Massachusetts Institute of Technology
Media Lab's Digital Currency Initiative
Sloan School of Management

The Shipping Industry & Blockchain Interoperability

Authors: Kenny Li (MIT Sloan), Eilon Shalev (MIT Sloan)

Keywords: Blockchain, Interoperability, Shipping Industry

Blockchain Lab Program
2018-2019 Working Groups Cycle
Taught by N. Narula, G. Gensler, S. Johnson, and M. Casey
Member Company: Deloitte
Project Group: Blockchain Interoperability

The Shipping Industry & Blockchain Interoperability

Introduction

In this paper, we discuss the definition of interoperability and blockchain interoperability, we identify three interoperability solutions and discuss their risks and risk mitigation methods, and we provide a market landscape of the shipping industry, all to suggest a framework for addressing interoperability issues. This paper serves as an initial approach to blockchain interoperability from both tech and business perspectives, and more research should accompany this paper to assess the challenges and solutions for blockchain interoperability in other industries, as well as further the research in the shipping industry.

Interoperability - Why Is It a Problem?

Before we discuss Blockchain Interoperability, we wish to establish a definition for the term, to which all the following assumptions, conclusions, and recommendations will adhere.

The oxford dictionary defines interoperability as: *"The ability of computer systems or software to **exchange** and **make use** of information"*[1]. By Blockchain Interoperability, we discuss the ability of computer systems or software that is specifically built on blockchain infrastructure, either public or private. We identify two parts to this definition:

1. Ability to exchange information; and
2. Ability to make use of the information that was exchanged.

Several papers[2] and opinions[3][4][5] have been written about Blockchain Interoperability, and we believe that they answer the first aspect of interoperability quite well - yes, it is technically possible for two different blockchains to exchange information, with some interesting limitations that we will further discuss. But what about the second aspect? The ability to make use of the information that was exchanged.

What does the ability to make use of the information mean? We argue that make use of information entails taking business decisions that include business logic that relates to the use case at hand. As such, we chose

1 https://en.oxforddictionaries.com/definition/interoperability
2 https://www.r3.com/wp-content/uploads/2017/06/chain_interoperability_r3.pdf
3 https://medium.com/@seelemonsonline/unlocking-corda-ethereum-interoperability-pt-1-1ea1413fe95f
4 https://medium.com/@seelemonsonline/unlocking-corda-ethereum-interoperability-pt-2-4a350d8ccd18
5 https://medium.com/@seelemonsonline/unlocking-corda-ethereum-interoperability-pt-3-15aa4de97e40

to follow a carefully picked business use case—supply chain in the shipping industry—to go through how business decisions are made, and whether Blockchain Interoperability is a viable expectation to have. We chose this use case because of market interest, as well as the merit of the line of reasoning behind using blockchain in this use case. Blockchains provide time-stamped, append-only logs that are shared among multiple stakeholders with various writing and reading permissions; stakeholders who can leverage this technology to reconcile information and value exchanges more quickly, and as such benefit from cost savings in two dimensions: cost of verification and cost of networking[6].

With the above-mentioned context in mind, the technical problem is solvable in several ways, and we will discuss three of them: 1. Notary Schemes; 2. Relays; and 3. Hash-Locking.
In September 2016, Vitalik Buterin published a report[7] with R3, discussing some of these technical solutions and their limitations:

1. Notary Schemes are trusted parties that help participants on Chain A confirm that some event occurred on Chain B, and vice versa.
2. Relays are systems inside of one blockchain that can validate and read events and/or states in other blockchains.
3. Hash-locking means setting up operations on chain A and chain B that have the same trigger, usually the revelation of the preimage of a particular hash.

Notary Schemes

The technical logic in the Notary Schemes solution is that multiple participants from various chains trust a third party or several third parties to facilitate cross-chain interoperability. Those trusted entities have a direct technical link to both chains and can facilitate cross-chain transactions. In this paper, this is the only solution that introduces a third party or third parties. As such, we wanted to dive deeper into the complexity created by introducing these notary entities. Not only might Chain A and Chain B participants not trust each other, but they now also need to agree on a trusted third party. At a small scale, these third parties might create extra friction in achieving a consensus around who is and what constitutes a trusted third party, however, at a large scale, it is reasonable to assume that the trusted third party will be trusted more easily and quickly by new entrants of the ecosystem, and as such reduce the cost of networking and cost of reconciliation[8]. For a notary-schemes solution, both the scale of the network and the difficulty level of achieving consensus around who are trusted third parties might play an important part at implementation.

