THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Print: 2516-3949
doi: 10.31585/jbba-1-1-(11)2018

A Future History of International Blockchain Standards

David Hyland-Wood[1] and Shahan Khatchadourian[2]
[1] School of Information Technology and Electrical Engineering, The University of Queensland, St. Lucia 4067, Queensland, Australia
[2] ConsenSys AG, Zug 6300, Switzerland
Correspondence: d.hylandwood@uq.edu.au
Received: 29 May 2018 **Accepted:** 14 June 2018 **Published:** 29 June 2018

Abstract
Blockchain and blockchain-related technologies are being rapidly invented to the point that it is difficult to define specifically which properties are necessary to constitute a blockchain. It may therefore seem far too early to meaningfully discuss the creation of international blockchain standards. This article will argue the opposite by summarizing some existing international standards work related to blockchains and propose directions for additional standards development that could meaningfully be explored in the near future without negatively impacting additional invention.
Keywords: *Blockchain, distributed ledger, standards, consensus, decentralisation, interoperability, identifiers, BPMN, enterprise systems.*

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
DH-W [1] & SK [2] designed and coordinated this research and prepared the manuscript in entirety.

Funding:
Funding is provided by ConsenSys.

Acknowledgements:
DH-W [1] & SK [2] acknowledges Vanessa Bridge, Robert Coote, Matt Halpern, Grant Noble, and Peter Robinson of ConsenSys AB, and Mariano P. Consens of The University of Toronto, and Marius Portmann of The University of Queensland for their feedback and suggestions on this paper.

Introduction

Any new technological paradigm wherein implementations have similar or overlapping functionality by many vendors has historically seen vendor cooperation via international standards development organizations (SDOs). We categorize international standards into two broad areas. Backward-looking standards formalize existing de facto implementations into a specification, e.g. ECMAScript (ISO 2018). Forward-looking standards fill gaps between black-box implementations by creating a specification that defines how such different systems may communicate, generally for the purpose of assisting interoperability, which we consider to be communications between systems that are "liberal in what you accept, and conservative in what you send" (Braden 1987). Recent and obvious examples include the development of international standards defining the World Wide Web, e.g. HTTP (Fielding et al. 1999), URL (Berners-Lee, Fielding, and Masinter 2005), HTML (Faulkner, Eicholz, Leithead, Danilo, and Moon 2017), the Internet and the TCP/IP (Braden 1987) family of protocols that includes its OSI (ISO 1994) conceptual abstraction and application-level protocols such as DNS (Mockapetris 1997), as well as other industry standards like relational databases, e.g., SQL (ISO 2016), and mobile telephones, e.g., GSM (3GPP 1999). Each of the mentioned standards began as technical implementations which were later harmonized into international standards as they converged and matured. It seems reasonable to expect blockchain technologies to follow a similar course.

There is little agreement within the blockchain community on the very definition of a blockchain. Ten years ago, Bitcoin (Nakamoto 2008) was the blockchain. Within a few years, others had implemented variations on a theme, some of which added substantial innovations, such as Ethereum's (Buterin 2013, Wood 2014) introduction of a Turing-complete virtual machine for execution of smart contracts (Szabo 1994), a computerized transaction protocol that executes contract terms, which Ethereum enables through algorithmically specifying and autonomously enforcing rules of interaction. After a decade of constant innovation in various (often competing) directions, what exactly is a blockchain?

One reasonable answer is that a blockchain is a public distributed ledger technology (DLT) used for the transfer of cryptocurrencies. That definition certainly matches Bitcoin, although it leaves out later innovations including the flexibility of smart contracts. Many newer blockchains would argue to exclude the word "public" or even the transfer (or existence) of cryptocurrencies. Should the resulting definition then be that a blockchain is a distributed ledger?

We argue not.

Imagine that one wished to create a simple double-entry accounting system in software. Each transaction is entered, a new running total is calculated, and the entire record stored. They might call each record a "block". Each record (or block) is linked (perhaps not even cryptographically) to the previous record. To keep data safe, the transaction is uploaded to a remote machine, which in turn copies it to other machines. They would have made a distributed ledger. Have they made a blockchain? Probably not. Surely blockchains have other intrinsic features such as cryptographically linked blocks to provide the feature of nonrepudiation, atomic commits, and a presumption of a peer relationship between nodes. Some might argue that a common consensus algorithm to determine block additions is also necessary.

