MetaX and DMA Provide Blockchain Solution for Digital Advertising," *Chain Finance*, June 13, 2017; https://blockchain-finance.com/2017/06/13/metax-and-dma-provide-blockchain-solution-for-digital-advertising/.
5. V.L. Lemieux, "Trusting Records: Is Blockchain Technology the Answer?" *Records Management Journal*, vol. 26, no. 2, pp. 110–139; https://doi.org/10.1108/RMJ-12-2015-0042.
6. A. Sill, "Socioeconomics of Cloud Standards," *IEEE Cloud Computing*, vol. 2, no. 3, July 15, 2015, pp. 8–11; doi:10.1109/MCC.2015.59.
7. A. Sill, "Forecasting Cloud Standards Success Patterns," *IEEE Cloud Computing*, vol. 4, no. 1, Mar. 15, 2017, pp. 56–60; doi:10.1109/MCC.2017.3.
8. M. Sporny, "A Web-Based Ledger Data Model and Format"; https://www.w3.org/2016/04/blockchain-workshop/slides/Sporny-Blockchains-The_Bits_That_Could_Be_Standardized.pdf.
9. World Wide Web Consortium, "Blockchains and the Web Report: A W3C Workshop on Distributed Ledgers on the Web," June 29–30, 2016; https://www.w3.org/2016/04/blockchain-workshop/report.html.
10. S. Higgins, "US Government Awards $2.25 Million to Blockchain Research Projects," *CoinDesk*, May 12, 2017; http://www.coindesk.com/us-government-awards-2-25-million-blockchain-research-projects.
11. Standards Australia, "Roadmap for Blockchain Standards," Mar. 2017; http://www.standards.org.au/OurOrganisation/News/Documents/Roadmap_for_Blockchain_Standards_report.pdf.
12. Cloud Standards Customer Council, "Cloud Customer Architecture for Blockchain." July 2017, http://www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-Blockchain.pdf.
13. T.T.A. Dinh et al., "BLOCKBENCH: A Framework for Analyzing Private Blockchains," *Proceedings of the 2017 ACM International Conference on Management of Data* (SIGMOD'17), pp. 1085–1100, http://dx.doi.org/10.1145/3035918.3064033.

ASHIQ ANJUM *is professor of distributed systems in the School of Computing and Mathematics at the University of Derby. His areas of research include*

distributed and parallel systems (including high performance computing, grid, and cloud computing), distributed toperating systems, and scalable methods to mine large and complex datasets. He has worked on a variety of research projects dealing with resource management of large scale systems, performance monitoring and optimization, data mining and service orchestration, and works closely with industry on applications of these topics. His current projects include working with a leading Pharma company to develop a large scale clinical trial management system across distributed data centers to optimize drug discovery while reducing operational costs, and on machine learning algorithms for processing of video streams in a cloud environment for security and surveillance purposes.

MANU SPORNY *is founder and CEO of Digital Bazaar, Inc. He has founded or helped start six software technology startups. He is cocreator of the JSON-LD, Linked Data Signatures, and Verifiable Claims standards and the Flex Ledger Protocol. He spends most of his time creating open standards and open technology that will integrate payments, identity, and blockchain into the core architecture of the Web.*

ALAN SILL *is senior director of the High Performance Computing Center and adjunct professor of physics at Texas Tech University. He codirects the US National Science Foundation's multiuniversity "Cloud and Autonomic Computing" industry/university cooperative research center, and holds a position as visiting professor of distributed computing at the University of Derby. Sill has a PhD in physics from American University and extensive experience in large-scale scientific computing. He serves as president for the Open Grid Forum and is an active member of the IEEE, the Distributed Management Task Force, and other cloud standards working groups, as well as national and international computing standards roadmap committees. For further details, visit http://nsfcac.org or contact him at alan.sill@standards-now.org.*