



**Blockchain Center of Excellence
White Paper Series**

***Towards Blockchain 3.0 Interoperability:
Business and Technical Considerations***

(BC CoE 2019-010)

Towards Blockchain 3.0 Interoperability: Business and Technical Considerations

Blockchain Center of Excellence Research White Paper

(BC CoE 2019-01)

By

Mary Lacity

Walton Professor and Director of the Blockchain Center of Excellence

Zach Steelman

Assistant Professor of Information Systems

Paul Cronan

Professor and M. D. Matthews Chair in Information Systems



About the Blockchain Center of Excellence (BC CoE):

The BC CoE is housed in the Information Systems Department of the Sam M. Walton College of Business at the University of Arkansas. The BC CoE was officially launched by US State Governor of Arkansas, the Honorable Asa Hutchinson, on August 1, 2018. The center's vision is to make the Sam M. Walton College of Business a premier academic leader of blockchain application research and education. The BC CoE's white paper series is one activity towards achieving that vision. As the BC CoE aims to be platform agnostic, open, and inclusive, our white papers are available to the public following a 60 day sequester period with our Executive Advisor Board member firms. In keeping with the spirit of blockchains as an immutable ledger, the hashes of each white paper are stored on the Bitcoin blockchain using a service by poex.io.

White paper audience:

The BC CoE's white papers are written for multiple audiences, including senior executives looking for the "So *what?*", IT and innovation directors in charge of blockchain initiatives needing deeper insights, and students at both the graduate and undergraduate levels. Given the readership diversity, we write an Executive Summary for senior executives interested in the overall findings, a Full Report for managers directly engaged with enterprise blockchains, and include a number of Appendices to assist novice readers.

Research objective and methods:

The Executive Advisory Board members for the BC CoE selected the topic for this white paper. Members from ArcBest Technologies; FIS; IBM; J.B. Hunt; McKesson; Microsoft; Tyson Foods; and WalMart, posed the research question: "*How can enterprises approach interoperability when the technology is immature and rapidly changing?*" The Director of the BC CoE assembled an academic research team that reviewed the academic and practitioner literature (see *Appendix A: Research Methods*). Executive Advisory Board members hosted a workshop where interoperability experts shared their insights with the research team.

Acknowledgements:

We thank and acknowledge the input and suggestions from our executive advisor board and workshop guests. We also thank Yaping Zhu, Doctoral Candidate in Information Systems, for her assistance with Appendix D.

Towards Blockchain 3.0 Interoperability: Business and Technical Considerations

Executive Summary

“So far, the notion of chain interoperability has seen much theory and little practice.”

Vitalik Buterin, co-founder of Ethereum in 2016¹

“At Hyperledger, we envision a world of many chains – some public like the cryptocurrencies and some permissioned like you will see in healthcare settings. That’s why we focus on developing the common frameworks for building all kinds of chains. Our diverse developer communities remain diligent in helping the industry advance interoperability above the layer of the DLT, and are on constant look out for simple and open cross-blockchain approaches.”

Hyperledger Project in 2018²

This white paper aims to answer the question: **“How can enterprises approach interoperability when the technology is immature and rapidly changing?”** (the so-called ‘Blockchain 3.0’ era). Many blockchain applications have been developed, both public and private, since the Bitcoin application was developed in 2009. As enterprises explore blockchain solutions, they are increasingly concerned about the proliferation of blockchains, how blockchain applications will connect with each other and with legacy systems, and the fear of getting locked into solutions too early. In short, enterprises are concerned about **blockchain interoperability**.^a

Based on a literature review, an interoperability workshop, and interviews, our research revealed a disconnect between **top-down business concerns** about specific ecosystem/application interoperability, and **bottom-up technical concerns** about general blockchain interoperability. The contribution of this white paper is to help bridge these two spheres by highlighting the top-down business and bottom-up technical interoperability considerations, as well as **emerging solutions**.

Business executives and IT/Innovation leads have **top-down business concerns** – how a particular blockchain **ecosystem/application** for a particular use case will interoperate with other blockchains and with other existing systems. Particular interoperability concerns – data standards; governance; risk assessment and mitigation; low switching barriers; overall business value – exist for blockchain application use cases (such as food traceability, tracking cargo containers, and financing trade). To achieve **interoperability from a business perspective**, several issues are considered and discussed in the paper – identity, data and event standardization; governance compatibility/acceptance; acceptable risks; and preventing vendor lock-in.

Business strategies for interoperability seem to follow one of two strategies: **doubling down** on a specific ecosystem/application or **hedging bets** by participating broadly in multiple ecosystems. In the double-down strategy, enterprises that commit firmly to one specific ecosystem/application gain the advantage of focused efforts and resources. Bringing a blockchain solution from POC to production is a challenging endeavor. Cooperating with competitors, working with a specific standards-making body to adapt identity, data, and

^a As per US National Institute of Standards and Technology (NIST), for this research, an interoperable blockchain architecture is a composition of distinguishable blockchain systems, each representing a distributed data ledger, where transaction execution may span multiple blockchain systems, and where data recorded in one blockchain is reachable and verifiable by another possibly foreign transaction in a semantically compatible manner.

event relevant industry standards, and working with regulators to ensure the solution will comply with laws, the founding enterprises aim to become the preferred solution, and likely could be, provided interoperability (and therefore vendor neutrality) is core to its design. Enterprises want the flexibility to switch solutions and to interoperate with systems. Moreover, a solution that considers interoperability as part of its key feature will result in enticing more organizations to participate. For some enterprises, this means doubling down on an open source project. With the **hedging bet** strategy, some enterprises fear it is too early to give commitment to one ecosystem/application and therefore participate widely in many initiatives.

From a bottom-up technical perspective, open source communities, consortia and startups are addressing technical solutions for interoperability. Technical projects aim to meet several interoperability requirements ('all or none' atomicity; between-chain, other chain security; universality; no need for trusted third parties; and source code availability). Importantly, an interoperability solution should be easy to use by developers and seamless to end-users. Two important differences exist between general APIs and blockchain APIs. Blockchain APIs can create, read, and submit reversal transactions, but a blockchain's digital ledger is immutable – once data is appended to the official digital ledger, the data cannot be altered or deleted as an inherent property of the application.^b Many blockchains maintain entire transaction histories on the blockchain to build a state database (current state of all assets/participants/etc.). Another major difference between a general API and a blockchain application API is that a blockchain API requires a waiting period before one can confidently view the response as valid, particularly across public blockchains. Important technical considerations are presented and discussed in this paper, including technical strategies for interoperability using notaries, sidechains, and hash-time locked contracts.

Although it is too early to declare which interoperability solutions will become de facto standards, enterprises can use a suggested checklist of blockchain business and technical criteria (discussed) to assess and compare the robustness of interoperability projects. Each enterprise will need to decide which criteria are required versus desired, and may add additional criteria as needed. Most enterprises will likely require that all the business criteria be met; but might accept trade-offs for the technical criteria in the short-term.

Lessons learned are also discussed in this paper. In short, it is still too soon to answer definitively the question "*How can enterprises approach interoperability when the technology is immature and rapidly changing?*" Our audience of senior executives are looking for the "*So what?*"; IT and innovation directors in charge of blockchain initiatives are in need of deeper insights. Based on our discussions, executives, IT, and innovation directors should: 1) be sure the use case calls for a blockchain solution; 2) choose blockchain solutions based on the ecosystems developing around specific business applications; 3) participate in interoperability technical projects so that IT will understand what it will take to execute a legitimate business case; and 4) expect custom interoperability solutions for a while. Technology providers should plan for multi-vendor, platform agnostic platforms.

^b This is true for normal operations, but under an extreme circumstance like a major hack or programming bug, people who operate the nodes might decide to overwrite a digital ledger. To do so would require that over 50 percent of the nodes roll back the ledger to an agreed upon point.

Towards Blockchain 3.0 Interoperability: Business and Technical Considerations

Table of Contents

1. Introduction

2. Three Eras of Blockchains

- 2.1 Blockchain 1.0: Single Applications
- 2.2 Blockchain 2.0: Multiple Applications/Platforms
- 2.3 Blockchain 3.0: Interoperable

3. Blockchain 3.0: Top-Down Business Considerations

- 3.1 Identity, Data and Event Standards
- 3.2 Governance Compatibility/Acceptance
- 3.3 Acceptable Risks
- 3.4 Low Switching Barriers
- 3.5 Business Strategies for Interoperability

4. Blockchain 3.0: Bottom-up Technical Considerations

- 4.1 APIs: The Foundation of Interoperability
- 4.2 Three Ways to Connect Blockchains
- 4.3 Technical Strategies for Interoperability
 - 4.3.1 Notaries
 - 4.3.2 Sidechains/relays
 - 4.3.3 Hash-time locked contracts

5. Bringing the Gap: Interoperability Solution Criteria

6. Lessons Learned

7. Appendices:

- A: Research Methods
- B: Glossary
- C: GS1 Standards
- D: Additional Interoperability Projects

End Notes

Towards Blockchain 3.0 Interoperability: Business and Technical Considerations

Full Report

“So far, the notion of chain interoperability has seen much theory and little practice.”

Vitalik Buterin, co-founder of Ethereum in 2016³

“At Hyperledger, we envision a world of many chains – some public like the cryptocurrencies and some permissioned like you will see in healthcare settings. That’s why we focus on developing the common frameworks for building all kinds of chains. Our diverse developer communities remain diligent in helping the industry advance interoperability above the layer of the DLT, and are on constant look out for simple and open cross-blockchain approaches.”

Hyperledger Project in 2018⁴

1. Introduction

Bitcoin, the first **blockchain application**^c, went live in January of 2009. Since then, many other blockchain applications have been developed, both public and private. Each individual blockchain application runs its own software and maintains its own digital ledger. As enterprises explore blockchain solutions, they are increasingly concerned about the proliferation of blockchains, how blockchain applications will connect with each other and with legacy systems, and they fear getting locked into solutions too early. In short, enterprises are concerned about **blockchain interoperability**.

Blockchain interoperability does not yet have a commonly accepted definition; academics, blockchain gurus, consortia, and standards bodies all have their own definitions. For the purposes of this research, we adopt the definition provided by the US National Institute of Standards and Technology (NIST):

“An interoperable blockchain architecture is a composition of distinguishable blockchain systems, each representing a distributed data ledger, where transaction execution may span multiple blockchain systems, and where data recorded in one blockchain is reachable and verifiable by another possibly foreign transaction in a semantically compatible manner.”⁵

This white paper aims to answer the question: **“How can enterprises approach interoperability when the technology is immature and rapidly changing?”** We are investigating the so-called ‘Blockchain 3.0’ era technologies of scalable and interoperable blockchain platforms, even as developers disagree about how to evolve the still immature and dynamic Blockchain 1.0 and 2.0 technologies. Not surprisingly, our investigation has revealed many *ideas* for answering the research question, but thus far interoperability projects have produced few production-ready *solutions*. One thing is clear: we see a disconnect between top-down business concerns about specific ecosystems/applications, and bottom-up technical concerns about general blockchain interoperability.

^c Please see the glossary for the definition of any terms in bold text.

Business executives and IT/Innovation leads have top-down business concerns. They worry about how a particular blockchain application for a particular use case will interoperate with other blockchains and with other existing systems. Specific blockchain application use cases, such as food traceability, tracking cargo containers, and financing trade, will drive particular interoperability concerns pertaining to data standards, governance, vendor lock-in, risk assessment and mitigation, and overall business value. The vast majority of enterprise applications will be **permissioned** blockchain solutions.

Meanwhile, open source communities, consortia and startups have launched technical projects to find ways to connect blockchains to fulfill technical interoperability requirements such as atomicity, scalability, and universality. The first interoperability projects focused on connecting two or more **permissionless** blockchains, but there are now technical solutions emerging for connecting two or more permissioned blockchains.

Our research indicates that the two worlds – enterprises concerned with top-down business interoperability at the ecosystem/application level, and technical projects aiming broadly to solve technical interoperability – are each evolving in their own spheres:

“Interoperability will require business standards and technical standards. At some point they will come together, but I don’t believe we should forcibly intertwine them. Once we get the two in unison, no one can stop the blockchain solutions tsunami that will follow!”

Usha Krishnan, Global Black Belt - Americas Blockchain Lead

One contribution of this white paper is to help bridge these two spheres by highlighting the top-down business and bottom-up technical interoperability considerations and emerging solutions.

We first provide an overview of the evolution of blockchains to stress the immature yet rapid advancements. Then we cover, in some detail, specific business and technical considerations – with some emerging solutions. We transform these considerations into a set of criteria to enable enterprises to assess and compare the robustness of interoperability solutions as they come online. In four appendices, we include: a description of the research methods; a glossary of terms; an overview of GS1 standards; and some promising interoperability projects to monitor.

Overall, it’s early days to declare proven and decisive answers to the research question.

2. Three Eras of Blockchains

Blockchains have been in existence for just ten years. Bitcoin ⁶, the first blockchain application, heralded the Blockchain 1.0 era in 2009. For the first six years, single blockchain applications prevailed (see Figure 1). The Blockchain 2.0 era began in 2015 with the launch of Ethereum, a decentralized platform that allows developers to use smart contracts to build applications on top of it. The Blockchain 3.0 era has a less identifiable launch, but the term is used to describe the myriad of projects aimed to improve scalability, interoperability, privacy, and sustainability.⁷

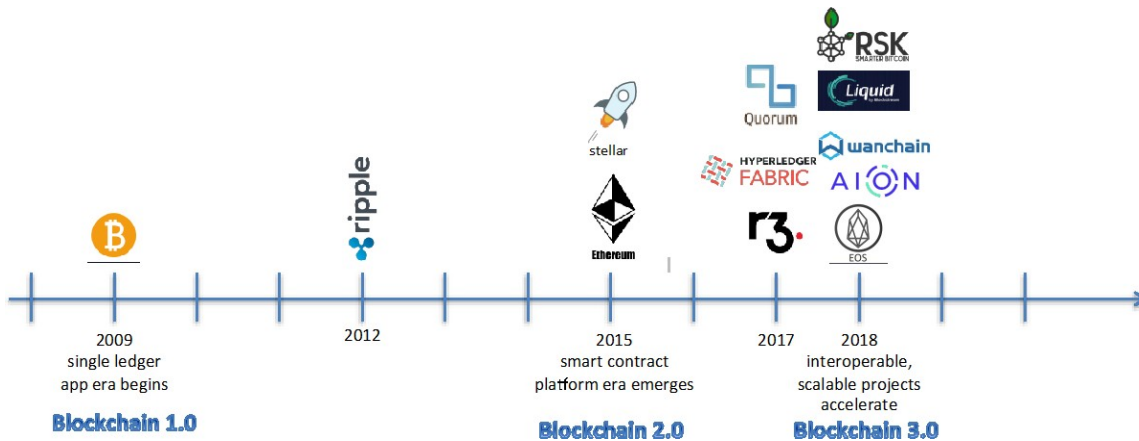


Figure 1: Timeline of Blockchain Eras

2.1. Blockchain 1.0: Single Applications

The Blockchain 1.0 era began with Bitcoin. Bitcoin is a single application: it's a **permissionless**, peer-to-peer payment system that validates and secures transactions using algorithms and cryptography to perform the functions normally done by trusted third parties, like financial institutions. No one person or institution owns or controls it. Instead, an open source community governs Bitcoin Core, the official code base for Bitcoin. Bitcoin proves (so far) that a crowd of independent computers can securely maintain a completely distributed application. Despite the governments that have tried to stymie it, the maleficent actors who have tried to break it, and the beneficent actors who forked it to make what they consider to be improvements, Bitcoin remains an unshakeable recorder of transactions (at least as of the time of this writing), albeit a less reliable store of value given its price volatility. Many other single-application blockchains emerged, most commonly by copying and altering the Bitcoin Core code to produce other digital currencies – the so-called 'Altcoins'. Namecoin and Litecoin were the first Altcoins – created as standalone blockchain applications in 2011. Enterprise blockchain applications began to emerge a few years after Bitcoin. For example, Ripple, the blockchain application for currency exchange, was launched in 2012. As single blockchain applications continued to evolve, Blockchain 2.0 platforms began to emerge, with the launch of Ethereum.

2.2. Blockchain 2.0: Multiple Applications/Platforms

Ethereum started the Blockchain 2.0 era in July 2015, by providing a platform onto which to build blockchain applications. Application developers can use **smart contracts** to build applications on top of the Ethereum platform, while its immutable ledger dutifully secures and records everyone's transactions. With 2.0, interoperability is native to the platform, as all the applications run on a single blockchain, with apps being able to interact.

As of 2018, Gartner identified over 70 blockchain platforms.⁸ There are no clear winners, universal frameworks, or de facto standards to guide enterprise adoption choices. Enterprises are concerned with technology lock-in or expensive switching costs if they decide to move platforms. Furthermore, several blockchain applications might prevail, even within the same application domain. For example, several blockchain-enabled solutions for food traceability now exist.⁹ What if an enterprise needs to use several of them? Even if an enterprise selects a single blockchain platform, it will need to assimilate the blockchain solution with their existing systems of records.¹⁰ In a nutshell, enterprises need blockchains to be interoperable. (Blockchains also need to be scalable – a topic we shall, perhaps, address in a future white paper.¹¹)

2.3. Blockchain 3.0: Interoperable

“To build a chain of chains that acts as an intermediary for all the other chains, and implements a layer, through which the entire blockchain space can route their traffic to allow for better communication, is painfully slow and complex.”

Lucasxhy, blockchain blogger in 2018¹²

The Blockchain 3.0 era promises to improve the interoperability, scalability, security, and performance of blockchains. Focusing on interoperability, Blockchain 3.0 projects aim to seamlessly interconnect:

- ❖ multiple public blockchains (e.g. Bitcoin and Ethereum)
- ❖ multiple private blockchains (e.g. Hyperledger Fabric and R3)
- ❖ public and private blockchains (e.g. Ethereum and Hyperledger)
- ❖ blockchains with legacy systems (e.g. MediLeder and SAP; Ripple and SWIFT)

There are many Blockchain 3.0 projects (see Figure 2). Traditional companies like Accenture and IBM; startups like Aion, Cosmos, and Polkadot; traditional standards bodies like the IEEE, ISO, and NIST; and blockchain consortia like the Hyperledger Project, all have interoperability projects underway.

