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

Success Factors for a Blockchain Consortium

Authors: Celine Dana Christory, Racem Benhamed, Sarah Xu, and Jeremy Obadia

Keywords: Blockchain Consortium

Blockchain Lab Program
2019-2020 Working Groups Cycle
Taught by N. Narula, G. Gensler, and S. Johnson
Member Company: Boston Consulting Group (BCG) Platinion
Project Group: Blockchain Consortium

SUCCESS FACTORS FOR A BLOCKCHAIN CONSORTIUM

Abstract

This research paper conducted as part of the Blockchain Lab (15.217) class at MIT, in collaboration with BCG Platinion aims at identifying the key success factors for blockchain consortia.

Celine Dana Christory, Racem Benhamed, Sarah Xu, Jeremy Obadia

29/05/2020

Executive Summary

Blockchain consortium has become more popular among businesses. The number of consortia increased from 1 in 2014 to 231 in 2020. Firms are interested in staying close to technology and leveraging it to improve operational efficiency gains. It is a hybrid of public and private blockchain where it keeps the decentralized structure while it is less resource-intensive.

Despite the rising interests and potential benefits, there is not a killer case yet. Most of the existing blockchain consortium has not been able to scale. Many more have died. It takes us to the question of what the success factors are for blockchain consortium. There have been several reports and op-eds discuss the success factors and challenges facing blockchain consortium. Our study provides insights by drawing lessons from literature, expert interviews, case studies, and survey. The success factors are discussed in depth. The findings are intended to inform industry, academia, and government to promote sustainable development of blockchain consortium.

Our findings include the following:

Success factors by rank

- We identified five success factors: business use case, governance, operation, data privacy, and regulation.
- The business use case is the most crucial success factor for blockchain consortium. This will become even more prominent during the post-COVID as firms are cutting capital investment. Governance is another critical factor, although less so than the business use case. Data privacy and regulation are less a challenge for blockchain consortium because methods have been developed to mitigate the constraints, such as private chain, sharding.

Relationships among success factors

- Blockchain is necessary for the success of a business use case. It also improves trust among members. However, it seems to be independent of governance.
- Trust can be improved through well-managed competition dynamics, blockchain technology, and governance. Trust turns out to be higher among horizontal players, and lower among vertical players. Blockchain technology appears to be promising in enhancing trust. Governance is the hardest way to improve trust. It needs to incentivize commitment from members or increase transparency to achieve greater trust. Otherwise, governance is independent of trust.