In Table 1, we show several blockchains that support a variety of consensus algorithms, including proof of work (PoW), proof of stake (PoS), proof of authority (PoA), as well as byzantine fault tolerant (BFT) variants. Essentially, a consensus algorithm provides an atomic commit capability in which peers on a blockchain network agree on the blockchain network's current state as well as any state updates. Furthermore, consensus algorithms affect how blockchain networks enable peers to engage with each other. In one instance, a public blockchain network, such as Ethereum's public network, intends to provide fair ability for peers of its peer-to-peer network to observe, validate, and participate in blockchain state updates. In private, permissioned settings, as supported by blockchains like Quorum and Hyperledger Fabric, more efficient BFT variants allow higher transaction throughput by restricting scalability in the number of peers actively participating in the consensus algorithm. In providing a range of modular, pluggable consensus algorithms, and with their integration at different layers of what is often seen as a decentralizing technology, it is a challenge to define and distinguish blockchains from their DLT counterparts.

The authors suggest that the current difficulty in defining a blockchain argues strongly against the creation of backward-looking standards. There is as yet simply no agreement as to which features a de facto blockchain possesses, nor is there broad agreement on a reference architecture. Facing such a challenge, it becomes especially important to free blockchains and DLTs from standardization that can impact their future development. We therefore suggest that SDOs do not pursue development of such standards at this time, focusing instead on future standards development.

This article explores areas and directions related to interoperability between different blockchains, between blockchains and blockchain-like technologies, and between blockchains and traditional technologies. A survey of existing and forthcoming standards is presented, and some suggestions made for future standards development.

Methods

In this short paper, we review existing international standards, including those that are related to blockchain technologies, followed by a survey of international standards development organizations to determine current work related to blockchain technologies. The authors then extrapolated informal likelihood of success of various efforts based upon knowledge of both emerging blockchain industry participants and the structure and concerns of standards development organizations. Suggestions for success criteria and likelihoods of success, as well as proposals for future standards efforts, are the conjecture of the authors.

Since SDOs are generally reluctant to develop new technologies, we categorize their activities into two predominant (sometimes opposing) directions: The first is to formally agree to some practices that already have wide adoptions, the so-called industry or de facto standards. The second is to create means to better allow competing interests to interoperate, in particular, the many national and international SDOs allow for standardization adoption at various levels of jurisdictions to address cultural, regional, and legal differences (Fyrigou-Koulouri 2018). It is in this latter area where we suggest the most useful blockchain standards could assist growth in the field.

We propose three areas for future interoperability standards: a representation of smart contracts in BPMN systems to integrate blockchain systems into enterprise modelling systems, decentralized identifiers to facilitate cross-blockchain identity, and interledger protocols to reduce data boundaries between blockchain systems.

Results

In this section, we review several existing and proposed enterprise and blockchain standards and relate them to technologies that we believe play a critical role in the advancement of blockchain standards.

Existing standards are relevant to the goal of interoperability between blockchains while also enabling flexible development of future blockchain technologies. Existing technologies not only allow interoperability between public blockchains, enterprise blockchains, and existing enterprise systems, they also support the extensibility of blockchain standards and their enterprise variants. One example of this arises with companies that are looking to integrate decentralized applications into their current businesses processes. Reasons to do so include cost reduction, increased

transparency, as well as benefiting from novel privacy and security schemes. As an existing standardized enterprise technology, BPMN is well-suited for enabling interoperability between blockchains in a variety of ways. First, BPMN supports interoperability between existing enterprise technologies and blockchain networks using typical approaches to service orchestration and choreography. These approaches are also applicable in the interoperability between public blockchain networks and private, permissioned variants, although their diversity and distinctiveness continue to undergo ongoing community debates (Buterin 2015, Khatchadourian, Lubin, Millar, & Buterin 2017, Ferris 2018, Allison 2018). It is important to note that the use of existing enterprise standards, such as BPMN, does not restrict how blockchains are used nor their future development.