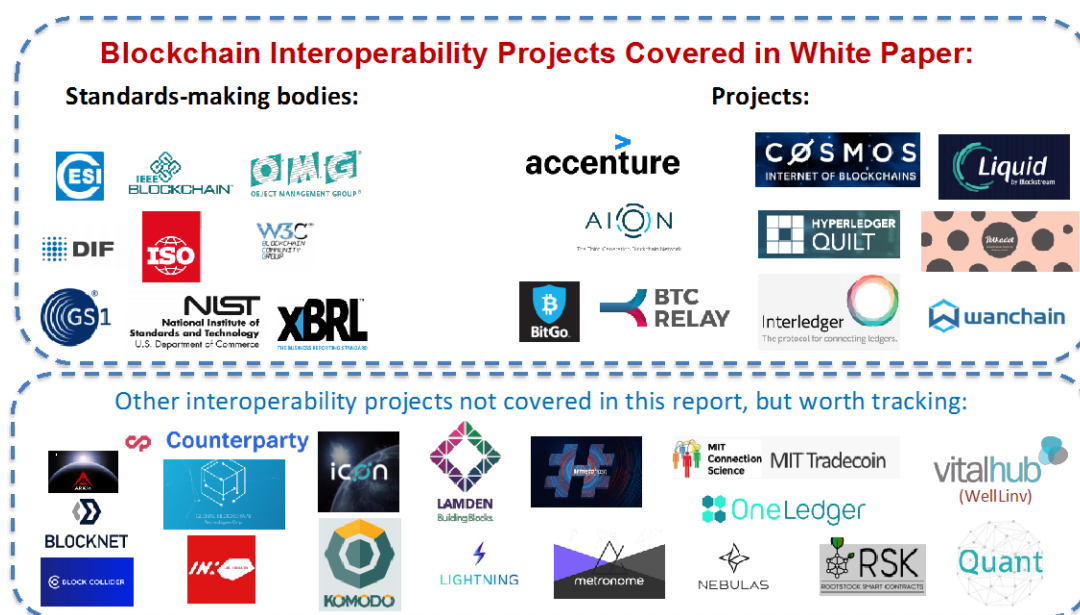


Figure 2: Blockchain interoperability projects

Most interoperability projects are still under development or in beta version. A few early solutions went live, but are no longer active, such as BTC Relay. Thus, three years after Vitalik Buterin wrote the opening quotation in this white paper, ***blockchain interoperability is still at the stage of “much theory and little practice”***. We can, however, frame the conversation around the business and technical concerns enterprises need from blockchain interoperability.

3. Blockchain 3.0: Top-Down Business Considerations

“For two or more blockchain ecosystems to interoperate, there needs to be equivalency in data and governance standards.”

Tejas Bhatt, Senior Director, Food Safety Innovations at Walmart

“Enterprises need to first solve business issues such as identity, data standards, and shared governance. If these are not solved there will be little adoption, so there is no point in worrying about technical standards.”

Ramesh Gopinath, VP, Supply Chain Solutions, IBM

From an enterprise perspective, interoperability is an ecosystem/application-specific issue.

Interoperability comes into play when selecting a particular blockchain solution for a use-case. Questions include:

- If an enterprise selects solution X, how will X connect to other systems now and in the future?
- Does X use identity, data and event formats that are or will likely become the industry de facto standards?
- Who governs the solution? Does the enterprise trust the governance of solution X? Does the enterprise trust the governance of other chains with which X interacts?
- What happens to the enterprise’s data and transaction history if the enterprise decides to switch solutions?
- What risks need to be mitigated concerning liability, non-compliance, and industrial espionage?
- Can the enterprise trace an asset and its owners or custodians, in chronological order, from chain X to other chains?

To achieve interoperability from a business perspective, the following issues must be considered and addressed:

- ✓ **Identity, data and event standardization:** A business solution should use well-established data standards that are semantically understood and accepted by trading partners, and should use a common language for processes/events. When connecting to another chain, the other chain should use the same standards to resolve identities of organizations, locations, and objects across chains. Currently, the industry has not yet delivered on these standards, although traditional standards-making bodies like GS1, ISO, and the IEEE are updating standards to accommodate interoperability in an ecosystem with multiple blockchain solutions. Additionally, blockchain consortia like the Hyperledger Project and Blockchain in Transport Alliance (BiTA) have interoperability projects.
- ✓ **Governance compatibility/acceptance:** The governance council for a blockchain solution defines rights of access, use, validation, data ownership, and overrides. For permissioned blockchains, a governance council will also likely engage a technology provider as implementer/operator and therefore must further define the business models and IP rights. When connecting to another chain, the governance *across* chains should be compatible or at least acceptable to one another. For example, if one chain relies on four trust anchors to verify and record transactions, any chain connecting to it must also rely on these four trust anchors; if an open source community governs one chain, chains connecting to it must accept the decisions of the open source community.

- ✓ **Acceptable risks:** A blockchain solution should minimize risks of liability, non-compliance, and industrial espionage. In what jurisdictions are data kept? When one blockchain solution is connected to another blockchain solution, these risks need to be revisited. If an enterprise sends data to another blockchain application, who is liable if the other blockchain abuses the data? Will parties be able to infer competitive information from metadata stored on the shared ledgers?
- ✓ **Low Switching Barriers:** A blockchain solution should enable an enterprise to switch blockchains or solution providers without the loss of its digital assets, contracts and transaction history. Furthermore, switching costs should be reasonable if an enterprise decides to abandon the current application in order to use another solution. While identity, data and event standards facilitate interoperability; the governance rights come into play as far as enabling or restricting switches to other solutions.

We now explore these business considerations in more detail.

3.1. Identity, Data and Event Standards

The Industrial Revolution prompted the need for technical standards. The Engineering Standards Committee, established in London in 1901, was the first standards organization.¹³ Since then, international, national and regional standards-making bodies proliferate, thus inspiring the famous quote:

“The nice thing about standards is that you have so many to choose from.”

Andrew S. Tanenbaum and David Wetherall (1981), p. 702¹⁴

In the world of digital business communications, the machine-readable barcode was invented in 1952; the Universal Product Code (UPC) was adopted in the retail sector in 1973; and the United Nations passed Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) in 1987. We’ve had eXtensible Markup Language (XML) standards since the 1990s, to pass business documents in both human and machine-readable form over the Internet. We’ve had industry specific standards from ISO, GS1, and the IEEE for decades. For example, GS1’s Electronic Product Code Information Services (EPICS) has been widely adopted in the pharmaceutical industry to track major events in the supply chain, capturing the **‘what, when, where, and why’** of a business transaction.¹⁵ Given all these standards, why do blockchains require more?¹⁶ According to GS1’s (2018) report, *Bridging Blockchains: Interoperability is Essential to the Future of Data Sharing*:

“It will not be enough to only leverage existing GS1 standards for identification, data capture and sharing as a best practice [to achieve blockchain interoperability]. Industry and the consortiums that serve industry will also need to collaborate on answers to some entirely new questions around governance and interoperability.”

Melanie Nuce, Senior Vice President, Corporate Development of GS1 US, elaborated:

“Everyone agrees that with a blockchain solution, the consensus algorithm matters, the hash matters, and the governance matters. Going across chains, it’s not just as simple as taking a set of hash data from a Hyperledger blockchain and giving it to someone on the Ethereum blockchain and say, ‘here, read this’. They can’t. The hash data by its very nature cannot be validated without the source data behind it.”

The British Standards Institution (BSI) published a 2017 report that identified five areas where standards could improve blockchain adoption:

- Standards could play an important role in ensuring interoperability between multiple DLT/Blockchain implementations and, in doing so, could help reduce the risk of a fragmented ecosystem.
- Using standards to establish a stronger consensus on consistent terminology and vocabulary could improve understanding of the technology and help progress the market.
- Establishing standards to address the security and resilience of, and the privacy and data governance concerns related to DLT/Blockchain could help create trust in the technology.
- Standards could play a role in digital identity management and foster end-user trust in the technology.
- There are potential opportunities for standards to play a role in sectors where provenance tracking is important.¹⁷

However, the report concluded that it was too early to develop and impose standards on an immature technology.

Many standards organizations are tackling blockchain extensions and adaptations, but few have produced drafts, let alone final reports. Here's the quick tour:

- ❖ GS1 is working to enhance its standards to apply to blockchain applications and called for a discussion group in 2018.¹⁸
- ❖ The IEEE started a blockchain group in January of 2018 and has five projects under development.¹⁹
- ❖ The International Organization for Standards (ISO) has eleven blockchain projects under development, one specifically on blockchain interoperability.²⁰
- ❖ The National Institute of Standards and Technology (NIST) is looking into blockchains and published a primer in 2018.²¹
- ❖ China Electronics Standardization Institute (CESI) will draft three blockchain standards (smart contracts, privacy, deposits) in the coming year.²²
- ❖ The Decentralized Identity Foundation (DIF) is working on standards that “*enable creation, resolution, and discovery of decentralized identifiers and names across underlying decentralized systems, like blockchains and distributed ledgers.*” They have overviews published for ‘the Universal Resolver’ and ‘Sidetree Protocol’.²³
- ❖ The Object Management Group (OMG) published a discussion paper on distributed immutable data objects.²⁴
- ❖ The World Wide Web Consortium (W3C)’s Blockchain Community Group published the 1.0 version of the Web Ledger Protocol.²⁵
- ❖ XBRL (eXtensible Business Reporting Language), the US non-profit framework that provides the open data exchange standard for business reporting, seems to be tracking the space.²⁶

Table 1 provides links to track progress for these standards initiatives. We also highlight four standards groups below.

Table 1: Blockchain Standards Initiatives	
Organizations with Blockchain Standards Initiatives	Reference sites to blockchain projects
China Electronics Standardization Institute (CESI)	http://www.cc.cesi.cn/english.aspx
Decentralized Identity Foundation (DIF)	https://identity.foundation/#home
GS1	https://www.gs1.org/articles/2463/gs1-releases-new-position-paper-future-blockchain-technology
IEEE Blockchain Initiative (BCI)	https://blockchain.ieee.org/
International Organization for Standards (ISO) TC 307	https://www.iso.org/committee/6266604.html
National Institute of Standards and Technology (NIST)	https://www.nist.gov/publications/blockchain-technology-overview
Object Management Group (OMG)	https://www.omg.org/hot-topics/distributed-immutable-data-object.htm
The World Wide Web Consortium (W3C)'s Blockchain Community Group	https://www.w3.org/community/blockchain/
XBRL (The Business Reporting Standard)	https://www.xbrl.org/tag/blockchain/

GS1. GS1 is working to enhance its standards to apply to blockchain applications (see Appendix C for more on GS1 standards). As an easy step, GS1 is creating a JavaScript Object Notation (JSON) version, which is the emerging standard for blockchain APIs. (The current EPCIS standard is enabled by XML.) More importantly, GS1 is working with industry partners like IBM and Microsoft to enhance the additional business steps needed for blockchain solutions. For example, for the US pharmaceutical sector, GS1 is adding a return verification event to its Electronic Product Code Information Services (EPCIS), as return verification is emerging as one of the first use cases the ecosystem partners are exploring with a blockchain solution. In addition to the pharmaceutical sector, GS1 is also working closely with IBM Food Trust to understand enhancements required for food traceability.

IEEE. The IEEE Blockchain Initiative (BCI)'s value statement reads, in part: *“Blockchain is a new and emerging technology family, positioned on the leading edge of the technology hype curve. It is not bleeding or cutting-edge technology; nor is it fully formed, standardized, or supported by best practices. The Blockchain Technical Community is highly fragmented and badly needs what the IEEE can deliver: a stabilizing think space of seasoned professionals specifically trained and positioned to make a difference.”*²⁷ The IEEE BCI has five active standards projects pertaining to IoT devices: standard data formats; a standard DTL framework for agriculture; a standard DTL framework for autonomous vehicles; and interoperability for electric power infrastructure. In January of 2019, The Blockchain in Transport Alliance (BITA) announced it would work with IEEE Industry Standards and Technology Organization (ISTO) to assist it with its standards activities.

ISO. Prompted by Australia, the ISO launched the Technical Committee (TC) 307 on blockchains and distributed ledgers in 2016.²⁸ The committee has 44 countries participating, including the American National Standards Institute (ANSI) and the BSI. ISO TC 307 has eleven blockchain/distributed ledger standards under development, but all are in preliminary to committee stages. (The ISO has seven phases until a standard is published: (00) preliminary stage; (10) proposal; (20) preparation; (30) committee; (40) enquiry; (50) approval of the Final Draft International Standard (FDIS); and (60) publication.²⁹) The projects cover terminology; privacy and personally identifiable information protection; security risks, threats and

vulnerabilities; identity management; reference architecture; taxonomy and ontology; legally binding smart contracts; interactions between smart contracts; security management of digital asset custodians, discovery issues related to interoperability, and governance.³⁰

W3C. The World Wide Web Consortium (W3C)'s Blockchain Community Group has a mission “to generate message format standards of Blockchain based on ISO20022 and to generate guidelines for usage of storage.”³¹ W3C published The Web Ledger Protocol 1.0 on Github.³² The project was partly funded by the US Department of Homeland Security's Science and Technology Directorate. W3C views a blockchain application as a decentralized state machine system where events modify the current state to create a new state. The 2019 protocol defines the JSON data model for the following types of events: configuration event (genesis block); storage event (designed to flexibly accommodate different vertical contexts); checkpoint event (to bootstrap new mirrors for the ledger); and consensus event (designed to accommodate multiple consensus mechanisms). It defines HTTP APIs for services such as creating and reporting on agent status, and ledger append and query services.³³ The Web Ledger Protocol 1.0, although published under the W3C banner, seems dominated by Digital Bazaar, a Virginia-based startup that received \$750,000 from the US government. W3C's Blockchain Community Group website indicates that it has 202 participants, but its last recorded meeting was November 2017.³⁴

When should/will blockchain standards emerge? Some experts argue that standards *shouldn't* emerge until the technologies mature:

“Most of existing distributed ledger platforms are not mature enough to have their developers and backers discuss ledger interoperability productively. We need to give the technology time to evolve, and give developers time to create their products. And the financial industry should be given time to reach consensus on key issues before standards and protocols are being defined and worked out. Trying to create industry wide common standards before there is common understanding will be a mistake.”

Carlo De Meijer, Senior Economist, MISFA³⁵

“It may be too early to think about standards related to the technical aspects of DLT/Blockchain. Considering the relative immaturity of the technology, aiming for standards on technical aspects could prove counter-productive at this stage.”

BSI white paper³⁶

There is a case for slowing down standards creation. If we move too quickly to apply or adapt today's standards on an emerging technology, might we strangle the blockchain innovations to conform to our current solutions? Other experts argue that standards will emerge when customers demand them:

“Eventually IBM, VeChain, Waltonchain, Ambrosus, OriginTrail, Devery, TE-FOOD and the others will be forced, by their customers, to create gateways to exchange data. And the common language of their connection will be based on GS1 standards.”

The role of GS1 in blockchain-based food traceability³⁷

“Standards representatives are often the last people to the table because technology companies build competitive differentiation and want to obtain market share. Then, when they reach the tipping point where they are no longer able to bring on additional members because Retailer A said, ‘I'm going with this solution because Retailer B went with that one’, they ask the standards groups to bridge the gap.”

Melanie Nuce, Senior Vice President, Corporate Development, GS1 US

3.2. Governance compatibility/acceptance

For a given blockchain solution, enterprises will need answers to these questions:

- **Who** is on the governance council? What process is used to select council members? How long do they serve? What rights and responsibilities do they have?
- **Rights of access:** What users (besides council members) can join? Who can view which data? Who can submit transactions?
- **Rights of validation:** Which nodes can validate transactions? Which nodes can store a copy of the fully distributed ledger?
- **Rights of overrides:** Who is authorized to reverse transactions in the instance of egregious errors?^d
- **Rights of ownership:** Who owns the data on a shared ledger? Who owns the software?
- **Liabilities:** Who is liable for mistakes in shared data, particularly in high-risk areas like Know-Your-Customer (KYC) and Anti-Money Laundering (AML)?

The answers to these questions, again, are use case specific. While there is a theoretical desire to develop governance standards across permissioned blockchains, it seems impractical. Most permissioned blockchains are being developed by a core group of partners. These partners – often comprising competitors as well as trading partners – form some sort of a council charged with developing and enforcing the rules for the application. By their very nature, the rules represent a negotiated treaty among the founding partners, maximizing their benefits. As additional partners decide whether to join the application, they need to assess whether the governance rules and overall business value are acceptable to them. As far as connecting a selected blockchain solution to another chain, the governance council will have to ensure the additional chains have compatible, or at least acceptable, governance rules:

“In IBM Food Trust, we have certain set of rules, which are basically promises to our community, our ecosystem. If data moves from IBM Food Trust to another blockchain, the data that is moving should remain compliant with the rules in the IBM Food Trust ecosystem. So if the governance models in the two solutions are largely incompatible, we won’t even have a starting point to discuss various aspects of interoperability.”

Ramesh Gopinath, VP, Supply Chain Solutions, IBM

3.3. Acceptable Risks

Liability/Non-compliance risks. Regulators all over the world are examining the blockchain space. Some regulators are supportive, some are not, and still others have yet to deliberate. Many participants in our prior research study wanted to educate regulators about blockchains, but at the same time, they did not want regulators participating too closely in consortia, lest their compliance weaknesses be exposed.³⁸ Given the regulatory uncertainty, it makes it even more difficult for enterprises to assess the risks of liability and non-compliance. One BC CoE member said:

“As far as compliance, don’t forget Bitcoin was designed to operate in an unregulated space. Now enterprises want to adapt the technology in highly regulated environments. We have to worry about things like subpoenas, record retention requirements, and compliance audits. If you receive a subpoena for somebody else’s data stored on your copy of the ledger, do you have to respond?”

Scott Mooney, VP Distribution Operations, McKesson

^d Transactions could only be reversed by creating a hard fork at an agreed upon place in the ledger

Industrial espionage. Will parties be able to infer competitive information from metadata stored on the shared ledgers? Certainly, few people now consider bitcoin to be fully anonymous:

“You can’t necessarily see the data in a shared ledger, but the metadata about the transaction might be just as important. It’s anonymous until you find the one piece of metadata and then you can track it back, the same way they reverse engineered Bitcoin to find out who had transactions when it was supposed to be anonymous. It’s that linkage that’s going to be the problem, not just the information in it.”

BC CoE member and member of the Tyson Foods IT Team

BC CoE board members are also concerned about revealing competitive data on a shared ledger:

“In pharmaceuticals, one of our big sticking points is competitive advantage. If we envision putting traceability data on a shared ledger, by its very nature, that means essentially, you’re putting market share information on it. And you may be potentially exposing it to people who would not normally see it. If a manufacturer, for example, ultimately figured out who the end customer was, could they go around the distributor and sell direct? Similarly, could a competitor identify opportunities from another competitor’s data to capitalize on? So, we talk about trusted partners, but its trading partners.”

Scott Mooney, VP Distribution Operations, McKesson

3.4. Low Switching Barriers

Enterprises are very concerned about getting locked into solutions. They need to consider the switching costs – including the monetary costs, time and effort – to change applications. Beyond the financial consequences, enterprises also need to ensure they can technically change solutions, such as exporting their data, contract and transaction history with them to the new solution. Given the immaturity of the technology, there are not many insights to share yet, other than to say that enterprises do consider switching barriers in their decisions.

3.5. Business Strategies for Interoperability

Enterprises seem to follow one of two strategies: **Doubling-down** on a specific ecosystem/application, or **hedging bets** by participating broadly in multiple ecosystems.

Double-down. Enterprises that commit firmly to one specific ecosystem/application gain the advantage of focused efforts and resources. Bringing a blockchain solution from POC to production is a challenging endeavor. By cooperating with competitors; by working with a specific standards-making body to adapt identity, data, and event-relevant industry standards; and by working with regulators to ensure the solution will comply with laws, the founding enterprises aim to become the preferred solution. They likely could be – provided interoperability (and therefore vendor neutrality) is core to its design. Enterprises want the flexibility to switch solutions and to interoperate with systems. Furthermore, a solution that considers interoperability as part of its key feature will entice more organizations to participate. For some enterprises, this means doubling-down on an open source project:

“Initially, State Street cast a reasonably wide net in our search for blockchain initiatives. We were really looking at pretty much every effort under the sun. However, last year, we began to devote more of a focus on specific projects supported by the Linux Foundation. Many of its initial contributors are from my team.”