6 https://www.nber.org/papers/w22952.pdf
7 https://www.r3.com/wp-content/uploads/2017/06/chain_interoperability_r3.pdf
8 https://www.nber.org/papers/w22952.pdf

Relays

The technical logic in the Relays solution is that participants on Chain A and Chain B know how to technically validate events that occurred on the other Chain. While this makes sense from a technical perspective, we introduce a question to those participants: do you trust the way the other Chain participants take decisions? Do you trust the governance? Do you trust the resiliency? In other words, and more practically, would participants on the Bitcoin blockchain trust Ethereum users and the other way around? After all, the dispute among the developers with regards to the consensus protocol and governance led to the creation of those two, somewhat competing—for nodes and network participants—blockchain networks. Moreover, would users on Bitcoin trust users on Bitcoin Cash or Bitcoin Gold? If the answer is yes, and given that technically it is possible, then Relays can be used to facilitate interoperability across various blockchains, as long as the chains involved are still functioning and haven't been compromised.

Hash-locking

The technical logic in the hash-locking solution is equivalent to establishing a smart contract between Chain A and Chain B. Technically, that makes sense. However, and as mentioned above in the Relays section, we would like to challenge the reasoning behind creating such a smart contract in the first place. Why are the chains interested in interoperating? And why were the distinct chains created in the first place. In some cases, the reason behind the creation of those two chains is disagreement on the consensus protocol: PoW vs PoS, proof of work and proof of stake respectively. And so, if the protocols are so different from one another, that network developers decided to diverge, how come now they are willing to both technically exchange information and make use of this information? How can the network participants on the two different application layers trust one another, if the developers had disagreements about the underlying consensus protocols. This technical solution is prone to problems if a corresponding Chain is not functioning or compromised.

To sum, the risks associated with relying not only on the above-mentioned interoperability solutions, but also on any interoperability solution are: 1. Creating exposure of information to distrusted parties; 2. Losing accessibility to important information stored in a corresponding Chain; and 3. Using information that was compromised.

Mitigating those risks are key, if one wants to use an application built on Chain A that interoperates with an application built on Chain B. In some cases, these risks need not be intimidating. For example, and specifically in the shipping industry, if a shipping company believes that both Chain A and Chain B have acceptable blockchain infrastructure from several point of views: resiliency, consensus protocol, governance, and future

existence, then it should feel comfortable using any solution, and more importantly, relying on interoperability to facilitate the exchange and use of information across these chains.

Market Landscape

What existing solutions are available and what are the value propositions and potential limitations of each?

Due to the nascency of the blockchain industry, no ideal solution for interoperability exists for the industry currently. While many projects are emerging to tackle data and ecosystem interoperability, none has delivered a fully scalable product. Community projects such as Interledger and Aion are making strides in creating an interoperable future for public blockchains, private blockchains, and centralized ledgers, but the technology is not mature enough for plug-and-play, and enterprise adoption would require a heavy commitment to build and maintain a scalable use case. On the other hand, use-case-specific solutions are emerging such as Tradelens, which is backed by IBM and Maersk. Some of these solutions are abstracting the blockchain, giving the users a product that provides data authenticity without the user needing to ever interact with the blockchain layer. Others take a more blockchain-centric approach, requiring users to store their own private keys (e.g., Wave).

Industry-specific Solutions

Private Blockchain: Tradelens

Tradelens[9], which processes over 10 million events per week for the global supply chain industry, is a blockchain-powered platform that stores the source of shipping data. It is a collaboration between team members from both IBM and Maersk. The collaboration is working on a blockchain solution that allows shipping companies to verify the authenticity of all documents manifested throughout the supply chain. According to the company, these documents can be digital or non-digital formats. The Tradelens solution creates a hash of the document, and the hash is what is stored on the blockchain. Whether the original document is an image upload or PDF, it is the hash of that uploaded file that is moved to the Tradelens blockchain. From there, Tradelens can verify the authenticity of documents that are shared among stakeholders in the ecosystem. In phase 2, Tradelens is moving to the store of the data itself in the IBM enterprise blockchain, rather than limiting itself to the hash of the data. This phase, though, would require not just the adoption of its own solution but also a shift in its consumers' habits. Projects like Vechain (public

9 https://www.tradelens.com/

blockchain) are working to tackle the phase 2 problem, but do not have a scalable solution at the time of writing.

Limitations

The Tradelens solution is limited in its granularity for authenticity at this point. While it is able to store files such as inventory documents, it cannot verify the authenticity of the individual items within the inventory. Phase 2 of the project tackles this problem by storing data such as Bill of Lading information directly on the blockchain, but the phase is conceptual now.