Several forward-looking standards either exist or are in progress. Figure 1 summarizes the Enterprise Ethereum Client Specification version 1.0 developed by the Enterprise Ethereum Alliance (EEA) (Enterprise Ethereum Alliance 2018). As far as the authors are aware, that specification represents the first blockchain standard created and approved by an SDO. The specification was publicly announced on 16 May 2018 and is the sole entry in Table 2, which lists existing blockchain standards.

Standardization efforts known to be being actively pursued at the time of this writing are listed in Table 3.

A list of current exploratory efforts at SDOs is provided in Table 4. It is worth noting that many exploratory efforts are likely to be abandoned prior to standardization. A recent example is the expired effort at the IETF to apply Application-Layer Traffic Optimization techniques to blockchains (Hommes 2017).

Many blockchains have developed implementation-specific APIs to allow applications such as cryptographic wallets and cryptocurrency exchanges to communicate with blockchain nodes. One might be tempted to conclude that standardization of such APIs could be fruitful areas for backward-looking standards development. However, blockchain-specific APIs are unlikely to generalize well across radically different technical implementations. Furthermore, it may be possible to develop general protocols to represent high-level conceptual actions such as data migration, data copying, cryptocurrency exchange or transfer, cross-chain smart contract operations, etc. Generalized protocols are more likely to be standardized than APIs as shown historically by successful standards efforts such as HTTP or the TCP/IP family.

In this section, we described existing blockchain standards that have focused on the interoperability of existing blockchain technologies, as well as ongoing standardization efforts and explorations. In the next section, we discuss the relevance of these standardization efforts with respect to interoperability of future blockchain developments.

Discussion

The International Standards Organization (ISO) is currently the only SDO actively pursuing backward-looking standards development related to blockchains. In an attempt to understand and ground the blockchain space, ISO's TC 307 Technical Committee is defining a reference architecture, taxonomy and ontology. Blockchain-related formal vocabulary is also being collected. As mentioned above, the rapid invention of blockchain types and the lack of an industry-wide agreement on a definition of a blockchain make such work particularly difficult. The authors believe such work to be premature.

A more productive approach is likely to be found by considering standards development in areas with the following properties:

- Pre-competitive or non-competitive areas of interest to blockchain developers and vendors (necessary with SDOs to preclude formal objections from disadvantaged vendors);
- Specifications that seem likely to enhance interoperability between different types of blockchains;
- Activities that would not limit explorations or invention of additional cryptography, privacy, consensus, management, or similar features of any individual blockchain.

We thus conclude that forward-looking interoperability standards are most likely to result in successful standards creation and facilitate industry growth.

We expect blockchain standards to mature in areas that foster interoperability. Apparently fertile areas for standardization would include those efforts that would assist with interoperability between blockchain implementations and between blockchains and established enterprise information systems. In neither area would vendor representatives to SDOs likely see competitive disadvantage.

Examples of work that would foster interoperability between blockchains include decentralized identifiers (Reed et al 2018), being considered for standardization at the W3C, verifiable claims (Burnett et al 2017), a data model and message syntax currently being standardized at the W3C, and various attempts to define interledger protocols. Decentralized identifiers would allow a given user to take coordinated action on multiple blockchains

using a single identity. Verifiable claims take advantage of blockchains' properties of being difficult to write yet simple to read to represent common social claims (including identity). Interledger protocols would facilitate necessary and common operations such as data migration from one blockchain to another, facilitate the creation of smart contracts that operate on information held by multiple blockchains, and allow data held canonically by one blockchain to be readily validated by another.

Two interledger protocols have been proposed: The Interledger Protocol (W3C Interledger Payments Community Group 2018) has been proposed by Ripple to allow cross-blockchain payments. The Web Ledger Protocol (Sporny and Longley 2018) has been proposed by the W3C Blockchain Community Group.

Some existing or upcoming standards efforts would support interledger protocols, such as the W3C's Verifiable Claims and Decentralized Identifiers. A properly specified and widely adopted interledger protocol would benefit from a decentralized identifier scheme to provide common user information across blockchains. The concept of operations of Verifiable Claims would be more easily implemented in an environment where a standard interledger protocol and decentralized identifiers exist and are adopted.