Moiz Kohari, SVP and Chief Technology Architect, State Street Corporation³⁹

Hedging bets. Some enterprises fear it is too early to commit to one ecosystem/application and therefore participate widely in many initiatives:

“The way we go about investing in blockchain is really multifaceted since nobody knows today which players will prevail... you cannot put all your eggs in one basket, so we have a very diversified approach with whom we work on the blockchain.”

Jacques Levet, Head of Transaction Banking, EMEA at BNP Paribas⁴⁰

“At this stage in the game, we’re not informed enough to pick a winner. There are lots of people vying for this strategic high ground, so I think it’s important for us to engage in places and keep our fingers on the pulse of all of them rather than try and pick a winner at a way too early stage.”

Head of a blockchain CoE for a global financial services firm.⁴¹

“So, from a strategy point of view, it’s early days. We’re probably in the situation that all the other big financial institutions are at the moment. Nobody’s really backing one horse. We’re all trying to get to know as much about it as possible and see where it takes us. All we know is that it’s going to be extremely disruptive.”

IT Consultant and Architect for an African-based bank⁴²

Thus far, we have covered the major business concerns about blockchain interoperability. Next, we cover the technical concerns.

4. Blockchain 3.0: Bottom-up Technical Considerations

From a bottom-up perspective, consortia, open source protects, and startups are addressing technical solutions for interoperability. They are attempting to answer these technical questions:

- How do we lock an asset in one chain while another chain is processing transactions relevant to that asset?
- How can we automate interconnectivity rather than just build custom API interfaces?
- How can we verify that the data reads from a chain are from the permanent ledger and not from a temporary soft fork?

Technical projects aim to meet the following interoperability requirements:⁴³

- ✓ **'All or none' atomicity:** An interoperability solution should ensure that *all* the actions associated with a cross-chain transaction execute, or *all* the actions should fail; no partial executions should be allowed. For example, if Alice records her assets on Chain A and wants to send some value to Bob who records his assets on Chain B, an interoperability solution should ensure that (a) Alice's account is debited AND Bob's account is credited or (b) that NEITHER action occurs.
- ✓ **Between-chain, other chain security:** An interoperability solution should minimize the security risks as data is transmitted, stored, or processed between chains. Furthermore, the security level of the 'weakest link' must meet minimum thresholds of the strongest link.
- ✓ **Universality:** An interoperability solution should be universal, i.e. not requiring a custom program to be built for each new chain.
- ✓ **No need for trusted third parties (TTPs):** An interoperability solution should not rely on centralized trusted third parties. If this criterion is required, it will eliminate the interoperability solutions that rely on notaries (explained below).
- ✓ **Source code availability:** An interoperability solution's source code should be available for audit so that other criteria can be assessed.
- ✓ **Developer and User Friendly:** An interoperability solution should be easy to use by developers and seamless to end-users.

All interoperability approaches 'get into' applications through **Application Programming Interfaces (APIs)**. APIs are used to connect existing systems of record(s) to blockchain application(s), or to connect two or more blockchains.

4.1. APIs: The Technical Foundation of Interoperability

All interoperability solutions rely on Application Programming Interfaces (APIs), a piece of software that connects two applications. In general, APIs allow one application to **Create, Read, Update, and Delete (CRUD)** data in another application. In the context of blockchains, an API allows Chain A to send a message to Chain B and for Chain B to send back a response. APIs can be used to query addresses and transactions on another chain, to watch for events on another chain, and to send and receive transactions on another chain. Many blockchain interoperability solutions rely on **Representational State Transfer (REST)** or **Response-Procedure-Call (RPC)** APIs⁴⁴ (see Glossary for an explanation and examples). Each blockchain application will typically have many APIs. For example, Bitcoin had nearly 70 APIs⁴⁵ and Ethereum had 32 APIs⁴⁶ as of December 2018.

There are two important differences between general APIs and blockchain APIs. **First, blockchain APIs can create, read, and submit reversal transactions, but a blockchain's digital ledger is immutable – once data is appended to the official digital ledger, the data cannot be altered or deleted as an inherent property of the application.**^e Thus it is more accurate to call blockchain APIs 'CRs' rather than 'CRUDs'. One subtlety to this statement is that many blockchains maintain entire transaction histories on the blockchain to build a state database (current state of all assets/participants etc.). If a user only has access to the state database, then from their perspective, they will view what appears to be 'updates'.

Another major difference between a general API and a blockchain application API is that **a blockchain API requires a waiting period before one can confidently view the response as valid, particularly across public blockchains** (see Figure 3). Why? A blockchain is secured by a network of distributed nodes. Normally *one* of the nodes successfully creates the next block on top of the chain and every other node agrees it is the next block – the network reaches consensus.

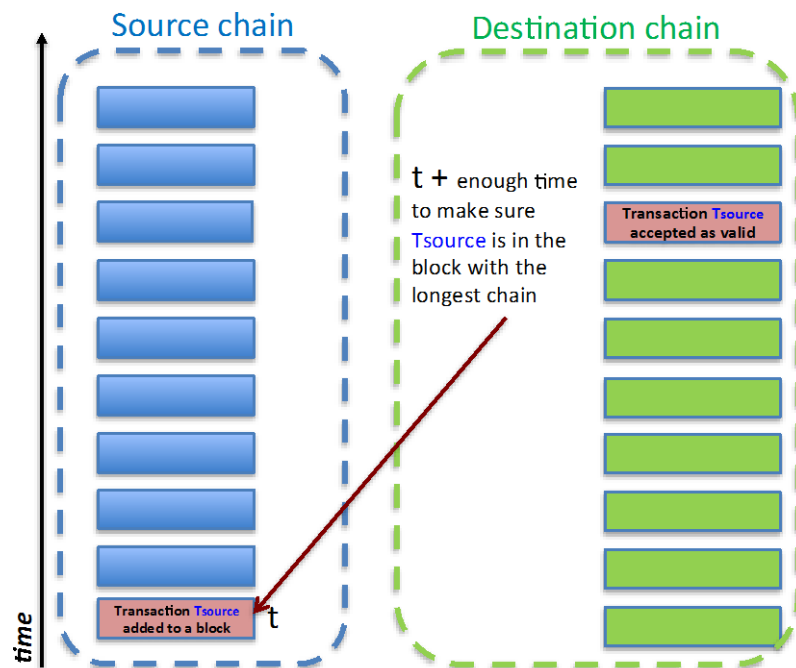


Figure 3: Blockchain time delay

In this figure, the destination chain uses an API to read data from the source chain. The destination chain needs to be confident that the nodes in the source chain have reached consensus before it accepts the transaction as settled.

^e This is true for normal operations, but under an extreme circumstance like a major hack or programming bug, people who operate the nodes might decide to overwrite a digital ledger. To do so would require that over 50 percent of the nodes roll back the ledger to an agreed up point.

Sometimes two nodes create the next block at the same time, resulting in two versions called a **soft fork**. For a short while, different nodes in the network will be working off of different branches of the ledger until one is established as the longest and therefore the valid branch. If Chain A wants to read something in Chain B, Chain A needs to make sure it is reading the longest chain in Chain B.⁴⁷ To confidently query Bitcoin, for example, it is generally recommended to wait until the transaction is six blocks deep, which takes, on average, an hour. Permissioned blockchains, such as Hyperledger, also require wait times but is entirely dependent upon the consensus mechanisms in regard to the speed at which those transactions are considered settled.

4.2. Three Ways to Connect Blockchains

There are three common ways for connecting two or more blockchains:

1. **One-time asset pass** where an asset is 'destroyed' on chain A before being 'created' on chain B.
2. A **cross-chain oracle** where one chain needs to read data from another chain. One-way reads are also called 'one-way pegs'.
3. **Cross-chain transaction processing** where two or more blockchains want to coordinate operations so that a single asset can be used by more than one chain. These are also called 'two-way pegs'.

Among these three, cross-chain transaction processing is the holy grail of interoperability; the first two are relatively easy to accomplish.

One-time asset pass. Enterprises want the ability to switch blockchain solutions. To exit one blockchain application, an enterprise will want to export those assets to the new solution. Since digital ledgers are immutable, how is this done technically? One way is to 'burn' the asset on one blockchain and then recreate it on a different blockchain (see Figure 4). A proof-of-burn is an algorithm that sends value to a verifiably un-spensible address that permanently locks that value on chain. For Bitcoin, this is achieved by using the scripting language for the transaction in a way that would ensure the value could never be redeemed. For example, setting the 'txout' to only execute if $2 = 3$.⁴⁸ This, of course, does not address the other needs for switching blockchain solutions, such as grabbing all of the prior transactions that created the final state values.

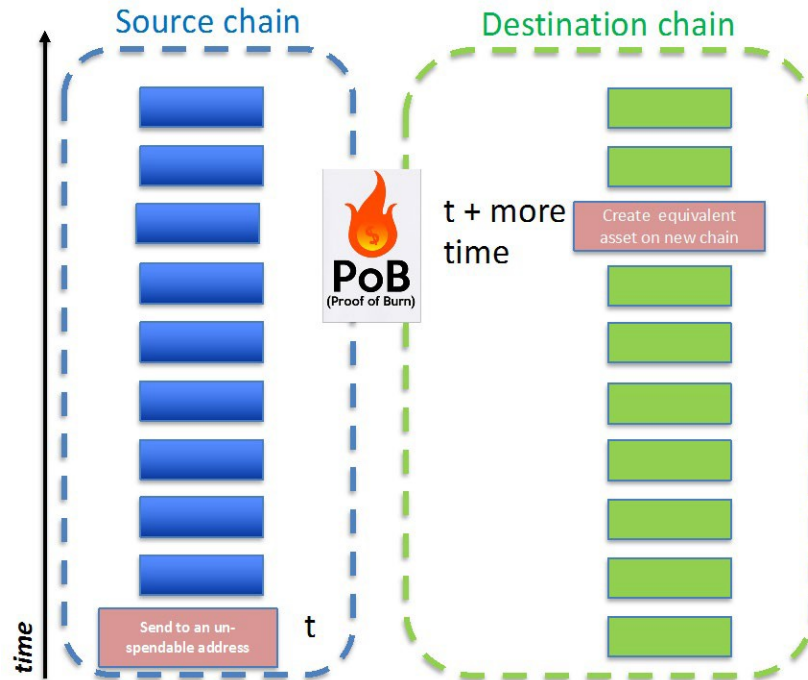


Figure 4: Proof-of-Burn is one way to ‘destroy’ assets on one blockchain and ‘recreate’ them on another

Cross-chain oracle. A cross-chain oracle is a one-way read of data from one chain by another chain. The term **oracle** refers to the external data needed from a source chain to perform some operation in a destination chain.

Bitcoin Relay. BTC Relay was one of the first cross-chain oracles. BTC Relay allows users of applications developed on the Ethereum platform to pay with bitcoins. Developed by Joseph Chow, BTC Relay is an open-source smart contract that was deployed on the Ethereum blockchain in May of 2016.⁴⁹ The open source community conveyed much enthusiasm for it and was seen as an important application of Satoshi Nakamoto’s **Simple Payment Verification (SPV)**.⁵⁰ (SPV proofs are explained below and in the glossary.)

BTC Relay stores Bitcoin’s blockchain headers inside of Ethereum, thus maintaining a mini-version of the entire Bitcoin blockchain. An application developer inside Ethereum can query BTC Relay to verify a transaction on the bitcoin network.⁵¹ BTC Relay automatically executes with no trusted third parties. BTC Relay is quite fascinating in how it incentivizes people to keep adding new Bitcoin blocks to the smart contract, on average, every ten minutes. ‘Relayers’ who submit new Bitcoin block headers to BTC Relay contract get paid a small transaction fee when other developers query BTC Relay to verify a transaction (see Figure 5).⁵² BTC Relay is in essence a ‘program’ that reads from one chain to ‘prove’ existence and then is used as a ‘true/false’ or as a value in the Ethereum platform.

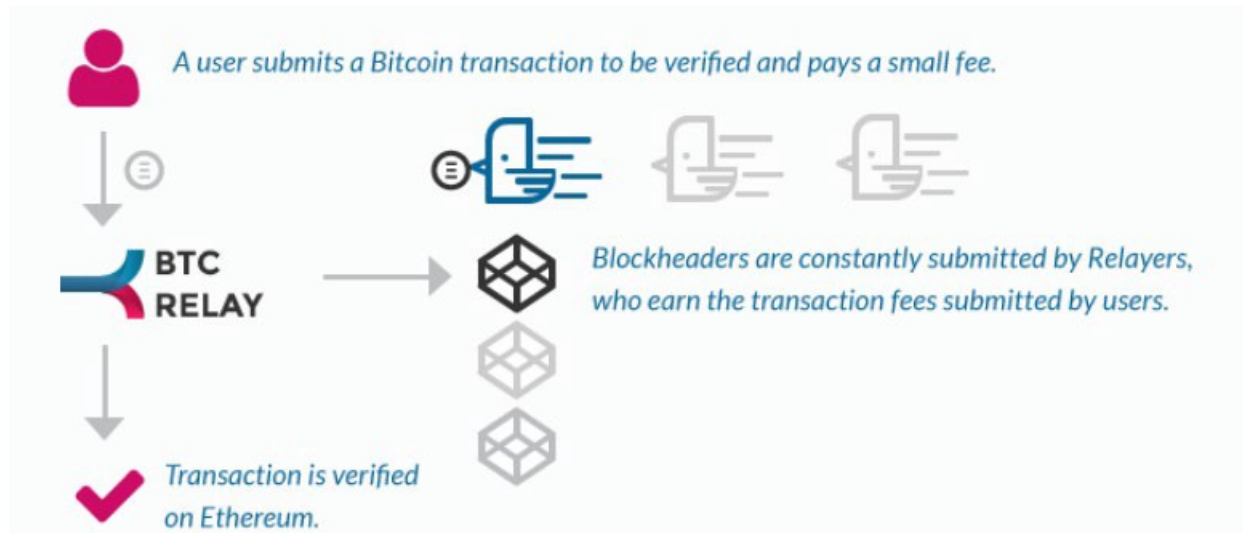


Figure 5: BTC Relay as an Example of a Cross-chain Oracle

Source: Ethereum <https://btc-relay.readthedocs.io/en/latest/frequently-asked-questions.html>

Despite the excitement of BTC Relay in 2016, its live deployment on Ethereum, in 2018, shows very few recent transactions.⁵³ Examining the details, it looks like originally there have been 65,824 transactions, but only 11 of those came within the last year. This may be due to increase in competition (especially in the open source market) and alternative oracles being provided (e.g. <http://docs.oraclize.it/#home>) which do more than just peg bitcoin – they also provide other external resources that are ‘authenticated’ with proofs. With the emergence of cross-chain APIs that are built into the underlying foundation (e.g. Hyperledger and Ethereum integration), relays like this may not be needed as much in the future.

Cross-chain transaction processing. For cross-chain transaction processing, a two-way peg is needed. With a two-way peg, an asset must be locked in the source chain before actions on the destination chain are taken. When the destination chain is finished processing, it locks the asset in the destination chain so that the source chain can once again take control (see Figure 6).

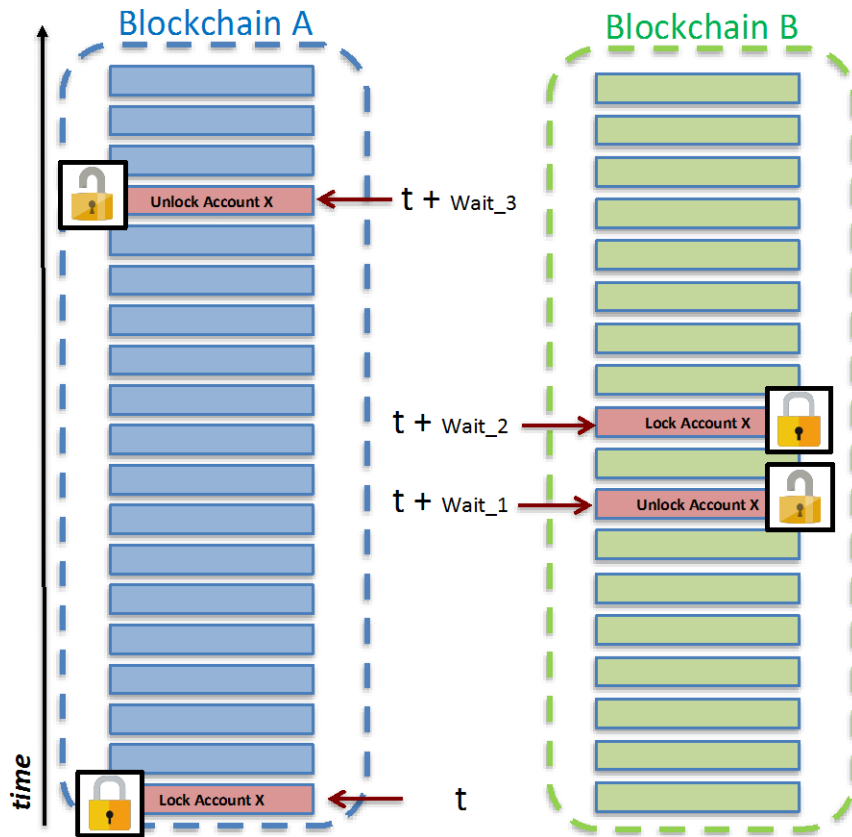


Figure 6: Blockchain time delays in cross-chain transactions

At time t , Chain A locks the address on Chain A and indicates an address on Chain B. That transaction requires some time for the Chain A nodes to reach consensus. After the wait, Chain B creates the equivalent number of assets on Chain B. (Assets are not moved across chains but are replaced with equivalent assets on Chain B). Chain B executes its transactions, locks the address, and indicates an address on Chain A. Some time must pass for the Chain B nodes to reach consensus. After a wait, Chain A unlocks the address and it is back in control of the asset.

We've covered three ways to connect blockchains. Next, we look at three examples of technical strategies for blockchain interoperability.

4.3. Technical Strategies for Interoperability

The technical strategies in this section address interoperability between two or more blockchains. This is because every interoperability project we examined was concerned with this challenge. (No project was focused on how to connect traditional systems with blockchains.)

In 2016, the R3 blockchain consortium commissioned Vitalik Buterin, the inventor of Ethereum, to investigate strategies for blockchain interoperability.⁵⁴ He described three blockchain interoperability strategies:

1. **Notaries:** A single third party or multiple parties coordinate cross-chain operations.⁵⁵

2. **Sidechains/relays:** A smart contract inside one blockchain automatically validates and reads events in another blockchain.
3. **Hash-locking:** Two or more blockchains coordinate operations using the same hash trigger. Operations can also be coordinated by adding a time-out feature to the shared hash feature, creating what are called hash-time locked contracts (**HTLCs**).

4.3.1 Notaries

Notaries are the simplest way to connect two or more blockchains. A notary has control of locks on both chains. A notary must operate full nodes (running the software and storing the entire ledger) for all of the chains to which it connects. This ensures that notaries are grabbing transactions as quickly as possible and have visibility to the entire set of transactions. Notaries may rely on just a single custodian or on multiple custodians. **A single notary** connects two or more blockchains using one trusted third party (see Figure 7).