Public Blockchain: CargoX

CargoX[10] operates its smart-contract-based Bill of Lading, Smart B/L, on the Ethereum blockchain. It offers a centralized SaaS interface that allows its users to create and process B/Ls directly on the interface, with its data stored on the Ethereum blockchain. CargoX was created by the team that created 45HC, which was founded in 2015. Since the start of CargoX, it seems that the 45HC project has been abandoned; its booking application returns no results regardless of the search inputs, and its latest blog entry occurred on April 5, 2017. Smaller competitors such as WaveBL are also tackling the value proposition of B/L on the blockchain.

Limitations

Similar to the Tradelens strategy on focus, CargoX is limited to the use case of Bill of Lading. The user onboarding process also involves a (see Appendix: Figures & Images - Figure 1) step that requires the user to be familiar with blockchain and private keys, which increases the learning curve and potentially curbs user adoption. Also, CargoX raised funds through an ICO (CXO Token). We believe that CargoX performed this ICO through partnership with a company called TokenMarket because CargoX's smart contract source code references an Apache Licensing term to the code licensed by TokenMarket[11]. The value of the token is dependent on the actions of a common enterprise (CargoX) and the company discusses pricing as a reason for buying the token. This does subject CargoX to potential securities regulation especially if it intends to deal with U.S. users.

10 https://cargox.io/
11 https://etherscan.io/address/0xb6ee9668771a79be7967ee29a63d4184f8097143#code Line 10

General Interoperability Projects

Community Projects: Interledger (& Hyperledger Quilt) - Transaction interoperability

Interledger protocol[12] is an open source project that connects ledger architectures. These ledgers can be distributed (i.e., blockchain) or centralized. Interledger conducts these connections and allows for transactions across ledgers using hash time-lock contracts (HTLCs), which are essentially atomic swaps[13]. With this type of approach, hashing must occur on both ends to unlock a transaction; therefore, if the transaction is cross-chain, both blockchains must use the same hashing algorithm. Interledger's interoperability standards are defined by the World Wide Web Consortium. Hyperledger Quilt[14] is Hyperledger's implementation of Interledger. Quilt is maintained by one full-time resource from each of the following companies: Everis (owned by NTT Data), NTT Data, and Ripple.

Limitations

The key value propositions from HTLCs are transaction related. Therefore, transferring data (even data as simple as hashes of data) is not a use case for HTLCs. Furthermore, from an operational perspective, because the project is not a packaged solution, a user would need to commit resources to support the development and maintenance of a custom solution for its own requirements within the community.

Public Blockchain: Aion - Data interoperability

Aion[15] refers to itself as a blockchain network. It builds on the premise that the future will be dominated by several different individual blockchain protocols; in that scenario, Aion positions itself to be a network to disseminate data among dissimilar blockchains through use of its Connecting Networks. Originally built as a fork of Ethereum, Aion recently proposed a hybrid PoW/PoS consensus protocol named Unity[16].

The Aion project has also recently made progress by demonstrating a transfer of Maven tokens between the Aion and Ethereum blockchain[17]. Aion sets itself apart from other blockchain-based interoperability projects like Wanchain and community projects like Interledger by offering the ability to interoperate not just for transactions, but also smart contracts.

12 https://interledger.org/
13 https://en.bitcoin.it/wiki/Atomic_swap
14 https://www.hyperledger.org/projects/quilt
15 https://aion.network/
16 https://blog.aion.network/unity-consensus-draft-paper-published-211004e5827e
17 https://www.youtube.com/watch?v=M53ou8S4ioY

Limitations

Similar to the Interledger project, Aion is also not an out-of-the-box solution; therefore, a user would need to commit resources to the development and maintenance of a custom-built solution.

A Framework for Interoperability & BoLs

Data Speed

- The speed at which the data must transact is a necessary question. For a Bill of Lading use case, immediacy is not required; therefore, a public PoW or PoS blockchain or a permissioned blockchain can each be a solution. The user should consider the extended use case of blockchain and how it can be applied to the company; if it is limited to non-urgent appends, then all three blockchains are available solutions. On the other hand, if the data requires immediacy (e.g., a point-of-sale transaction), then PoW blockchains such as Ethereum (as of now) will not match the requirements of the company, and only public PoS or permissioned blockchains should be considered.