As an existing enterprise standard that is agnostic to blockchains, BPMN has successfully enabled blockchain interoperability in proof of concepts. However, enterprises could gain additional benefits from the consideration of significant blockchain paradigms in BPMN's evolution. For instance, defining new role and activity types based on decentralized identifiers and smart contracts, potentially hosted on one or more decentralized peer-to-peer systems, could help businesses define, model, and validate their processes more easily and accurately.

Table 5 lists suggested areas for potential standardization that have the desired properties.

Conclusions and Further Work

The current state of blockchain standards is both nascent and exploratory. Two existing international SDOs are currently producing blockchain standards (W3C and EEA), and several others are exploring future standards development (ISO, IEEE, IETF, IRTF, and OMG).

Of the SDOs currently pursuing blockchain-related standards development, the authors propose W3C as the best candidate for interledger protocol development if the consortium's membership allow for a broadening of the definition of the World Wide Web (W3C 2017). ISO, as a body consisting primarily of national standards bodies is unlikely to agree on interledger protocols in a time frame that will promote market growth. The missions of IEEE, IETF, and IRTF are rather far afield from application-layer protocols. The EEA's mission is specifically limited to the Ethereum blockchain, and the EEA executive has expressed a desire to produce a single blockchain client standard. The W3C could readily adopt work on blockchain protocols if (and only if) their membership permits the consortium to accept blockchain's "Web 3.0" positioning as a broadening of the definition of the World Wide Web. The current W3C definition of the Web is based on the HTTP and HTML client-server structure of the historic Web. We propose that the W3C broaden their definition of the Web to include any peer-to-peer or other non-client-server protocol relationships between components. Such a broadening of mission might be easier than establishing a new SDO with a mandate specific to blockchain developments.

The authors support continued development of cross-chain smart contract specifications at the W3C and ISO and propose that extensions to the existing BPMN standards be conducted at the Object Management Group.

Efforts by national standards organizations were not comprehensively surveyed by the authors. National standards organizations, e.g. the American National Standards Institute (ANSI), Standards Australia (SA), and Standardization Administration of China (SAC), coordinate national interests with ISO and other international SDOs. The authors note that several such organizations (including the ones named) have some local efforts to explore blockchain standardization. A comprehensive survey of those activities would be a valuable additional contribution, and hopefully lead to a more complete understanding of worldwide efforts.

References

3rd Generation Partnership Project (3GPP), Technical specifications and technical reports for a GERAN-based 3GPP system, 1999, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=5.

Allison, I., Public or private? blockchain distinctions are falling out of fashion, 2018, https://www.coindesk.com/public-private-blockchain-distinctions-falling-fashion/.

Berners-Lee, T., Fielding, R. and Masinter, L., Internet Engineering Task Force, IETF RFC 3986, Uniform resource identifier (URI): generic syntax, 2005, https://tools.ietf.org/html/rfc3986.

Braden, R. (ed), Internet Engineering Task Force, IETF RFC 1122, Requirements for internet hosts -- communication layers,

1989, https://tools.ietf.org/html/rfc1122.

Buterin, V., Ethereum white paper, 2013, https://github.com/ethereum/wiki/wiki/White-Paper.

Buterin, V., On public and private blockchains, ethereum blog, August 2015, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

Enterprise Ethereum Alliance. Enterprise ethereum client specification v1.0, 2018, https://entethalliance.org/resources/.

Faulkner, S., Eicholz, A., Leithead, T., Danilo, A. and Moon, S., HTML 5.2, W3C recommendation, 2017, https://www.w3.org/TR/html/.

Ferris, C., Two enter, one leaves, May 2018, https://developer.ibm.com/code/2018/05/11/two-enter-one-leaves/

Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and Berners-Lee, T., Internet Engineering Task Force, IETF RFC 2616, Hypertext transfer protocol -- http/1.1, 1999, https://tools.ietf.org/html/rfc2616.

Fyrigou-Koulouri, M., Blockchain technology: an interconnected legal framework for an interconnected system, 9 Case W. Res. J.L. Tech. & Internet 1 (4th), 2018, https://scholarlycommons.law.case.edu/jolti/vol9/iss1/7.