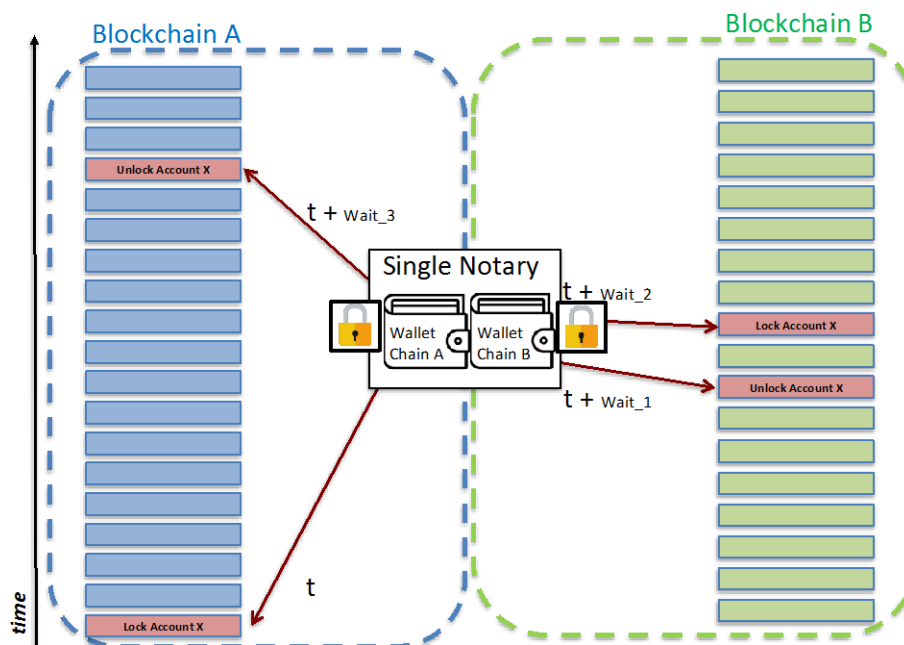


Figure 7: Single Notary

Source: Figure adapted from Lerner (2016)⁵⁶

In this figure, a centralized exchange runs full nodes for both chains. It controls the wallets and locks for addresses stored on both chains. It is the simplest interoperability solution but relies on trusting one centralized party.

Exchanges are common examples of single notaries. Exchanges allow users to easily buy and sell cryptocurrencies and to exchange cryptocurrencies for fiat currencies; but that convenience comes at the acceptance and trust of centralized control, and with the risks of a single point of failure. Cyber-thieves target exchanges because of the large honeypot of value stored all in one place.

Accenture's Interoperability Node. In the permissioned space, Accenture's 'Interoperability Node' serves as a trusted notary. According to Accenture's white paper, a trusted interoperability node sits between the target distributed ledger systems (see Figure 8). Accenture is first creating interoperability nodes between R3 Corda, Digital Asset, Quorum (the enterprise version of Ethereum), and Hyperledger Fabric. The

process to create a node begins with the leaders of two blockchain applications. The leaders define acceptable business rules, policies, standards and governance. These understandings are used as inputs for Accenture to create the integration protocol in terms of agreed upon business logic. Accenture takes the integration protocol and configures an interoperability node that handles asset locking and prevents double spending.⁵⁷ The service was tested in October 2018. Specifically, Accenture showed that information could be shared between R3 Corda and Digital Asset and between Hyperledger Fabric and Quorum.⁵⁸

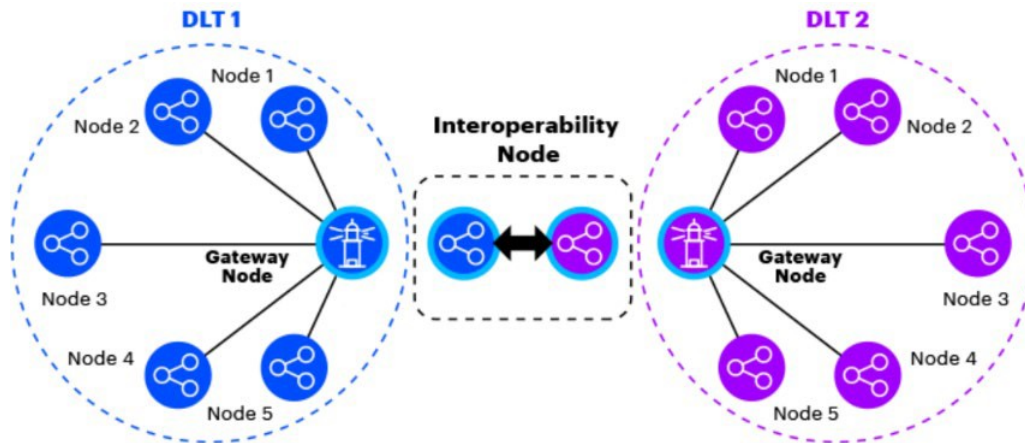


Figure 8: Accenture’s Interoperability Node

Source: Treat et al. (2018)⁵⁹

In 2019, Accenture plans to continue working with clients to define cross-industry and cross-process collaborations with blockchain technologies.⁶⁰ Accenture aims to assuage the fears of vendor locking:

“Applying this capability with our clients is already unlocking new opportunities to bring ecosystems together, mitigating key concerns about picking the ‘wrong’ platform or having to re-build if one partner uses something different.”

David Treat, Managing Director and co-head of Accenture’s Global Blockchain Practice⁶¹

A multi-signature notary, or federation, relies on multiple, independent custodians (see Figure 9). Multi-signature addresses require multiple users to sign a transaction before it can be broadcast onto the blockchain network.⁶² This method is more secure than a single notary, but trust remains centralized within the hands of a few entities. Typically, algorithms require that a majority of the notaries validate a transaction or event. More specifically, the federation requires that ‘ n of m ’ members sign the transaction.

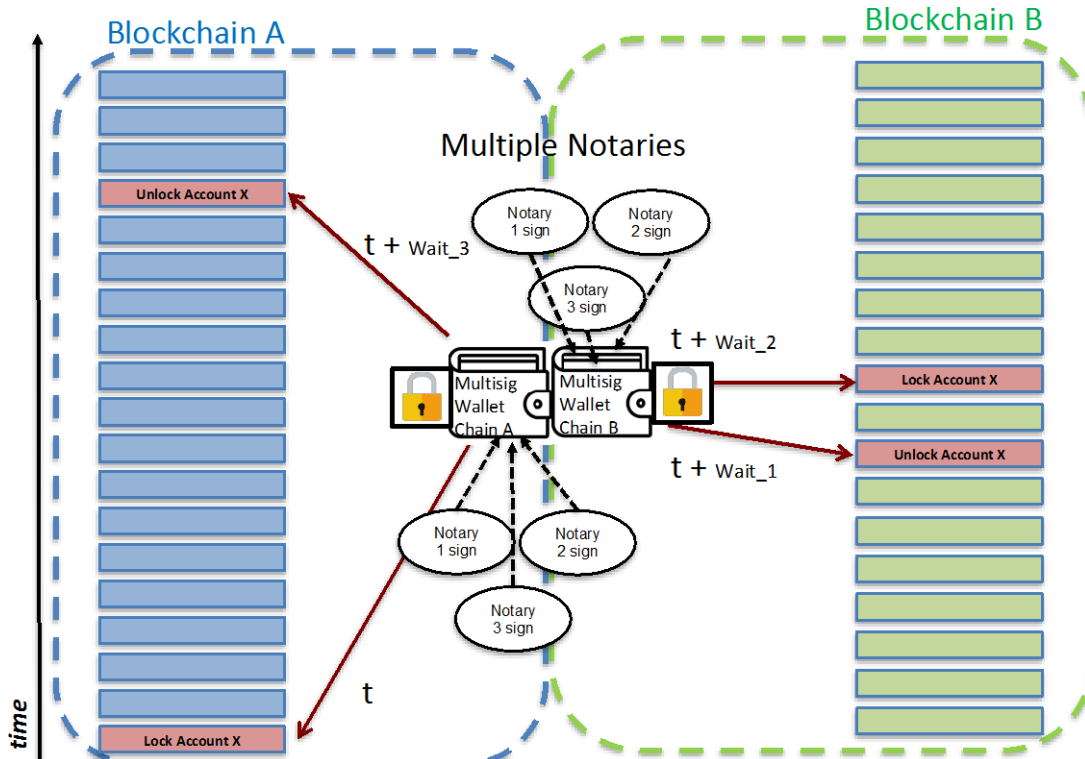


Figure 9: Multiple notaries

Source: Figure adapted from Lerner (2016)⁶³

In this figure, an exchange runs full nodes for both blockchains. It holds the wallets and locks for addresses stored on both chains, but funds are only released when n of m signatures from federation members are signed. It is a simple interoperability solution, but relies on trusting the federation.

BitGo's Multisig Wallet. BitGo was the first multi-signature wallet, launched in August of 2013. The BitGo wallet required two out of three signatures, of which BitGo was one signatory. In 2015, the exchange Bitfinex adopted BitGo, providing all its customers with BitGo's multi-signature wallets. In 2016, Bitfinex was hacked and the perpetrator used the keys to steal \$60 million from the exchange.⁶⁴ Since that fateful event, BitGo has reached many milestones, including providing multisignature wallets for 100 coins. According to a November 2018 press release, BitGo's customers include the world's largest cryptocurrency exchanges, operating in more than 50 countries.⁶⁵ By 2019, BitGo serves as custodian to more than \$2 billion in digital assets, which are insured by a \$100 million policy with Lloyds.⁶⁶

Sergio Demian Lerner, cofounder and Chief Scientist of RSK Labs, offers this advice for multi-signature notaries:

- ✓ There should be between 10 and 30 notaries. Too few, and security and collusion risks increase; too many, and it's difficult to assess and monitor their behaviors.
- ✓ Notaries should span nations to minimize the risks of censorship and government shutdowns.
- ✓ Notaries should span geographies to minimize threats from a natural disaster.
- ✓ Notaries should span multiple entities, such as not all working for the same financial institution.
- ✓ Notaries should be renown.⁶⁷

4.3.2. Sidechains/Relays

Sidechains and relays provide the functions of a notary, but rely on automatically executing algorithms instead of on custodians. Back et al. (2014) first conceived of 'pegged sidechains' as a way for bitcoins and other ledger assets to be transferred between multiple, independent blockchains.⁶⁸ For these authors, a sidechain is a two-way peg to a parent chain (or main chain) that allows assets to be interchanged at a predetermined rate. But the term is relative to the asset, not to the network. For this reason, Vitalik Buterin laments the term 'sidechain' in his white paper on interoperability.⁶⁹ He argued it is better to use the phrase, "a relay of chain A exists on chain B" or "D is a cross-chain portable digital asset with home ledger A that can also be used on chain B."⁷⁰

According to Back et al. (2014), sidechains should:

- run in parallel to main chains
- allow free movement to/from the main chain
- be firewalled so theft in one chain cannot be replicated in the other chain
- allow for different consensus algorithms
- be fully independent from the main chain
- be fast and efficient⁷¹

Liquid. Liquid is an example of a federated sidechain to the Bitcoin blockchain. Developed by Blockstream, it allows members to settle Bitcoin transactions in seconds. According to its website, the federation of members include:

*"... exchanges, traders, and financial institutions from 9 countries across 4 continents. The current list of members is: Altonomy; Atlantic Financial; Bitbank; Bitfinex; Bitmax; BitMEX; Bitso; BTCBOX; BTSE; Buull Exchange; DGroup; Coinone; Crypto Garage; GOPAX (operated by Streami; Korbit; L2B Global; OKCoin; The Rock Trading; SIX Digital Exchange; Unocoin; Xapo; XBTO; and Zaif."*⁷²

Many sidechains/relays use Satoshi Nakamoto's **Simple Payment Verification** (SPV). The idea is that someone can prove that their transaction is included in a valid block and that many other valid blocks were built on top of it. Nakamoto (2008) described SPV as a way to verify bitcoin transactions without running a full network node. Rather, one only needs to maintain a copy of the block headers and then find the security links (called a **Merkle tree** branch) to the transaction to prove it was verified and accepted by the network. SPV shows that "tokens have been locked up on one chain so validators can safely unlock an equivalent value on the other chain."⁷³ Figure 10 illustrates that SPV Proofs can be used to coordinate cross-chain transactions without relying on a notary but instead relying only on the algorithmic proofs.

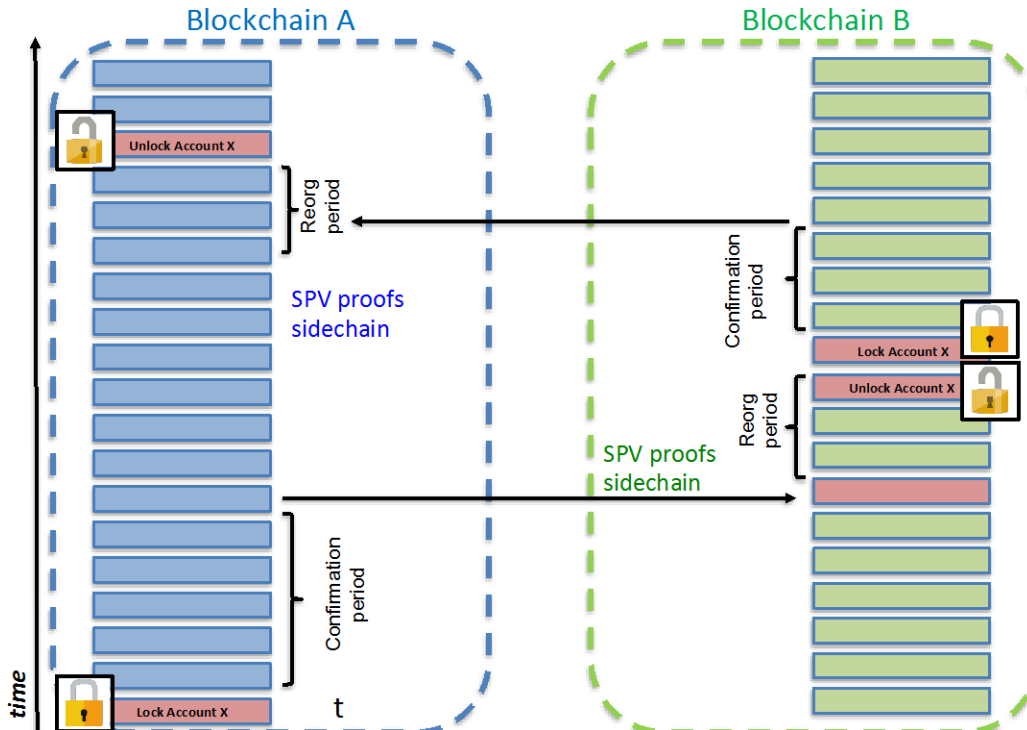


Figure 10: Cross-chain transactions using *Simple Payment Verification (SPV) Proofs*

Source: Figure adapted from Lerner (2016)⁷⁴

SPV proofs run automatically and thus do not rely on TTPs.

Chain A locks the asset and then must wait until the transaction has settled and more valid blocks have been created on top of it so that parties are confident that they are dealing with the longest, and thus most valid, chain.

After the confirmation period, an SPV proof can be submitted to Chain B. Chain B now has to wait, a time called the 'reorg period'. It's possible, another party may submit an SPV proof that contradicts the previous SPV proof. Chain B will select the SPV with the longest chain.

Once confident the SPV proof is valid, it unlocks the asset on Chain B, executes transactions, locks the asset, and waits for the transaction to settle before sending an SPV proof back to Chain A.

4.3.3. Hash-Time Locked Contracts (HTLC)

HTLCs are a clever way to coordinate transactions across two blockchains by relying on the same data trigger, called a 'secret key', 'private key' or 'preimage'. Figure 11 shows how it works. Alice initiates a smart contract on one blockchain that locks value into an address with the hash of the secret key so that one of two things happen: The receiver, Bob, either retrieves the value in the address using the secret key (this is the 'hash lock') and his digital signature, or the contract expires and returns the value to Alice (this is the 'time lock'). So how will Bob get the secret key in a safe manner? Bob creates a smart contract on his chain and locks value using the same hash of the secret key. Alice must reveal the secret key (and her digital signature) to unlock the value in the Bob's contract. The instance that happens, Bob's smart contract learns the secret key and uses it to unlock the value on Alice's smart contract. It's a simple, yet brilliant, solution that eliminates counter-party risks.

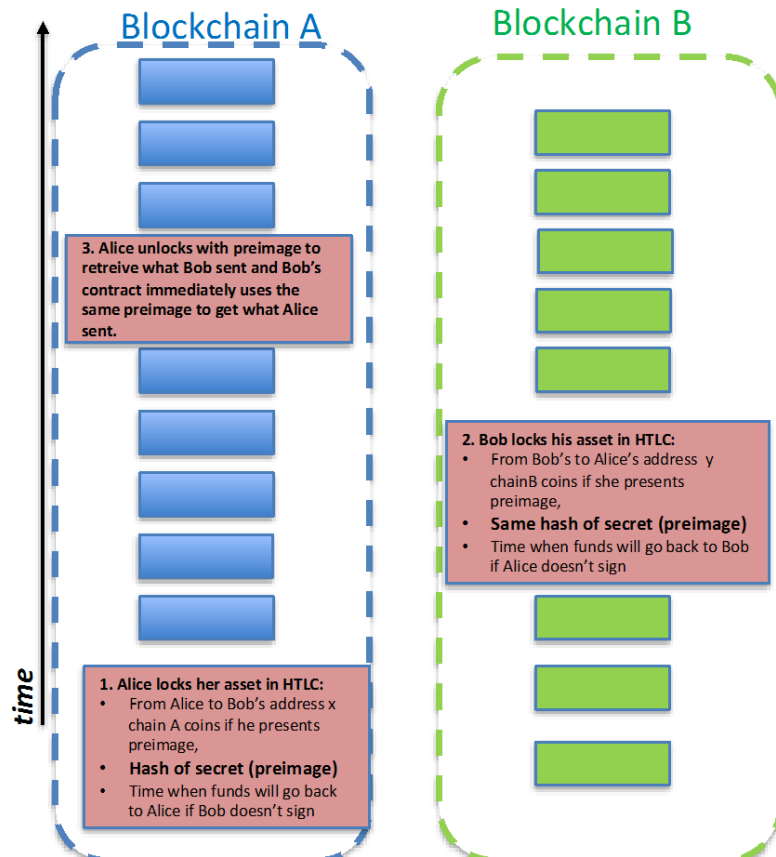


Figure 11: Conceptual rendering of a Hash-Time Locked Contracts (HTLC)

Interledger Protocol. The Interledger Protocol (ILP) accommodates HTLCs. Two Ripple engineers published the ILP's white paper back in 2015. For a given payment, the ILP protocol sends many micropayments with confirmations between micropayments to minimize the risk that a node could steal or fail to send a payment through a network. ILP proposes to use 'cryptographic escrow' that *"conditionally locks funds to allow secure payments through untrusted connectors."*⁷⁵ NTT DATA and Ripple initially led the ILP effort, but a community group within the W3C now manages it, and both public and private blockchain consortia support it.⁷⁶ For a given transaction, the ILP recognizes three types of participants: sender, connectors, and receiver. Connectors are nodes that find a trust path between the sender and receiver. Nodes use the same hashlock for HTLCs across the paths.⁷⁷ (For a detailed example of how HTCLs flow through an end-to-end transaction, see <https://interledger.org/rfcs/0022-hashed-timelock-agreements/>.) While HTLCs are used, they still require that the Interledger Module be updated and installed for each of the ledgers (blockchains) that are being interacted with. This means that as new platforms come online, if they do not follow a standard the protocol recognizes, one needs to be added.