Interoperability

- Unfortunately, at this time, blockchain interoperability is limited regardless of the initiatives ongoing in the space.
    - *API/Ecosystem:* the availability of APIs allows third-party application development on top of the existing platform. Solutions including Tradelens and CargoX offer API integration, giving companies more flexibility in how they interact with the respective platforms, as well as the ability for additional third-party services to build additional solutions that can leverage the platform and underlying data. With Tradelens, access to the API is public and available through Swagger[18]. CargoX's API[19] is available upon request to partners and clients.
    - *Data:* a universal standard does not currently exist regarding data storage on the blockchain. This explains why projects such as Tradelens store hashes of files on the blockchain, while projects such as CargoX store raw data for Bill of Lading on the blockchain. Data interoperability is non-existent at this point, although projects such as Aion are working to become the bridge between blockchains, allow disparate chains to conduct transactions and transfer information (the project is in progress, and is far from enterprise-grade usability). Enterprise blockchain solutions such as Tradelens, which is powered by IBM's blockchain solution (Fabric), lean

18 https://docs.tradelens.com/reference/api_documentation/
19 https://cargox.io/platform/API-integrations/

towards ecosystem interoperability but intend to control the blockchain layer; therefore, it does not have any plans to create or assist in creating data bridges to other blockchains. Solutions built on Ethereum have a higher likelihood of data interoperability--at least with other solutions built on Ethereum--due to the single, consistent layer: Ethereum. This layer provides a hashing standard and allows data to be shared without leaving the blockchain and potentially depending on a third-party (e.g., notary schemes or oracles).

Operational Integration

- The company should consider the operational implications that are involved in implementing one solution over another. The increase in flexibility with regards to operational changes to achieve a company's blockchain adoption strategy is positively correlated with the variety of choices that the company has for solutions; i.e., the more flexibility a company has, the more choices it has for solutions.
    - If the company has very low flexibility, then the ideal solution would be one that requires 1) little to no change in its daily operations, and 2) a familiar user experience that requires minimal specialized knowledge. In this case, a solution such as Tradelens would be ideal, as it provides no direct exposure to the blockchain layer and allows its users to preserve its existing operational practices.
    - If the company's strategy is more flexible, it can consider options that 1) provide more exposure to the blockchain layer, and 2) offers more data resiliency through writes directly to the blockchain. For example, Wave requires rudimentary knowledge of blockchain to generate and hold a private key but allows users to write information for a Bill of Lading directly into the Ethereum blockchain.

Data Formatting

- Hash Only: Hash-only data stores are primarily used for validation of authenticity. The advantages of this methodology:
    1. Relies on the fact that hashing can be applied to any digital format: PDF, text, images, video, audio, etc.
    2. Aligns more closely with existing user experience: the ability to hash any type of digitized file allows for flexibility. For players in the industry that still use paper documents, an image or scan of the paper document can be hashed and stored on the blockchain (with the caveat being that the original paper itself cannot be authenticated via the blockchain, but rather the original image or scan becomes the reference document to prove authenticity).

Once the hash of a file is written to the blockchain, the authenticity of that file can be verified by comparing the stored hash vs. the presented document's hash. The disadvantage in this methodology is two-fold:

1. Its inability to store the raw data. The contents of the file are hashed; therefore, the contents of the file themselves are not stored on the blockchain. This means that the original file must still be preserved and referenced.
2. Its dependence on the original file. Because the hash is stored, the original file is the only file that can be referenced. For images, this means that another photo of the exact same document cannot be used, because the resulting hash will be different than the original photo of the document. Even text documents cannot be re-saved to produce the same hash due to the metadata (e.g., timestamps).

- Raw Data Storage: Raw data storage places all of the data on the blockchain. It eliminates the need of a hash of files because it contains the contents of files themselves. This type of storage is use-case specific and will require more changes to existing processes for entering and storing shipping information. If participants traditionally use paper documents, for example, then they must transition into a digital storage process that requires interaction with digital devices rather than paper formats.

  The advantage of this process is that the use case for Bill of Lading already exists through startups like Wave. Furthermore, the option is superior to physical copies of B/Ls because they do not need to be transported from one party to the next. It is also superior to centralized B/Ls because the authenticity and ownership of each B/L can be verified and tracked by the blockchain.

  The disadvantage of this process is, as mentioned previously, that the use cases are limited. While the solution is arguably superior to the existing, transforming fragmented methodologies requires operational changes, not just a technological transformation.

Conclusion

Currently, various solutions exist and/or are being developed for the shipping industry. Each one takes a different approach in applying blockchain technology to solve the issue of verifying contracts and documents. This report provides a framework for assessing which solution(s) best fit a company's specific criteria for its blockchain adoption strategy, and any related interoperability considerations associated with each choice. Taking the time to consider the implications behind decisions such as data formatting, data storage, and API access will better position a company to select the right strategy not only based on current needs, but also its level of integration with blockchain in the future.

Appendix

Figure 1

CargoX Sign-up Process

The interface of CargoX exposes users to the blockchain layer. It requires them to create a private key or connect via a hardware wallet.