Hommes, S., Fiz, B., State, R., Zuenko, A., Caetano, R. and Gurbani, V. ALTO for the blockchain, expired internet-draft (individual), 2017, https://datatracker.ietf.org/doc/draft-hommes-alto-blockchain/.

International Organization for Standardization, ISO/IEC 9075:2016 Information technology -- database languages -- SQL -- part 1: framework (SQL/framework), 2016, https://www.iso.org/standard/63555.html.

International Organization for Standardization, ISO/IEC 7498-1:1994 Information technology -- open systems interconnection -- basic reference model: the basic model, 1994, https://www.iso.org/standard/20269.html.

International Organization for Standardization, ISO/IEC 22275:2018 Information technology -- programming languages, their environments, and system software interfaces -- ECMAScript® specification suite, 2018, https://www.iso.org/standard/73002.html.

Khatchadourian, S., Lubin, J., Millar, J. and Buterin, V., Enterprise ethereum alliance - vision, 2017, https://www.researchgate.net/publication/325655669_Enterprise_Ethereum_Alliance_-_Vision.

Mockapetris, P., Internet Engineering Task Force, IETF RFC 1035, Domain names - implementation and specification, 1987, https://tools.ietf.org/html/rfc1035.

Nakamoto, S., Bitcoin: a peer-to-peer electronic cash system, 2008, https://bitcoin.org/bitcoin.pdf.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R. and Sabadello, M., Data model and syntaxes for decentralized identifiers, draft community group report, May 2018, https://w3c-ccg.github.io/did-spec/.

Sporny, M. and Longley, D., Verifiable claims data model and representations, W3C first public working draft, August 2017, https://www.w3.org/TR/2017/WD-verifiable-claims-data-model-20170803/.

Sporny, M. and Longley, D., The web ledger protocol 1.0, draft W3C community group report, June 2018, https://w3c.github.io/web-ledger/.

Szabo, N., Smart contracts, 1994, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

W3C. W3C mission, 2017, https://www.w3.org/Consortium/mission.

W3C Interledger Payments Community Group. Interledger protocol v4, draft W3C community group report, 2018, https://interledger.org/rfcs/0027-interledger-protocol-4/.

Wood, G., Ethereum: a secure decentralised generalised transaction ledger, ethereum project yellow paper 151, 2014, https://ethereum.github.io/yellowpaper/paper.pdf.

Tables

Table 1. Variations of "Blockchains" and their Consensus Algorithms

Project/Product	Consensus Algorithm
Bitcoin	Proof of Work (PoW)
Ethereum	PoW, Proof of Authority (PoA), Proof of Stake (PoS)
Hyperledger Fabric	Practical Byzantine Fault Tolerance (PBFT)
Hyperledger Sawtooth	Proof of Elapsed Time (PoET)
Quorum	Raft, Istanbul BFT (IBFT)
Corda	Validity and Uniqueness
Veres One	Leaderless electors
Hashgraph	Gossip about Gossip/Virtual Voting
Byteball	SPECTRE

Table 2. Existing Standards

SDO	Effort
EEA	Enterprise Ethereum Client Specification v1.0

Table 3. Current Standardisation Efforts

SDO	Effort
W3C	Verifiable Claims data model and message syntax
EEA	Enterprise Ethereum Client Specification v1.1

Table 4. Current Explorations by Standards Development Organisations

SDO	Working Group	Exploration
ISO	• ISO/TC 307/SG 1 Reference architecture, taxonomy and ontology • ISO/TC 307/SG 2 Use cases • ISO/TC 307/SG 3 Security and privacy • ISO/TC 307/SG 4 Identity • ISO/TC 307/SG 5 Smart contracts • ISO/TC 307/SG 6 Governance of blockchain and distributed ledger technology systems • ISO/TC 307/SG 7 Interoperability of blockchain and distributed ledger technology systems • ISO/TC 307/WG 1 Foundations • ISO/TC 307/WG 2 Security, privacy and identity • ISO/TC 307/WG 3 Smart contracts and their applications	• Vocabulary • Reference architecture • Taxonomy and Ontology • Legally binding smart contracts • Identity • Cross-chain contracts • Security risks
IRTF	• Decentralized Internet Infrastructure Research Group	• Decentralizing infrastructure services (e.g. P2P transport and naming)
IEEE	• P2418	• IoT security • Pharma provenance • Digital identity
W3C	• Not yet established	• Decentralized identifiers
EEA	• Core Layer • Integration Layer	• Vertical industry-specific extensions