Hyperledger Quilt. Quilt is an interoperability project under the Hyperledger Project umbrella that aims to implement the ILP protocol. According to its website, *"Hyperledger Quilt offers interoperability between ledger systems by implementing the Interledger Protocol (also known as ILP)."* Launched in 2017, Hyperledger Quilt is still in its incubation phase as of February 2019.⁷⁸

We have thus outlined the major business and technical interoperability considerations and described some projects seeking to develop interoperability solutions. We next bring the business and technical concerns together.

5. Bringing the Gap: Interoperability Solution Criteria

Although it is too early to declare which interoperability solutions will become de facto standards, enterprises can use a checklist of blockchain business and technical interoperability solution criteria to assess and compare the robustness of interoperability projects. The starting checklist might include:

Business criteria:

- ✓ Identity, data and event standardization
- ✓ Governance compatibility/acceptance
- ✓ Acceptable risks
- ✓ Low switching barriers

Technical criteria:

- ✓ Atomicity
- ✓ Security
- ✓ Universality
- ✓ No TTPs/fully automated
- ✓ Open source/auditability
- ✓ Developer/user friendly

Each enterprise will need to decide which criteria are required versus desired, and may add additional criteria as needed. For example, enterprises might add speed and scalability requirements for a particular use case. Blockchain applications that execute financial transactions will need swifter cross-chain settlements than blockchain applications that transfer land titles.

Most enterprises will likely require that all the business criteria be met, but might accept trade-offs for the technical criteria in the short-term. For example, an enterprise might be willing to rely on a TTP service to build and maintain the middleware to connect two or more blockchains in the short term until more universal technical solutions mature. Considering the entire list, one can create a robustness profile for an interoperability solution (see Figure 12).

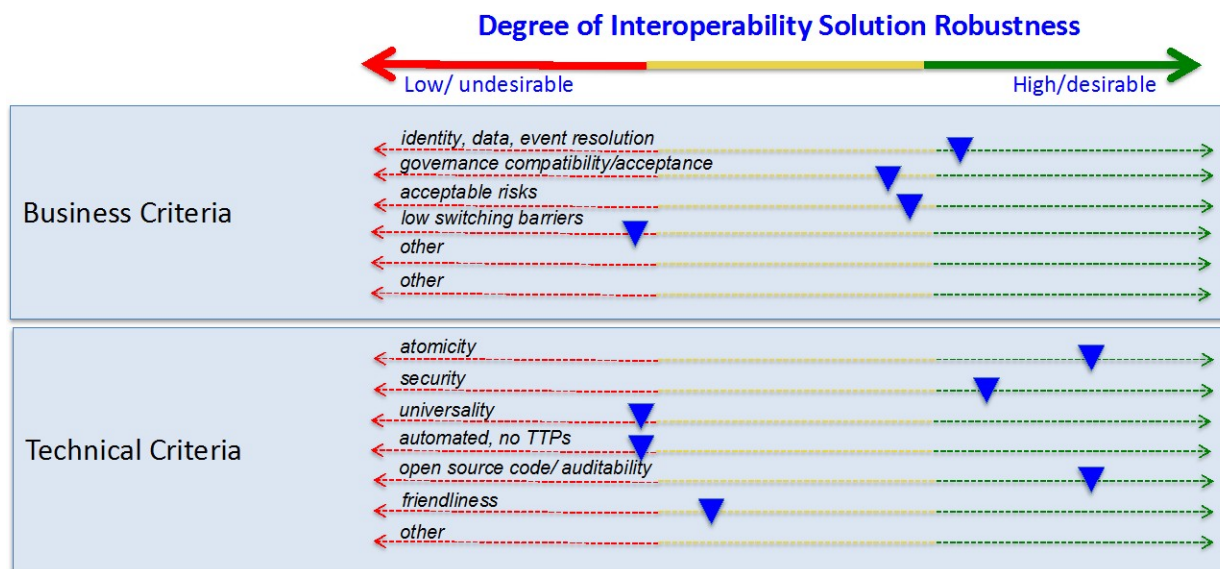


Figure 12: Interoperability robustness profile for a hypothetical solution

This profile shows a solution that rates acceptable or high on all business criteria except switching barriers, suggesting vendor lock-in is a major issue with this proposed solution. The technical criteria are high on atomicity and security, but low on universality and no TTPs, suggesting this is a trusted, centralized third party that built a custom solution. At least it has made its code available for audit.

6. Blockchain 3.0: Lessons Learned

This white paper's overall message is that it is too soon to answer definitively the question "How can enterprises approach interoperability when the technology is immature and rapidly changing?" Our investigation highlighted business and technical concerns, revealed many *ideas* for answering the research question, and highlighted promising interoperability projects. What lessons have we learned? Returning to our audience of senior executives looking for the "So what?" and IT and innovation directors in charge of blockchain initiatives needing deeper insights, we offer these perceptions:

1. For executives, IT and innovation directors: be sure the use case calls for a blockchain solution.

Many technologists are excited about blockchain tools, but, given the immaturity of blockchain technologies and the business and technical concerns about how solutions will interoperate, it's important to make sure a blockchain is the enterprise's best option. A member of the Tyson Foods IT Team warns:

"While many use cases need immutable records, I have a hard time coming up with a use case that actually needs distributed trust."

Ramesh Gopinath, Vice President of Supply Chain Solutions for IBM, outlined the circumstance in which distributed trust is needed:

"It depends on the individual business case. If I want to create a solution for permissioned information sharing in the food ecosystem, for example, I need a few properties. Number one, I need to have nonrepudiation of transactions which means everything has to be digitally signed, and cannot be changed after that signature is in place. Number two, I want to make sure no matter where in the network a smart contract is executed, consensus happens with me included, for every transaction that other multiple parties update. Number three, I want the data itself in the hands of multiple independent parties; I want multiple copies that are not controlled by any one or group of others. It's the properties we are after, not the blockchain itself."

To help ensure a use case is suitable for distributed ledger technologies, we recommend a forthcoming article in *MIS Quarterly Executive* by Asger Pedersen, Marten Risius, and Roman Beck titled, "When to use a blockchain". For them, blockchains are suitable when ALL of these criteria are met:

- ✓ When there is a need to share data
- ✓ When multiple parties update the database
- ✓ When parties have conflicting incentives
- ✓ When parties want to avoid a trusted third party
- ✓ When governing rules vary (e.g. who can see and do what)
- ✓ When transaction rules are stable so that smart contracts can be specified
- ✓ When immutability of records is needed

2. For executives, IT and innovation directors: choose blockchain solutions based on the ecosystems developing around specific business applications.

“It makes sense to do some kind of a review of the ecosystems that are revolving around this that would need to interoperate from a business standpoint. For two or more blockchain ecosystems to interoperate, there needs to be equivalency in data and governance standards.”

Tejas Bhatt, Senior Director, Food Safety Innovations at Walmart

“It’s early days. Given that, it is important to lay out the landscape of blockchain as part of any interoperability study. Interoperability requirements for permissionless and permissioned blockchains will be quite different. For permissioned blockchains, we need to focus on the multiple ecosystems forming around solutions and ask: ‘How do we interoperate between these ecosystems?’”

Ramesh Gopinath, VP, Supply Chain Solutions, IBM

3. For IT and innovation directors: participate in interoperability technical projects so that IT will understand what it will take to execute a legitimate business case. This lesson was offered by a member of the Tyson Foods IT Team and a Master Software Engineer at J.B. Hunt Transport, Inc. They wanted to test out the interoperability of two smart contracts running on two platforms. Their use case involved cold chain traceability of a raspberry pie through the supply chain. They connected a sensor device to the pie that measured temperature and humidity and uploaded the IoT data to a smart contract running in Microsoft Azure. They used the API for a connected vehicle to send geolocation data to a transportation smart contract running on Google Cloud Platform. They ran into a number of technical issues surrounding security authentication, requiring a little ‘trickery’ to expose Azure’s RPC to Google. They had abandoned one sensor for tracking geolocation data before using the vehicle’s integrated telemetry sensor. They also learned lessons about user errors: one of the software developers coded the wrong latitude and longitude for the smart contract delivery location. The member of the Tyson Foods IT summarized the experience, *“Yes, it was difficult, but at the end of the day, we delivered a load and tracked it across different [blockchain] platforms.”*

4. For IT and innovation directors: expect custom interoperability solutions for the next few years. Based on a review of the interoperability projects, we seem years away from universal interoperability solutions that will seamlessly connect blockchains to our systems of record and to other blockchains. The majority of blockchain projects are still focusing on addressing the functionality and features of a single blockchain and yet to focus on inherent interoperability. This means that each blockchain application will need custom API interfaces, and the interfaces will need updating as these technologies continue to evolve.

5. For technology providers: plan for multi-vendor, platform agnostic platforms. Technology providers are in a precarious position in that they are leading some of the most promising blockchain solutions. They’ve corralled ecosystem partners and invested capital, cash, and talent to build solutions, so they should be able to earn a return on those investments. Furthermore, their solutions rely on strict adherence to their own security, scalability, and change management policies; they cannot simply allow other providers to run nodes without a significant vetting process. Many enterprise customers, however, are reluctant to adopt solutions until they feel the business interoperability concerns have been met. They are concerned about vendor lock-in, losing control over their data and transactions, adding significant risks, and questioning the overall value. Technology providers are responding to customer concerns. For example, IBM is opening its IBM Blockchain Platform for use in multiple different computing infrastructures – including on-premises and on diverse public clouds:

"A blockchain network is only as strong as its weakest member. In the real world, a strong network of diverse members means that you will have some who are running on one cloud, others who are running on another. To support the vision of the widespread use of enterprise blockchain, IBM is working with other technology providers to enable organizations to access the IBM Blockchain Platform from their existing infrastructure of choice. Any solution - like IBM Food Trust - that is built on the IBM Blockchain Platform inherits these deployment options for the underlying blockchain nodes"

Ramesh Gopinath, VP, Supply Chain Solutions, IBM

Appendix A: Research Methods

For this white paper, we reviewed the existing literature and incorporated, with permission, the presentations and discussions from the Executive Advisory Board workshop of the University of Arkansas Blockchain Center of Excellence (BC CoE). Additional insights from interviews conducted by the Director of the BC CoE are also included.

Literature Review

We searched Google Scholar, ABI/Inform, and the publications of the Association of Information Systems (AIS) for current academic literature on blockchain interoperability (see Table A.1). We also searched on the terms 'blockchain integration' and 'Blockchain 3.0' to broaden the review. As of January 2019, there were relatively few academic publications, which is understandable given the lead times between author submission, peer review and publication. In contrast, there is an abundance of information about blockchain interoperability on the Internet.

Search Term	'Blockchain Interoperability'	'Blockchain Integration'	'Blockchain 3.0'
Search Site			
Google	35,200	135,000	98,600
Google Scholar	58	259	209
ABI/Inform	39	317	107
AIS	0	10	3

We read all of the abstracts for the Google Scholar, ABI/Inform, and AIS articles. We downloaded and read papers that were particularly relevant for this white paper and included their findings as credited in the endnotes.

BC CoE Workshop

Members of the Executive Advisory Board of the BC CoE met in January to address the issue of interoperability. Members invited interoperability experts within their firms to present and discuss interoperability concerns and solutions. Workshops use the Chatham House Rule:

"The Chatham House Rule originated at Chatham House with the aim of providing anonymity to speakers and to encourage openness and the sharing of information. It is now used throughout the world as an aid to free discussion. The Rule reads as follows: 'When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.'"

Chatham House Royal Institute of International Affairs⁷⁹

Members gave permission to be cited in this white paper.

Appendix B: Glossary

Application Programming Interface (API): An API is a piece of software that connects two software applications so that one application can send a message to and receive a response from another application. As a simple illustration of a blockchain API, suppose we want to know which Bitcoin block number has the unique block header ID:

000000000000000004ec466ce4732fe6f1ed1cddc2ed4b328fff5224276e3f6f

Chain Query offers user-friendly web-based APIs for Bitcoin's blockchain to answer such questions (see Figure B.1). We used the 'getblock' API to search the Bitcoin ledger for the block with the ID above. The API response, presented in JSON format, showed that this hash belongs to block 400000 (called 'height'). The response also showed that this block had been confirmed 154,073 times. The response also listed the transaction IDs within the block. At the bottom of the response (not visible in Figure B.1), information on block size, time stamp, version of the Bitcoin Core, and other block information was also provided.

A web based interface to the Bitcoin API JSON-RPC

Query requires three input parameters

Response returns all the information in the block

Command: getblock ?

Notes: The `getblock` RPC gets a block with a particular header hash from the local block database either as a JSON object or as a serialized block.

Parameter #1—header hash
Parameter #2—JSON or hex output
Result (if format was false/hex)—a serialized block
Result (if format was true/json or omitted)—a JSON block

Block Hash*

The hash of the header of the block to get, encoded as hex in RPC byte order.

Output* true:JSON false:hex

Set to false to get the block in serialized block format; set to true (the default) to get the decoded block as a JSON object

Command Result

```
{
  "result": {
    "hash": "000000000000000004ec466ce4732fe6f1ed1cddc2ed4b328fff5224276e3f6f",
    "confirmations": 154073,
    "strippedsize": 948994,
    "size": 948994,
    "weight": 3795976,
    "height": 400000,
    "version": 4,
    "versionHex": "00000004",
    "merkleroot": "b0e8f88d4fb7cbc49ab49a3a43c368550e22a8e9e3e04b15e34240306a53aeec",
    "tx": [
      "a8d0c0184dde994a09ec054286f1ce581bebf46446a512166eae7628734ea0a5",
      "0de586d0c74780605c36c0f51dcd850d1772f41a92c549e3aa36f9e78e005284",
      "fc12dfcb4723715a456c6984e298e00c479706067da81be969e8085544b0ba08",
    ]
  }
}
```

Figure B.1: Example of a Blockchain API Query and Response

Query: Which block number has the unique block hash identifier of '000000000000000004ec466ce4732fe6f1ed1cddc2ed4b328fff5224276e3f6f'?

Response: Block 400000

Source: <http://chainquery.com/bitcoin-api/getblock/>

Blockchain application: An application that relies on independent computer nodes to validate and secure an immutable record of chronological transactions. More formally, a blockchain application is:

“A distributed, peer-to-peer system for validating, time-stamping, and permanently storing transactions on a distributed ledger that uses cryptography to authenticate digital asset ownership and consensus protocols to add validated transactions to the ledger and to ensure the ongoing integrity of the ledger’s complete history.”

Many blockchains also use smart contracts that apply rules to automatically execute transactions based upon pre-agreed conditions.

Blockchain interoperability: There are several good definitions:

“An interoperable blockchain architecture is a composition of distinguishable blockchain systems, each representing a distributed data ledger, where transaction execution may span multiple blockchain systems, and where data recorded in one blockchain is reachable and verifiable by another possibly foreign transaction in a semantically compatible manner.”

National Institute of Standards and Technology⁸⁰

“As a primitive, we cautiously introduce a rigid definition of cross-chain interaction as ‘interoperability’: An intelligent characteristic of effective communication and direct information exchange from one blockchain to another, while retaining the essence of each individual blockchain, including irreversibility and traceability.”

Jin et al. (2018)⁸¹

“Interoperable chains open up a world where moving assets from one platform to another, or payment versus-payment and payment-versus-delivery schemes, or accessing information from one chain inside another (e.g. ‘identity chains’ and payment systems may be a plausible link) becomes easy and even implementable by third parties without any additional effort required from the operators of the base blockchain protocols.”

Vitalik Buterin⁸²

Fork: a divergence of a blockchain into two or more separate paths. Soft forks are temporary, whereas hard forks are permanent.

Fork (Hard): Hard forks are permanent, divergent paths of a blockchain. Hard forks typically occur under two circumstances. First, someone may create their own blockchain or digital asset by copying and modifying source code. Second, hard forks can occur when the open source community disagrees on the rules of the next version of the protocol. For example, Bitcoin forked into Bitcoin and Bitcoin Cash when miners disagreed over a proposed upgrade in 2017. In another example, Ethereum split into Ethereum and Ethereum Classic when the community disagreed about remediating The DAO hack.

Fork (Soft): Soft forks are temporary branches that typically occur under two circumstances. Under normal operations, two new blocks of transactions might be submitted to the blockchain network at nearly the same time, creating two branches of the ledger. Nakamoto (2008) anticipated this occurrence and proposed the simple solution:

“Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.”

Soft forks also occur during planned upgrades to the open source software. A temporary divergence in the blockchain happens when non-upgraded nodes do not follow the new consensus rules.⁸³ The non-upgraded nodes can still mine for a set time period, so it is up to the upgraded nodes to mine faster and become the longest, and thus, most valid chain.⁸⁴ In practice, the open source community tries to get most people to agree to the upgrade in advance.

Merkle root: Named after the US computer scientist, Ralph Merkle, the Merkle root is the result of a sequence of hashes between pairs of numbers. In blockchain applications, the numbers are pairs of transactions (see Figure B.2). The process to calculate the Merkle root produces a very secure block because if just a single digit is altered in any individual transaction, a subsequent calculation check of the Merkle root would reveal an alteration. For a given block, the Merkle root is added to the block’s header.

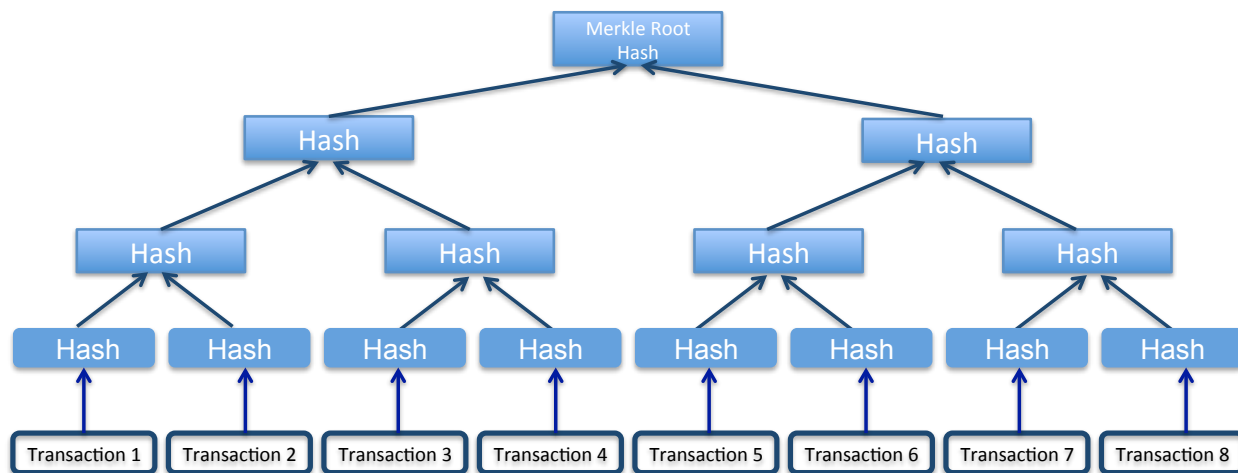


Figure B.2: Merkel Tree

In this example, a block comprises eight transactions. Each transaction is secured with a hash. Then, the transaction hashes are secured again by hashing four pairs of transactions. Next, two pairs of the hashes are hashed. Then the last hash pair is hashed again, resulting in the root hash called the Merkle root.

Oracle: An ‘oracle’ is a Latin term derived from ancient Greece to describe priests who were thought to convey information from the gods to humanity. Within the context of blockchain interoperability, an oracle is a piece of information from a source chain, which is needed by a destination chain.

Permissioned Blockchain: A blockchain application that restricts access and confines which nodes are allowed to observe, transact, validate and add transactions to the distributed ledger.

Permissionless Blockchain: A blockchain application that does not restrict access; anyone with access to the Internet can observe the blockchain application. Anyone can operate a node in the blockchain application network by downloading the source code and compete (or be semi-randomly assigned) to validate and add transactions to the digital ledger.

Proof-of-Burn: With a one-way peg, an asset is ‘destroyed’ in the source chain before being ‘created’ in the destination chain. The main use case is bootstrapping a new cryptocurrency from an existing one. In practice, this can be accomplished with a ‘Proof of Burn’ – an algorithm that sends value to a verifiably unspendable address in the source chain.⁸⁵ How can one make such a verification? In Bitcoin, for example, a script could be written so that the value could only be spent if some silly statement would be true, such as “Only spend bitcoins from this address if date equals May 1, 1888.” The destination chain would need to wait to make sure the block that stores the transaction remains in the longest chain, typically one hour if Bitcoin is the source chain.

Representational State Transfer (REST) APIs: When the client from one application queries the server in another application about a certain resource – like an address, block, or transaction – the server will transfer the representation of the state of that resource in a useable format, such as JSON (Java Script Object Notation), XML (eXtensible Markup Language), or HTML (HyperText Markup Language). The benefit of REST APIs is that they are standard, so no additional software needs to be installed to use them. However, they are slower to execute than RPCs.

Response-Procedure-Call (RPC): With an RPC, one blockchain can call upon another blockchain to execute a process and return the results (see Figure B.3). Thus, whereas REST APIs are queries about a certain state of a blockchain, RPCs are requesting that a process be executed.

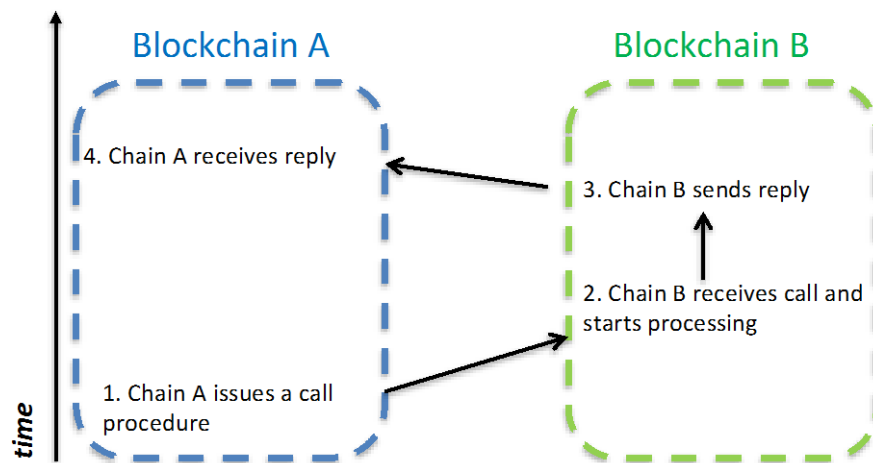


Figure B.3: Response-Procedure-Call (RPC)

Simple Payment Verification (SPV): SPV is a way to verify bitcoin transactions without running a full network node. Nakamoto (2008) wrote:

“A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he’s convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it’s time stamped in.”⁸⁶

An SPV wallet only needs a copy of the block headers of the longest chain. The wallet using SPV client gets the **Merkle Root** branch linking the transaction to its block, proving that the transaction is in the active chain.⁸⁷ Figure B.4 provides an example of this.

Longest chain

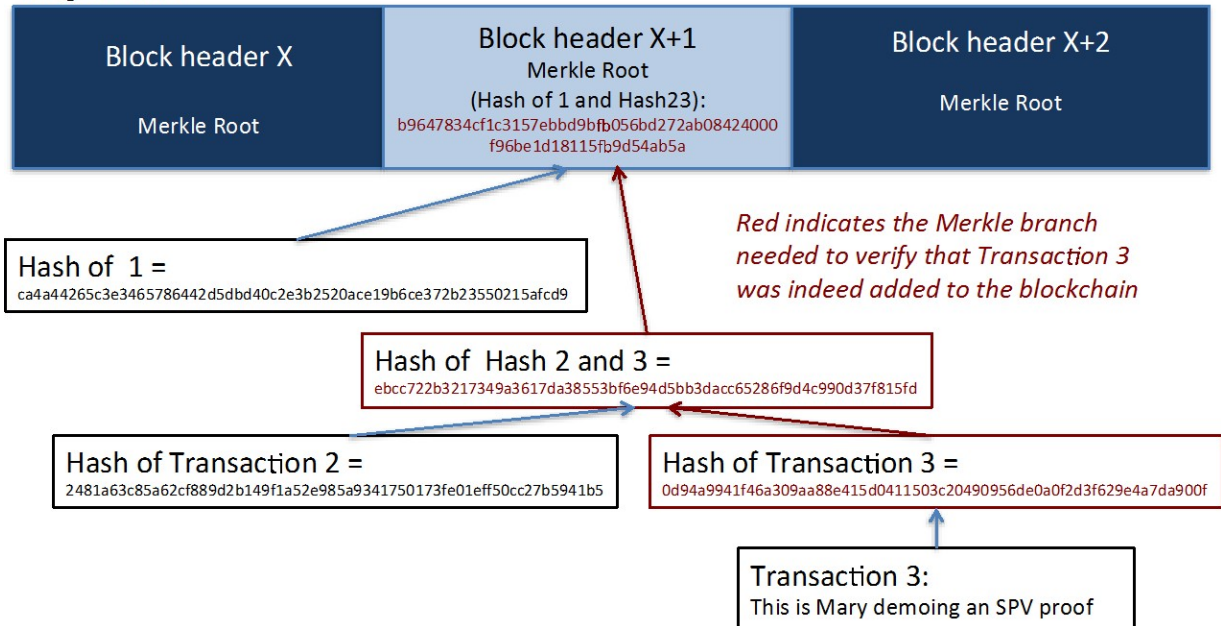


Figure B.4: Example of an SPV Proof

Sources: Nakamoto (2008) and Bitcoinwiki.org

Suppose you want to prove that the text, *“This is Mary demoing an SPV proof”* was verified and secured on the blockchain. You could use an algorithm that grabs the Merkle branches for the text. This proves that (a) the network did verify and accept your transaction and (b) the fact that other blocks come after it further establishes that the text is in the permanent ledger (and not in a temporary soft fork).

Smart Contract: A smart contract is a bit of programming logic that stores rules of engagement that are agreed upon among trading partners. Once parties launch the smart contract live on a blockchain network, the terms of the agreement automatically execute. Nick Szabo invented the concept.⁸⁸

Appendix C: GS1 Standards

We focus more on GS1 data standards because members of our BC CoE Executive Advisory Board are working close with GS1 to expand existing standards to accommodate supply chain blockchain applications, particularly in food and pharmaceutical traceability (see Table C.1).

GS1 is a not-for-profit organization that develops and maintains data standards for business communications. It was founded in 1969 by US retailers searching for ways to speed up checkout. Today, GS1 is a global entity. Its management board includes Amazon; Alibaba Group; Carrefour; eBay; Google; Independent Grocers Association; Johnson & Johnson; Mondelez; Nestlé; Procter & Gamble; Smuckers; Walgreens; and WalMart.

According to Melanie Nuce, Senior Vice President, Corporate Development at GS1 US, blockchain solutions require additional data fields to be included in GS1 standards:

“The primary use cases we’ve been addressing are in the pharmaceutical and food safety sectors. There’s a lot of missing data that’s going to prevent companies from building these really large ecosystems. Most enterprises are not capturing the data, so it cannot be shared. We’ve really been trying to emphasize the fundamental messages of: you have to know what you’re trying to share, with whom you’re trying to share it, and how you’re going to go about sharing it, regardless of the technology you use.”

GS1’s global standards are widely adopted in supply chain contexts. The individual standards work in concert to facilitate the tracing of products through a supply chain. For example, Figure C.1 shows a hierarchy of codes comprising GLN, GSIN, SSCC, and GTIN data standards (see Table C.1).

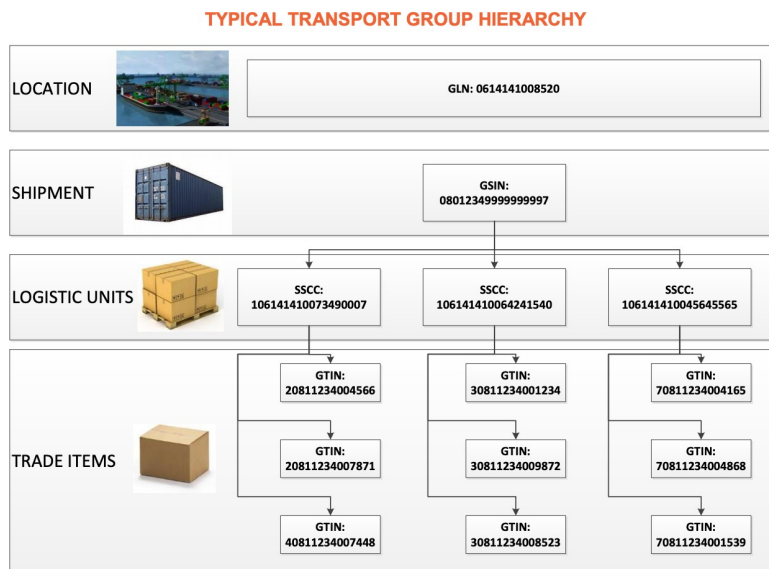



Figure C.1: Example of how GS1 standards work in concert to track items through a supply chain

Source: https://www.gs1si.org/CashEDI/Doc/GSIN_Intro.pdf

Table C.1 Examples of GS1 Data Standards		
Sample GS1 Standards	Describes	Description
Global Location Number (GLN)	Parties and locations	Includes codes for company prefix and location reference; A location could be a room within a building, a dock door, and accounts payable department. ⁸⁹
Serial Shipping Container Code (SSCC)	Logistical units	Includes codes for company prefix and serial reference. It's an 18-digit barcode, preceded by a "(00)", placed on the outside of a shipping container/pallet that uniquely identifies the contents. ⁹⁰
Global Shipping Identification Number (GSIN)	Shipments	Includes codes for application identifier, company prefix, shipping reference. ⁹¹ <div style="text-align: center;"> <p>Example of a GSIN with a 7-digit GS1 Company Prefix</p>  <p>(402) 0801234 999999999 7</p> <p>Application Identifier GS1 Company Prefix Shipper Reference Check Digit</p> </div>
Global Trade Item Number (GTIN)	Products and services	GTIN includes codes for company prefix, item reference. For example, the GTIN number 038900006198 maps to "Dole Crushed Pineapple in Its Own Juice, 8 oz" ⁹²

GS1's EPCIS and EDIFACT standards help trading partners execute business transactions (see Table C.2). An EDIFACT message comprises an interchange header (UNA), functional group header (UNB), message header UNH), user data types (as required), message trailer (UNT), functional trailer (UNE) and interchange trailer (UNZ). Below is a message to check for flight availability:⁹³

```

UNA:+.? '
UNB+IATB:1+6XPPC:ZZ+LHPPC:ZZ+940101:0950+1'
UNH+1+PAORES:93:1:IA'
MSG+1:45'
IFT+3+XYZCOMPANY AVAILABILITY'
ERC+A7V:1:AMD'
IFT+3+NO MORE FLIGHTS'
ODI'
TVL+240493:1000::1220+FRA+JFK+DL+400+C'
PDI++C:3+Y::3+F::1'
APD+74C:0::6+++++6X'
TVL+240493:1740::2030+JFK+MIA+DL+081+C'
PDI++C:4'
APD+EM2:0:1630::6+++++DA'
UNT+13+1'
UNZ+1+1'

```

Table C.2 Examples of GS1 Electronic Standards		
Electronic Product Code Information Services (EPCIS)	Event data	"Product X with serial numbers 111, 112, and 113 were observed at 10:23am on April 2017 at Location ABC, during a 'shipping' operation." ⁹⁴
Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT)	Documents, messaging	EDIFACT comprises an interchange header, functional group header, message header, user data types, message trailer, functional trailer and interchange trailer. ⁹⁵

ⁱⁱ UPC 038900006198 is associated with Dole Crushed Pineapple In Its Own Juice, 8 oz

<https://www.upcitemdb.com/upc/38900006198>

Appendix D. Additional Interoperability Projects

The full report covered some of major blockchain interoperability projects including the Interledger Protocol (ILP); Hyperledger Quilt; Accenture’s Interoperability Node; BT Relay; BitGo; and Liquid. Our literature review also produced many mentions of Aion, Cosmos, Polkadot, and Wanchain (see Figure D.1). Well-respected blockchain gurus founded these projects; they are governed by foundations and are transparent and well-funded. In our opinion, these projects are worth monitoring.

Aion, Cosmos, Polkadot, and Wanchain are all aiming to produce interoperability solutions that meet the technical criteria of atomicity, security, and universality. They all have native digital tokens to mirror assets in other chains, to incentivize and reward validators, and to prevent Denial of Service (DoS) attacks. Their solutions use SPV proofs and hash-time locked contracts. Aion, Cosmos, and Polkadot are based on hub-and-spoke designs. However, their consensus mechanisms, message formats, and message types differ. At least two of these projects are considering how their interoperability solutions will work with each other; leaders from Aion, Wanchain, and Icon decided it was in the best interests of all parties to share information. They formed the Blockchain Interoperability Alliance in 2017, to establish a common standard for inter-chain communications, but little follow-up information exists about its progress.⁹⁶

Next, we cover the four projects in more detail.

Blockchain Interoperability Projects





				
Hub	Aion Connection	Cosmos hub	Relay Chain	Wanchain
Spoke	Spoke	Zones	Parachain	
Consensus	Lightweight BFT with 2/3 vote; Hybrid DPoS and PoI	Tendermint’s PoS and BFT	PoS	PoS
Founded	Deloitte leads founded in 2016	Ethan Buchman & Jae Kwon (CEO Tendermint) in 2016; Nuco ties	Gavin Wood (Co-founder of Ethereum fame)	Jack Lu (Lives in Austin TX)
Token Sale Funds	\$22 million in 2017 (AION)	\$17 million in 2017 (ATOM)	\$144 million in 2017 (DOT)	\$36 million in 2017 (WAN)
Governed	The Aion Foundation, Canada	Interchain Foundation, Switzerland	Parity Technologies/Web3 Foundation, UK	Wanchain Foundation, Singapore
Products	TokenBridge alpha released in May 2018	IBC (InterBlockchain Communication) protocol keeps a constant record of total tokens in each zone	Genesis block scheduled Q3 2019	Wanchain 1.0, 2.0, and 3.0 are launched;
Notes	Focused on connecting public & private chains	Focused on connecting public chains, particularly Bitcoin & Ethereum	Had a bug in their multisign wallet;	Mainnet PoS scheduled to go live 4 th quarter 2019.

Figure D.1: Overview of Aion, Cosmos, Polkadot, and Wanchain

Aion

Introduction. Three Deloitte blockchain leads — Kesem Frank, Matthew Spoke, and Jinius Tu — started Aion in 2016.⁹⁷ Aion is a project of Nuco, a Toronto-based blockchain startup company that hails Vitalik Buterin (architect of Ethereum) as an advisory board member.⁹⁸ Aion raised \$22 million in an Initial Coin Offering (ICO) and token sales.⁹⁹ The AION token is used to pay transaction fees to miners in the Aion network and to prevent DoS attacks (since the perpetrator would run out of tokens). Aion is an open

source project governed by the Aion Foundation, of which Matthew Spoke and Jin Tu serve as directors (no other directors are listed).¹⁰⁰ The Aion Foundation holds about 30 percent of the circulating and locked supply of the AION coins.¹⁰¹ As of December 2018, Aion had spent \$10 million and had opened offices in Canada, Barbados, and China.¹⁰²

Technical Overview. Aion is based on the idea of a federated blockchain network, with a multi-tier, multi-hub-and-spoke design (see Figure D.2). From its 2017 white paper, Aion aims to:

- Route messages between different blockchain networks through a common bridging protocol that involves translation and propagation of the message, which must be considered final.
- Provide decentralized accountability.
- Provide a bridging protocol.¹⁰³

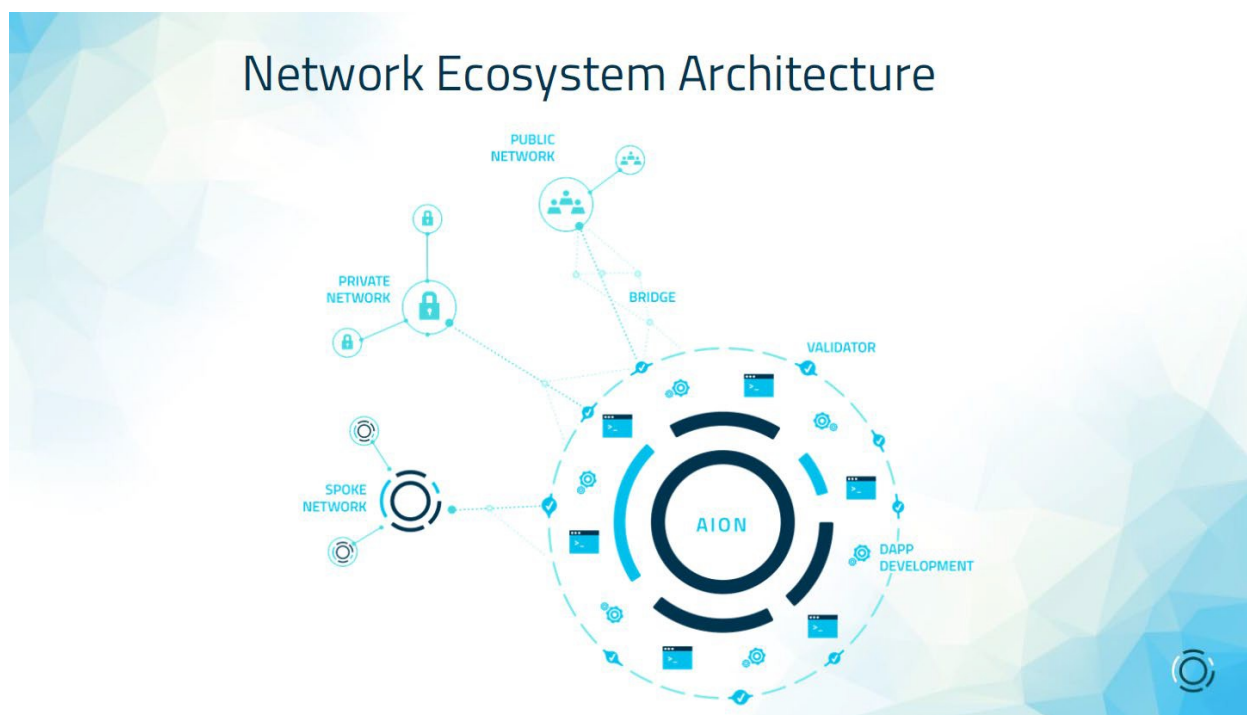


Figure D2: Aion Network

Source: https://cryptocanucks.com/wp-content/uploads/2018/04/ii_jgflzq780_162feb0b36955db3.png

In the Aion network, a *bridge* signs and broadcasts interchain transactions, provided two-thirds of the *validators* have voted to approve the transaction.