Table 5. Proposed Standards Development

Possible SDO	Area of Interoperability
W3C	• Interledger protocol(s)
ISO, W3C	• Cross-chain smart contracts
OMG	• BPMN

Figure captions

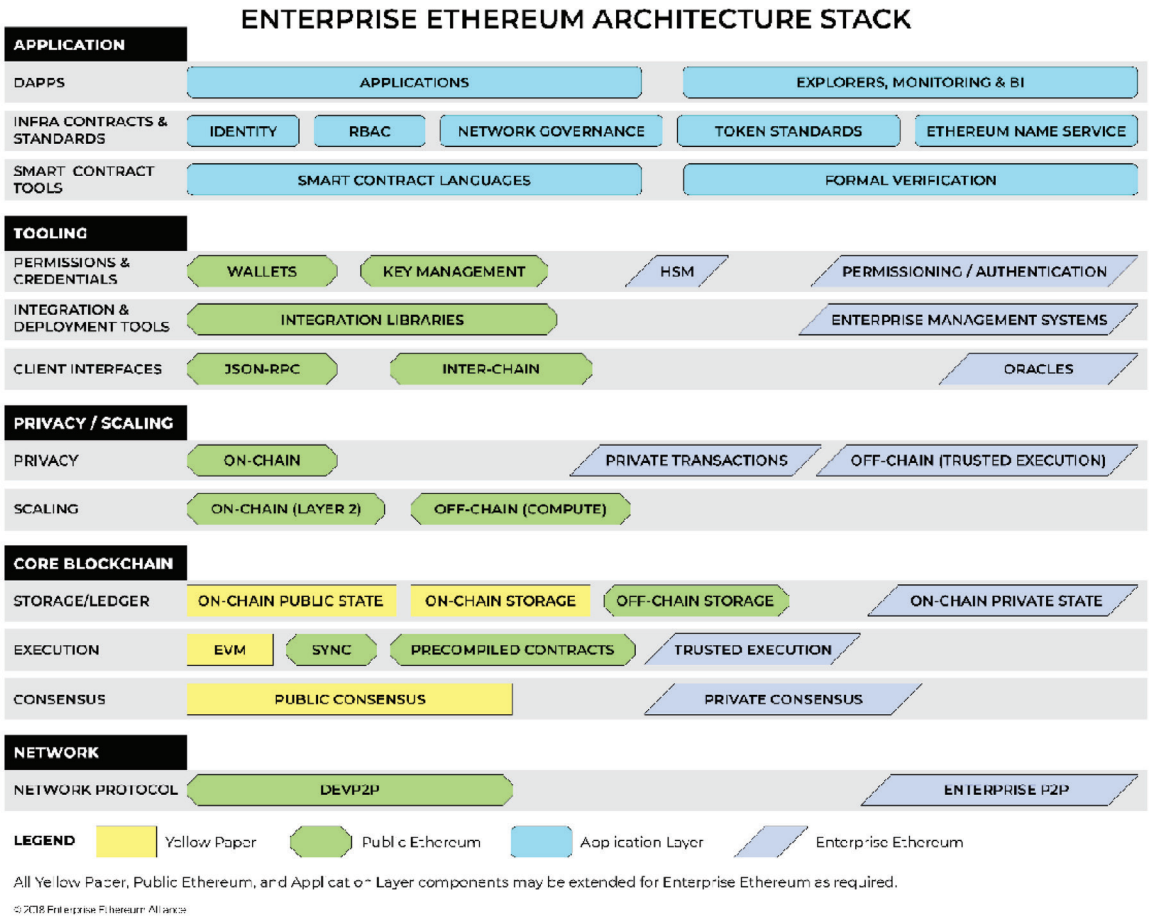

Figure 1. Enterprise Ethereum Stack Diagram