Aion's interchain transaction format defines (1) a payload of data specific to the originator, (2) metadata about the interchain transaction such as the to/from networks, transaction hash, Aion transaction fee, and digital signature, and (3) an optional Merkle proof (see Figure D.3).¹⁰⁴

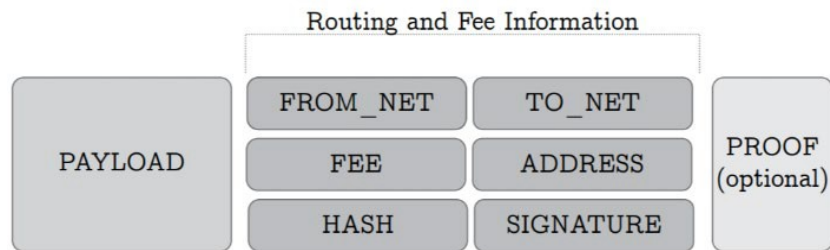


Figure D.3: Aion's Interchain Transaction Format

Source: <https://learn.aion.network/docs/why-is-aion-network-different>

Progress. The Aion Network's mainnet first phase called 'Kilimanjaro' went live in April 2018. The network can be explored on <https://mainnet.aion.network/#/dashboard>. Its first version connected the Aion network to an Ethereum Virtual Machine (EVM). According to Aion's website, the second phase, 'Denali', will deliver the Aion Virtual Machine (AVM); Aion Scripting language; and a proof-of-intelligence (PoI) consensus protocol that requires miners to perform an artificial intelligence computation.¹⁰⁵ The third phase, called 'Everest', will launch the participating network bridge, a validator nominator for the Hybrid DPoS/PoS consensus mechanism, and the second version of AVM.¹⁰⁶ As of January 2019, three million AION have been mined. Overall, the chatter on social media praises the foundation for being transparent about their finances, coin distribution, and aims.

Cosmos

Introduction. Jai Kwon and Ethan Buchman, the CEO and CTO of Tendermint, wrote the 2016 Cosmos white paper titled, *A Network of Distributed Ledgers*.¹⁰⁷ Cosmos is governed by the Interchain Foundation, with three Board members (Kwon, Buchman, and one other). Cosmos raised \$16 million in the first eight minutes of its ICO in 2017.¹⁰⁸ Its token is called Atom. The public holds 75 percent of the tokens; the Interchain Foundation holds 10 percent; Tendermint holds 10 percent; and seed investors hold 5 percent.¹⁰⁹ The coins are not yet traded on any exchange.¹¹⁰

Technical Overview. Cosmos is a permissionless blockchain project that proposes to connect different blockchains through its hub. The idea is that Cosmos will create the hub as the first blockchain, and it will connect to other sovereign blockchains called zones, which can be either public or private¹¹¹ (see Figure D.4).

The Cosmos network will use Tendermint's proof-of-stake consensus algorithm, and its interface is called Application BlockChain Interface (ABCI). Cosmos chose 100 validators, which will increase 13 percent each year until it reaches 300 validator nodes.¹¹² Validator nodes will get paid in Atoms, or with other tokens. They must maintain a stake of tokens to continue serving the validator role. Validators that do not vote in a timely manner or behave maliciously will be deactivated.¹¹³

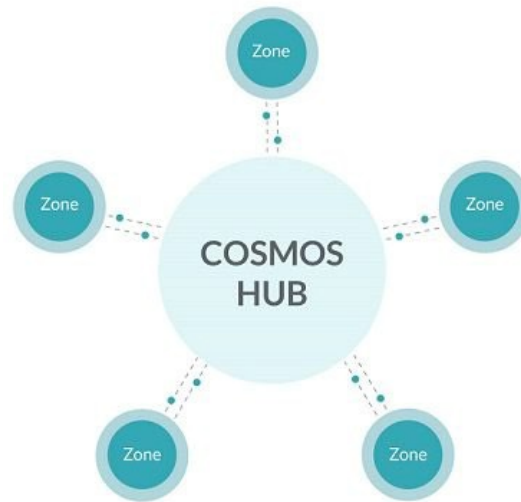


Figure D.4: Cosmos’ proposed solution for blockchain interoperability

Source: <http://news.sys-con.com/node/4201542>

To connect the Cosmos Hub to zones, it will use the Inter-Blockchain Protocol (IBC), (see Figure D.5).¹¹⁴ The IBC protocol is payload agnostic. The IBC uses SPV proofs. Here is a simple explanation:

*“Let us take an example where an account on chain A wants to send 10 tokens X on chain B. First, these tokens are locked on chain A. Then, a proof that these 10 tokens X are locked is relayed from chain A to chain B. Chain B tracks the validator set of chain A. If the proof is signed by more than two-thirds of chain A’s validators, then it is valid, and 10 tokens X are created on chain B. Note that the tokens that have been created on chain B are not actually **real** tokens X, as token X only exists on chain A. They are just a **representation** on B of tokens X from chain A, along with a proof that these tokens are frozen on chain A.”*¹¹⁵

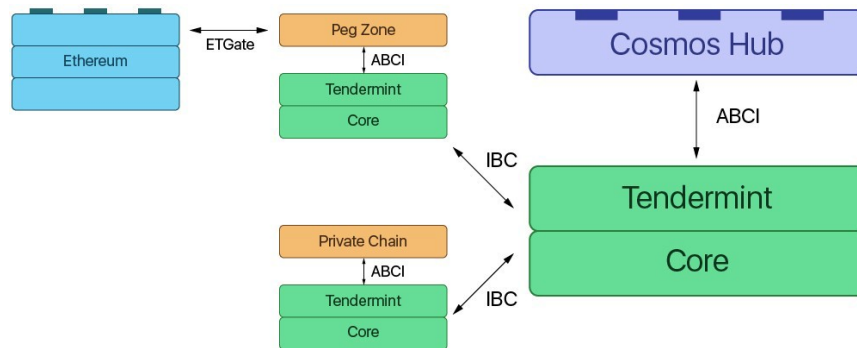


Figure D.5. Cosmos Hub and Spoke Detail

Source: <https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecaef63350d116>

In this figure, the Cosmos Hub interacts with two other blockchains, which run on top of Tendermint. They read and act upon states through the IBC protocol. The top left depicts a peg zone, which connects to other live blockchain networks, in this case, Ethereum.

The IBC packet has the following fields:

1. **Sequence:** an unsigned, arbitrary-precision integer
2. **Source:** a string uniquely identifying the chain, connection, and channel from which this packet was sent
3. **Destination:** a string uniquely identifying the chain, connection, and channel which should receive this packet
4. **Data:** an opaque application payload¹¹⁷

Progress. According to the Cosmos White Paper, they tested the performance using 64 nodes located in seven data centers on five continents, and were able to process thousands of transactions per second (TPS) with one to two second commit times.¹¹⁸ Thus far, the project has completed a security audit and a Game of Stakes testnet. Cosmos' genesis transaction and mainnet was launched March 13, 2019.¹¹⁹

Polkadot

Introduction. Gavin Wood, the co-founder of Ethereum, founded Polkadot. Parity Technologies and the Web3 Foundation govern Polkadot. Polkadot raised \$145 million with its ICO in October of 2017. DOT is its digital asset. Half of the tokens were sold during the ICO, and the other half are held by Web3 Foundation and in reserve for projects. In January of 2019, Polkadot announced it would have a second token sale, hoping to raise an additional \$60 million.¹²⁰

Technical Overview. Polkadot's relay chain coordinated consensus and makes sure transactions are delivered to parachains and bridges (see Figure D.6).

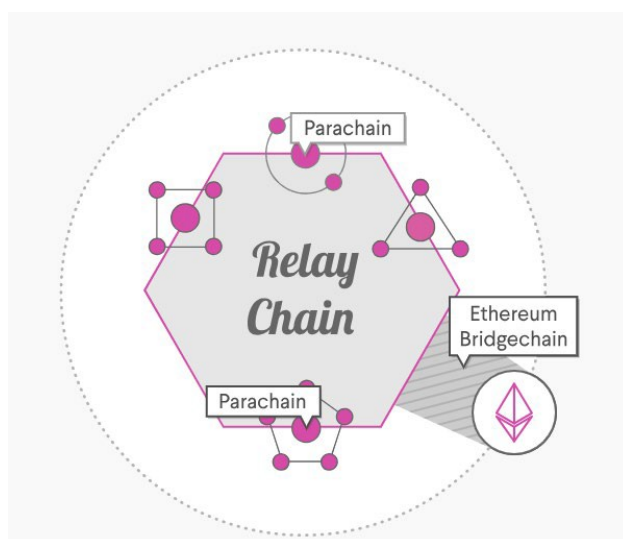


Figure D.6: Polkadot Architecture Overview

Source: <https://polkadot.network/#whatisit>

Relay chains coordinate transactions and consensus between chains.

Parachains gather and process transactions.

Bridges link to other blockchains, such as Ethereum.

Polkadot's verification method consists of 'nominators', 'validators', 'collators' and 'fishermen' nodes, each securing the network in different ways (see Figure D.7).¹²¹ Nominators stake DOTs on validators. Collators maintain parachains and produce state transition proofs for validators. Fisherman nodes troll the network for bad behaviors and submit proofs of bad behaviors to validators.¹²² Blocks are produced by randomly selected validator nodes and then finalized via BFT agreement before creating the next block, with a consensus protocol called Nominated Proof-of-Stake. With this method, "nominators choose the block validators by staking tokens on the presumed strongest candidate, and the validators in return are bonded heavily by their stakes. Any misbehavior is punishable by a slash."¹²³

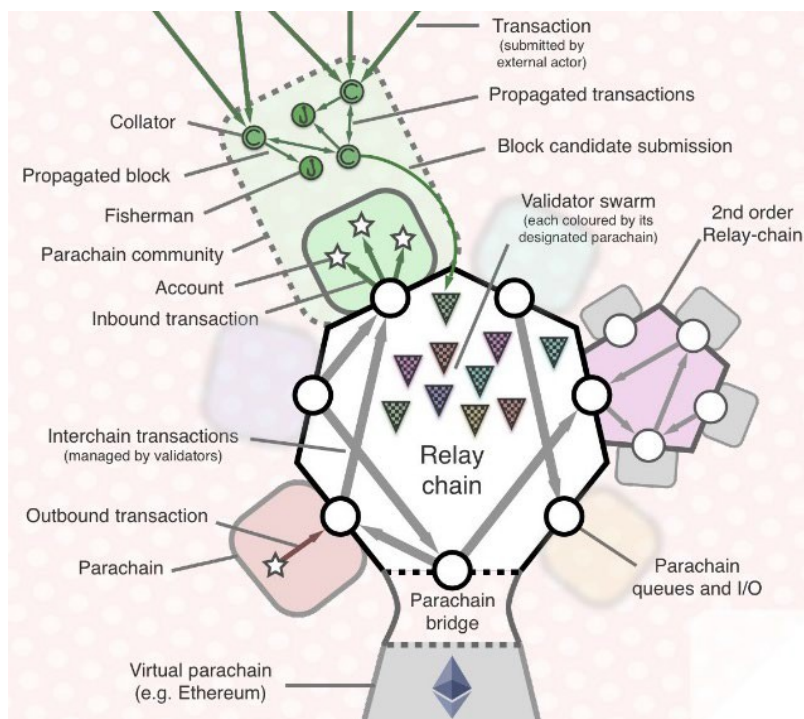


Figure D.7: Polkadot's Architecture in Detail

Source: <https://image.slidesharecdn.com/polkadotprezo-170329122819/95/polkadot-presentation-7-638.jpg?cb=1490790541>

Progress. Polkadot's testnet called Substrate went live in May of 2018.¹²⁴ It plans to release the mainnet in the third quarter of 2019.

Wanchain

Introduction. Wanchain, founded by Jack Lu in Beijing and Austin Texas, is a protocol that aims to connect blockchains. The Wanchain Foundation, registered as a non-profit in Singapore, governs Wanchain. Wanchain raised \$36 million with its ICO in October of 2017 in just 12 minutes.¹²⁵ Wanchain's token is called Wanchain (WAN). During its ICO, 107 million WAN were sold, leaving 103 million for the development of the solution. According to its white paper, the coins are allocated as follows: 60% for research and development, 10% for community development, 10% for marketing, 10% for infrastructure and 10% for daily operations.¹²⁶

The Wanchain network is launched and can be viewed at <https://explorer.wanchain.org/>.

Technical Overview. Based on an Ethereum hard fork, Wanchain allows intrachain transactions using Ethereum’s protocol but with the addition of ring signatures to ensure privacy (similar to Monero). Locking an asset on one blockchain, minting a new proxy token for that asset as it enters the Wanchain, and then connecting it to other blockchains, accomplishes cross-chain transactions. Wanchain itself is a blockchain that will record cross-chain and intra-chain transactions (see Figure D.8.)¹²⁷ Wanchain uses a proof-of-stake consensus protocol. Three verification nodes are specified: cross-chain transaction proof ‘voucher’ nodes, locked account management ‘storeman’ nodes, and ‘validator’ nodes. The verification nodes earn transactions fees.¹²⁸

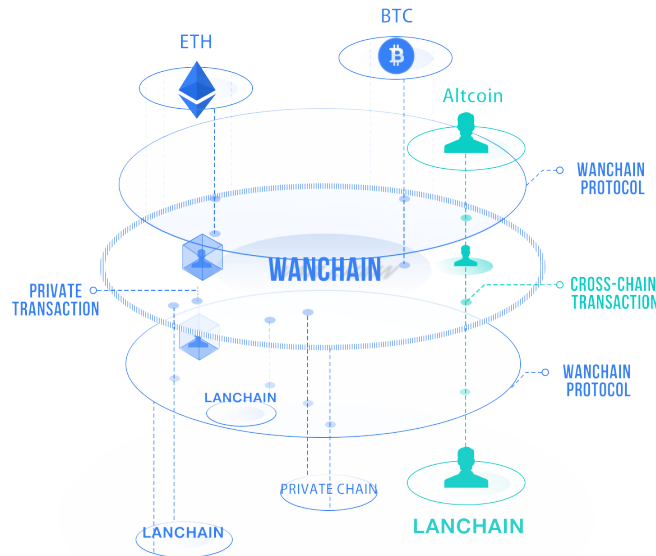


Figure D.8: Wanchain’s proposed solution for blockchain interoperability

Source: <https://wanchain.org/>

Lanchain allows private cross-chain smart contracts. So far, Wanchain has implemented bridges to Bitcoin and Ethereum.

Progress. According to its roadmap, Wanchain 1.0 was released in January of 2018, with two subsequent versions released at six-month intervals. Wanchain 2.0 connected Wanchain to Ethereum. “*Ether can be transferred cross-chain from Ethereum’s blockchain and accurately represented 1:1 on Wanchain’s blockchain with a proxy token called WETH (WAN-ETH).*”¹²⁹ Wanchain 3.0 connected Wanchain to Bitcoin, using the proxy token WBTC. It also has proxy tokens for Dai, Aurora, Loopring, Chainlink, Crptocurve, and BlockMedX.¹³⁰ Its major release for the mainnet with the proof-of-stake, cross-chain transaction protocol is scheduled to go live in the fourth quarter of 2019.¹³¹

Endnotes

¹ Buterin, V. (September 9, 2016), *Chain Interoperability*, <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf>

² Hyperledger Blog (May 24, 2018), *One Year Later: Interoperability & Standardization Shine at Consensus*, <https://www.hyperledger.org/blog/2018/05/24/one-year-later-interoperability-standardization-shine-at-consensus>

³ Buterin, V. (September 9, 2016), *Chain Interoperability*, <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf>

⁴ Hyperledger Blog (May 24, 2018), *One Year Later: Interoperability & Standardization Shine at Consensus*, <https://www.hyperledger.org/blog/2018/05/24/one-year-later-interoperability-standardization-shine-at-consensus>

⁵ Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2018) *Blockchain Technology Overview*, NIST Draft NISTIR 8202, <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf> (Curiously, NIST's definition appeared in a preliminary report that now holds the status "withdrawn".)

⁶ Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf>

⁷ Ackerman, J. and Meier, M. (2018), *Blockchain 3.0: The Next Generation of Blockchains*, https://www.researchgate.net/profile/Jakob_Ackermann5/publication/327672110_Blockchain_30_-_The_next_generation_of_blockchain_systems/links/5b9e146a299bf13e60348b65/Blockchain-30-The-next-generation-of-blockchain-systems.pdf?origin=publication_detail

⁸ Gartner Report G00315765; Gartner PeerInsights (2018) *Review of Blockchain Platforms*.

⁹ Chandler, S. (December 15 2018), *From South Korea to IBM Food Trust – How Blockchain is Used in the Food Industry*. CoinTelegraph.

¹⁰ Several websites rate over 100 food traceability software products. For example, see: Capterra, *Food Traceability Software*, <https://www.capterra.com/food-traceability-software/>

Software Advice, *Food Traceability Software*, <https://www.softwareadvice.com/distribution/food-traceability-comparison/>

¹¹ Enterprises also need increased blockchain scalability; Blockchain 1.0 and 2.0 technologies typically process 50 or fewer transactions per second for public blockchains and fewer than four thousand transactions per second for private blockchains, whereas some enterprise applications need to process tens of thousands of transactions per second.

CryptoCoin (October 15, 2018), *The Fastest Cryptocurrency Transaction Speeds for 2018*.

O'Keefe, D. (June 5, 2018), *Understanding Cryptocurrency Transaction Speeds*.

¹² Lucasxhy (September 11, 2018), *Cross-Chain-Interoperability*, <https://medium.com/@lucx946/cross-chain-interoperability-3566695a1a72>

¹³ https://en.wikipedia.org/wiki/Standards_organization

¹⁴ Tanenbaum, A. and Wetherall, D. (1981), *Computer Networks*, Boston, Prentice Hall, 5th edition, p. 702.

¹⁵ GS1 (2017) EPCIS and CBV Implementation Guideline, Release 1.2., Ratified, Feb 2017, https://www.gs1.org/docs/epc/EPCIS_Guideline.pdf

¹⁶ Mainelli, M. (January 3, 2017), *Which way for blockchain standards in 2017?* Coindesk, <https://www.coindesk.com/which-way-for-blockchain-standards-in-2017>

¹⁷ Deshpande, A., Stewart, K., Lepetit, L. and Gunashekar, S. (2017), *Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards*, BSI/RAND white paper, <https://www.bsigroup.com/en-IE/Innovation/dlt/>

-
- ¹⁸ <https://www.gs1us.org/what-we-do/about-gs1-us/media-center/press-releases/detail/articleid/1302/gs1-us-launches-cross-industry-blockchain-discussion-group>
- ¹⁹ <https://blockchain.ieee.org/>
- ²⁰ *Standards Catalogue: ISO/TC 307 Blockchain and DLT*, <https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0>
- ²¹ <https://www.nist.gov/publications/blockchain-technology-overview>
- ²² Coleman, L. (August 8 2018), *China to Draft for Three Domestic Blockchain Standards in 2018*, CNN, <https://www.cnn.com/china-to-drafts-for-three-domestic-blockchain-standards-in-2018>
- ²³ DIF Website, Identifiers, Names and Discovery Working Group, <https://identity.foundation/working-groups/identifiers-names-discovery.html>
- ²⁴ <https://www.omg.org/hot-topics/distributed-immutable-data-object.htm>
- ²⁵ The Web Ledger Protocol 1.0, <https://w3c.github.io/web-ledger/>
- ²⁶ <https://www.xbrl.org/tag/blockchain/>
- ²⁷ About the IEEE Blockchain Initiative <https://blockchain.ieee.org/about>
- ²⁸ Iwata, H., Tominaga, T. and Morikawa, T. (2018), Trends in Standardization of Blockchain Technology by ISO/TC 307, *NTT Technical Review*, 1-5.
- ²⁹ International harmonized stage codes <https://www.iso.org/stage-codes.html#30.60>
- ³⁰ *Standards Catalogue: ISO/TC 307 Blockchain and DLT*, <https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0>
- ³¹ W3C Blockchain Community Group: <https://www.w3.org/community/blockchain/>
- ³² W3C Github site, *Format and protocol for decentralized Ledgers on the Web*, <https://w3c.github.io/web-ledger/>
- ³³ The Web Ledger Protocol 1.0 <https://w3c.github.io/web-ledger/>
- ³⁴ The Web Ledger Protocol 1.0 <https://w3c.github.io/web-ledger/>
- ³⁵ Meijer, C. (September 20, 2016), *Blockchain and standards: first things first!* FinExtra, <https://www.finextra.com/blogposting/13114/blockchain-and-standards-first-things-first>
- ³⁶ Deshpande, A., Stewart, K., Lepetit, L. and Gunashekar, S. (2017), *Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards*, BSI/RAND white paper, <https://www.bsigroup.com/en-IE/Innovation/dlt/>
- ³⁷ TE-Food (May 25, 2018), *The role of GS1 in blockchain based food traceability*, <https://medium.com/te-food/the-role-of-gs1-in-food-traceability-857c1a1d1642>
- ³⁸ Lacity, M. (2018), Addressing Key Challenges to Making Enterprise Blockchain Applications a Reality, *MIS Quarterly Executive*, 17(3), pp. 201-222.
- ³⁹ Personal interview with Mary Lacity and Kate Moloney.
- ⁴⁰ Personal interview with Mary Lacity and Kate Moloney.
- ⁴¹ Personal interview with Mary Lacity and Kate Moloney.

⁴² Personal interview with Mary Lacity.

⁴³ The technical requirements come from several sources, particularly from Jin, H., Dai, X., Xiao, J. (2018), Towards a Novel Architecture for Enabling Interoperability Amongst Multiple Blockchains, *IEEE 38th International Conference on Distributed Computer Systems*, pp. 1203-1211. We also relied on:

Treat, D., Giordano, G., Schiatti, L., Borne-Pons, H. (Oct 22, 2018), *Connecting ecosystems: Blockchain integration*, Accenture White Paper, <https://www.accenture.com/us-en/insights/blockchain/integration-ecosystems>

Hardjono, T., Lipton, A., and Pentland, A. (2018), *Towards a Design Philosophy for Interoperable Blockchain Systems*, MIT Connection Science, <https://arxiv.org/pdf/1805.05934.pdf>

⁴⁴ While both REST APIs and RPCs are similar, RPC runs programs directly on the kernel on the server system while REST APIs focus on the data as a resource. RPCs focus on specific functions that need to be done and are controlled while REST APIs focus on sharing data out and allowing CRUD updates without specific functions running on the platform.

⁴⁵ https://en.bitcoin.it/wiki/Original_Bitcoin_client/API_calls_list

⁴⁶ <https://etherscan.io/apis>

⁴⁷ Jin, H., Dai, X., Xiao, J. (2018), Towards a Novel Architecture for Enabling Interoperability Amongst Multiple Blockchains, *IEEE 38th International Conference on Distributed Computer Systems*, pp. 1203-1211.

⁴⁸ https://en.bitcoin.it/wiki/Proof_of_burn

⁴⁹ Hallam, G. (May 2 2016), *The BTC Relay is live! Bitcoin can now exist on the Ethereum blockchain*. Post to Reddit: https://www.reddit.com/r/Bitcoin/comments/4hhtwh/george_hallam_the_btc_relay_is_live_bitcoin_can/

⁵⁰ Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf>

⁵¹ <http://btcrelay.org/>

⁵² Ethereum, *Welcome to BTC Relay's Documentation!*, <https://btc-relay.readthedocs.io/en/latest/index.html>

⁵³ BTC Relay's transactions can be viewed at <https://etherscan.io/address/0x41f274c0023f83391de4e0733c609df5a124c3d4>

⁵⁴ Buterin, V. (September 9, 2016), *Chain Interoperability*, <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf>

This video is also helpful in explaining notaries, multisig federations, and SPV proofs: James, c. (January 6, 2018), *Bitcoin Sidechains & SPV Proofs*, <https://www.youtube.com/watch?v=rzLhw7Xl1uo>

⁵⁵ For our interoperability discussion, notaries are trusted third parties. There are also projects in which smart contracts can serve as a notary, such as POEX.io that is used to 'time stamp' a document.

⁵⁶ Lerner, S. D. (April 2016), *Drivechains, sidechains, and hybrid 2-way peg designs*, https://uploads.strikinglycdn.com/files/27311e59-0832-49b5-ab0e-2b0a73899561/Drivechains_Sidechains_and_Hybrid_2-way_peg_Designs_R9.pdf

⁵⁷ Treat, D., Giordano, G., Schiatti, L., Borne-Pons, H. (Oct 22, 2018), *Connecting ecosystems: Blockchain integration*, Accenture White Paper, <https://www.accenture.com/us-en/insights/blockchain/integration-ecosystems>

⁵⁸ <https://newsroom.accenture.com/news/accenture-enables-interoperability-between-major-blockchain-platforms.htm>

-
- ⁵⁹ Treat, D., Giordano, G., Schiatti, L., Borne-Pons, H. (Oct 22, 2018), *Connecting ecosystems: Blockchain integration*, Accenture White Paper, <https://www.accenture.com/us-en/insights/blockchain/integration-ecosystems>
- ⁶⁰ Treat, D., Giordano, G., Schiatti, L., Borne-Pons, H. (Oct 22, 2018), “*Connecting ecosystems: Blockchain integration*”, Accenture White Paper, <https://www.accenture.com/us-en/insights/blockchain/integration-ecosystems>
- ⁶¹ <https://www.businesswire.com/news/home/20181022005892/en/Accenture-Enables-Interoperability-Major-Blockchain-Platforms>
- ⁶² <https://en.wikipedia.org/wiki/Multisignature>
- ⁶³ Lerner, S. D. (April 2016), *Drivechains, sidechains, and hybrid 2-way peg designs*, https://uploads.strikinglycdn.com/files/27311e59-0832-49b5-ab0e-2b0a73899561/Drivechains_Sidechains_and_Hybrid_2-way_peg_Designs_R9.pdf
- ⁶⁴ Higgins, S. (August 3, 2016), *The Bitfinex Bitcoin Hack: What We Know (And Don't Know)*. News Article, CoinDesk
- ⁶⁵ Press release (November 15 2018), *BitGo First to Deliver Multi-Signature Security for Over 100 Coins and Tokens*, <https://www.businesswire.com/news/home/20181115005640/en/BitGo-Deliver-Multi-Signature-Security-100-Coins-Tokens>
- ⁶⁶ Kharif, O. (February 19 2019), *Crypto Startup Offers Insurance Against Quadriga Wallet Dilemma*, Bloomberg, https://www.bloomberg.com/news/articles/2019-02-19/crypto-startup-offers-insurance-against-quadriga-wallet-dilemma?srnd=cryptocurrencies&utm_campaign=chain_letter.unpaid.engagement&utm_source=hs_email&utm_medium=email&utm_content=70058664&_hsenc=p2ANqtz-
- ⁶⁷ Lerner, S. D. (April 2016), *Drivechains, sidechains, and hybrid 2-way peg designs*, https://uploads.strikinglycdn.com/files/27311e59-0832-49b5-ab0e-2b0a73899561/Drivechains_Sidechains_and_Hybrid_2-way_peg_Designs_R9.pdf
- ⁶⁸ Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., and Wuille, P. (Oct 22 2014), *Enabling Blockchain Innovations with Pegged Sidechains*, <https://blockstream.com/sidechains.pdf>
- ⁶⁹ Buterin, V. (September 9, 2016), *Chain Interoperability*, <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf>
- ⁷⁰ Buterin, V. (September 9, 2016), *Chain Interoperability*, <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf>
- ⁷¹ “Back, A., Friedenbach, M., Miller, A., Poelstra, A., Timon, J., and Wuille, P. (Oct 22 2014), *Enabling Blockchain Innovations with Pegged Sidechains*, <https://blockstream.com/sidechains.pdf>
- ⁷² <https://blockstream.com/liquid-faq/>
- ⁷³ *SPV, Simplified Payment Verification*, Bitcoin.Org glossary.
- ⁷⁴ Lerner, S. D. (April 2016), *Drivechains, sidechains, and hybrid 2-way peg designs*, https://uploads.strikinglycdn.com/files/27311e59-0832-49b5-ab0e-2b0a73899561/Drivechains_Sidechains_and_Hybrid_2-way_peg_Designs_R9.pdf
- ⁷⁵ Thomas, S., and Schwatz, E, (2015), *A Protocol for Interledger Payments*, <https://interledger.org/interledger.pdf>
- ⁷⁶ Interledger Payments Community Group <https://www.w3.org/community/interledger/>
- ⁷⁷ Hashed-Timelock Agreements (HTLAs) <https://interledger.org/rfcs/0022-hashed-timelock-agreements/>
- ⁷⁸ Hyperledger Quilt, <https://www.hyperledger.org/projects/quilt>

⁷⁹ Chatham House Rule, https://www.chathamhouse.org/chatham-house-rule?gclid=EAlaIqobChMkaCERbbK4AIVeR-tBh2CoAJREAAAYASAAEgl9JvD_BwE

⁸⁰ Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2018), *Blockchain Technology Overview*, NIST Draft NISTIR 8202, <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf> (Curiously, NIST's definition appeared in a preliminary report that now holds the status "withdrawn".)

⁸¹ Jin, H., Dai, X., Xiao, J. (2018), *Towards a Novel Architecture for Enabling Interoperability Amongst Multiple Blockchains*, IEEE 38th International Conference on Distributed Computer Systems, pp. 1203-1211.

⁸² Buterin, V. (2016), *Chain Interoperability*, <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Cchain+Interoperability.pdf>

⁸³ *The Differences Between Hard and Soft Forks*, posted by We Use Coins on August 23, 2016 on <https://www.weusecoins.com/hard-fork-soft-fork-differences/>

⁸⁴ *Hard & Soft Forking Explained*, by Loshil and MLPFrank on <https://www.youtube.com/watch?v=pdaXY1OOiWQ>

⁸⁵ Proof of Burn was developed by Iain Stewart,

⁸⁶ Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf>

⁸⁷ *Simplified Payment Verification*, Bitcoinwiki.org.

⁸⁸ Szabo, N. (September 1997), *Formalizing and Securing Relationships in Public Networks*, FirstMind, Vol, 2, 9, DOI: <https://doi.org/10.5210/fm.v2i9.548>

⁸⁹ Global Location Number (GLN) Implementation Guide (2002), https://www.naesb.org/pdf3/weq_jiswg052108w1.pdf

⁹⁰ SSCC (Serialized) Barcodes for Master Cartons, Pallets, and Skids https://www.simplybarcodes.com/Serialized-shipping-carton_SSCC-18-Barcodes.html

⁹¹ https://www.gs1si.org/CashEDI/Doc/GSIN_Intro.pdf

⁹² UPC 038900006198 is associated with Dole Crushed Pineapple In Its Own Juice, 8 oz <https://www.upcitemdb.com/upc/38900006198>

⁹³ <https://en.wikipedia.org/wiki/EDIFACT> EDIFACT comprises an interchange header (UNA), functional group header (UNB), message header UNH), user data types (as required), message trailer (UNT), functional trailer (UNE) and interchange trailer (UNZ). Below is a message to check flight availability:

```
UNA:+.? '
UNB+IATB:1+6XPPC:ZZ+LHPPC:ZZ+940101:0950+1'
UNH+1+PAORES:93:1:IA'
MSG+1:45'
IFT+3+XYZCOMPANY AVAILABILITY'
ERC+A7V:1:AMD'
IFT+3+NO MORE FLIGHTS'
ODI'
TVL+240493:1000::1220+FRA+JFK+DL+400+C'
PDI++C:3+Y::3+F::1'
APD+74C:0::6+++++6X'
TVL+240493:1740::2030+JFK+MIA+DL+081+C'
PDI++C:4'
APD+EM2:0:1630::6+++++DA'
UNT+13+1'
UNZ+1+1'
```

⁹⁴ Banker, S. (February 15, 2019), GS1 Will Have A Role To Play In Supply Chain Blockchain Applications, *Forbes*, <https://www.forbes.com/sites/stevebanker/2019/02/15/gs1-will-have-a-role-to-play-in-supply-chain-blockchain-applications/#27aecc77615d>

⁹⁵ <https://en.wikipedia.org/wiki/EDIFACT>

⁹⁶ Presentation at Invest Conference, November 28, 2017 <https://youtu.be/SPk1-PRrafU>

⁹⁷ https://en.wikipedia.org/wiki/Aion_Network

⁹⁸ <https://en.wikipedia.org/wiki/Nuco>

⁹⁹ Cuen, L. (December 5 2018), *Aion Token Project Estimates 18-Month Runway After Bitcoin and Ether Sales*, Coindesk, <https://www.coindesk.com/aion-token-sells-crypto-for-fiat>

¹⁰⁰ Michael del Castillo (Jun 20, 2016, updated Jun 21, 2016) Crowdfund Insider, *Deloitte Blockchain Leads Depart to Launch New Startup*, <https://www.crowdfundinsider.com/2017/10/122975-aion-ico-pre-sale-raises-7-2m-week-adds-22-million/>

¹⁰¹ Aion Foundation Report (January 31, 2019). Download the report from this website: <https://www.aion.org/how-we-operate/>

¹⁰² Cuen, L. (December 5 2018), *Aion Token Project Estimates 18-Month Runway After Bitcoin and Ether Sales*, Coindesk, <https://www.coindesk.com/aion-token-sells-crypto-for-fiat>

¹⁰³ Spoke, M. and Nuco Engineering Team, (2017), Aion White Paper, <https://aion.network/media/en-aion-network-technical-introduction.pdf>

¹⁰⁴ Spoke, M. and Nuco Engineering Team, (2017), Aion White Paper, <https://aion.network/media/en-aion-network-technical-introduction.pdf>

¹⁰⁵ What does the Aion roadmap look like? <https://learn.aion.network/docs/what-does-the-aion-roadmap-look-like>

¹⁰⁶ What does the Aion roadmap look like? <https://learn.aion.network/docs/what-does-the-aion-roadmap-look-like>

¹⁰⁷ Kwon, J. and Buchman, E. (2019) Cosmos White Paper, *A Network of Distributed Ledgers*, <https://cosmos.network/resources/whitepaper>

¹⁰⁸ <http://cryptoeconomy.info/2017/04/06/cosmos-ico-over-17-m-raised-in-just-8-minutes/>

¹⁰⁹ Lutsch, F. (October 26 2018), *Proof-of-Stake Contenders: An Overview of the Cosmos Network*, <https://blog.chorus.one/proof-of-stake-contenders-cosmos-network/>

¹¹⁰ <https://www.cryptocompare.com/coins/atomstar/overview>

¹¹¹ <https://cosmos.network/about/whitepaper>

¹¹² <https://blockgeeks.com/guides/cosmos-blockchain-2/>

¹¹³ Blockgeeks, *What is Cosmos Blockchain? The Most Comprehensive Guide*, <https://blockgeeks.com/guides/cosmos-blockchain-2/>

See also details of Cosmos governance: https://github.com/cosmos/cosmos/blob/master/GOVERNANCE_DOC.md

¹¹⁴ <https://cosmos.network/about/whitepaper>

¹¹⁵ Martin, G. (April 3 2018), *Understanding the Value Proposition of Cosmos* <https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecaef63350d>

-
- ¹¹⁶ Martin, G. (April 3 2018), *Understanding the Value Proposition of Cosmos* <https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecae63350d>
- ¹¹⁷ <https://cosmos.network/docs/spec/ibc/channels-and-packets.html> - 32-definitions
- ¹¹⁸ Kwon, J. and Buchman, E. (2019) *Cosmos White Paper, A Network of Distributed Ledgers*, <https://cosmos.network/resources/whitepaper>
- ¹¹⁹ <https://cosmos.network/roadmap>
<https://www.coindesk.com/a-blockchain-to-connect-all-blockchains-cosmos-is-now-officially-live>
- ¹²⁰ Khatri, Y. (January 25, 2019), *Blockchain Project Polkadot Plans Second Token Sale to Raise \$60 Million*, Coindesk, <https://www.coindesk.com/blockchain-project-polkadot-plans-ico-to-raise-another-60-million-report>
- ¹²¹ Fransham, J. (November 27, 2018), *Never Fork Again*, <https://medium.com/polkadot-network/never-fork-again-438c5e985cd8>
- ¹²² Polkadot. <https://polkadot.network/#howitworks>
- ¹²³ Block, E. (October 27, 2018), *Polkadot*, <https://coinsavage.com/content/2018/10/polkadot/>
- ¹²⁴ Khatri, Y. (January 25, 2019), *Blockchain Project Polkadot Plans Second Token Sale to Raise \$60 Million*, Coindesk, <https://www.coindesk.com/blockchain-project-polkadot-plans-ico-to-raise-another-60-million-report>
- ¹²⁵ Wanchain <https://en.bitcoinwiki.org/wiki/Wanchain>
- ¹²⁶ Wanchain Commercial white paper <https://wanchain.org/files/Wanchain-Commercial-Whitepaper-EN-version.pdf>
- ¹²⁷ Wanchain is a fork of Ethereum and uses Monero style-ring signatures (it's a tumbling mechanism that creates privacy) to help secure multi-party compute. <https://wanchain.org/>
- ¹²⁸ Wanchain white paper <https://wanchain.org/files/Wanchain-Whitepaper-EN-version.pdf>
- ¹²⁹ Lu, J. (October 17, 2018), *The Importance of Blockchain Interoperability*, <https://medium.com/wanchain-foundation/the-importance-of-blockchain-interoperability-b6a0bbd06d11>
- ¹³⁰ Wanchain Mainnet Tokens <https://explorer.wanchain.org/tokens>
- ¹³¹ Wanchain Roadmap <https://wanchain.org/roadmap>