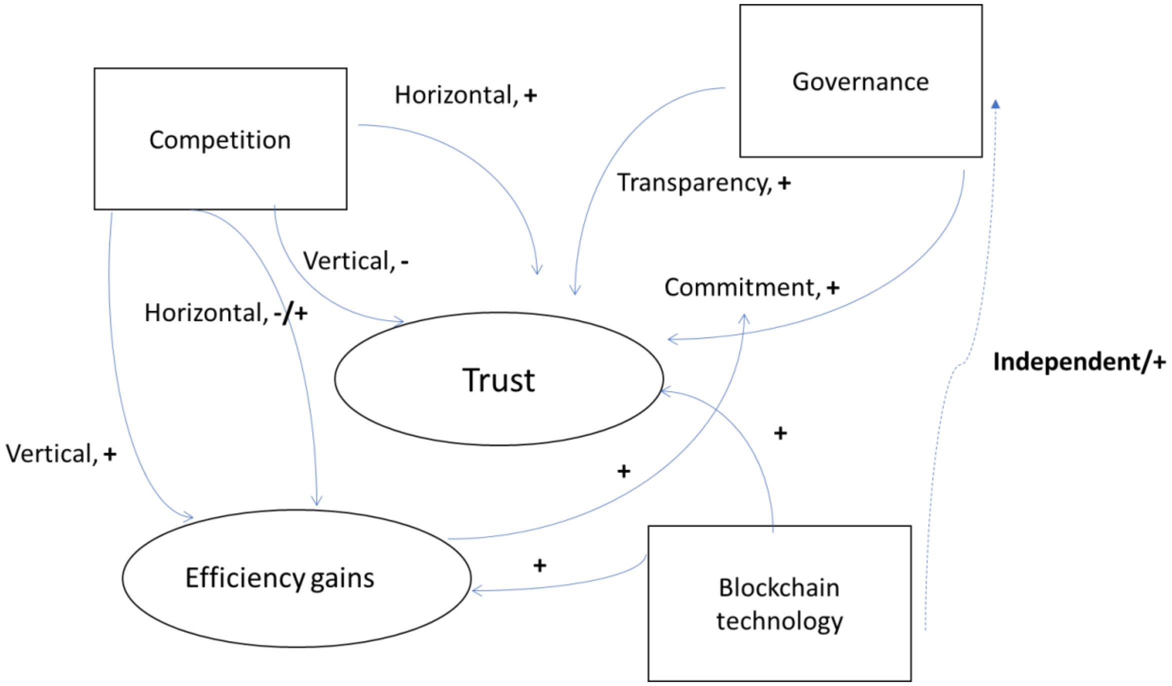


Figure 1: Diagram illustrating relationships between success factors.

Table of Contents

I. Project Problem and Scope

a. Scope and Problem

Blockchain consortium is defined as a group of companies form a consortium using blockchain technology and develop blockchain-enabled business. There have been growing interests among businesses in understanding blockchain technology and using it in their products and services. The consortium brings interested firms together to collaborate. It helps the firms to stay close to the technology, share resources, know what competitors are doing, develop blockchain-enabled products more efficiently, setting influencing standards, or simply due to fear of missing out.

The finance consortium dominates the consortia space. Finance consortia are focusing on trade finance, insurance, KYC requirement, transactions and processing, standards-setting, and research. Other consortium types include logistics, healthcare, energy, and anti-counterfeit, etc. The number of consortia has been increasing from 1 in 2014 to 231 in 2020. The initiatives spread across the globe, covering the U.S., Europe, China, India, Australia, and BRICS, etc.

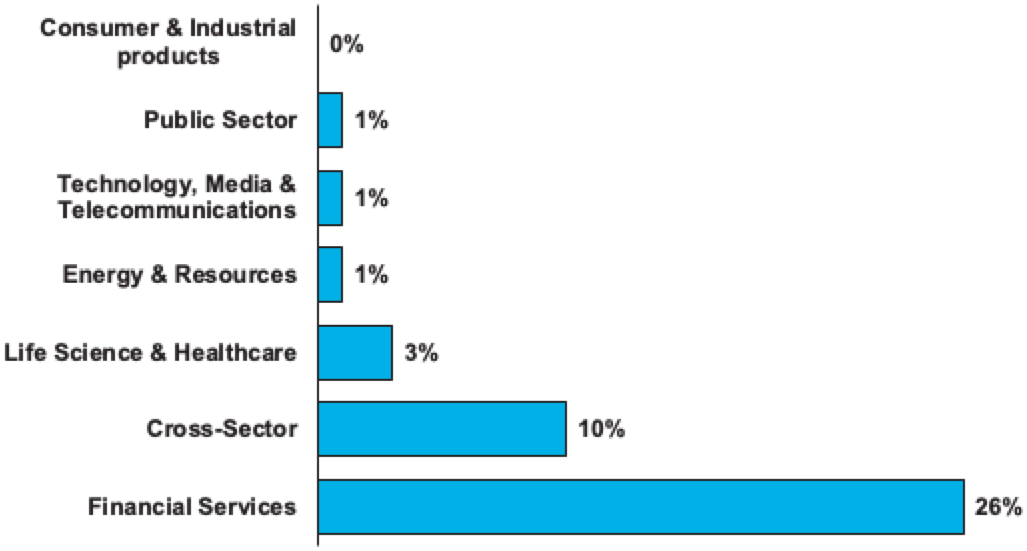


Figure 2: Consortium by industry. Source: Deloitte.

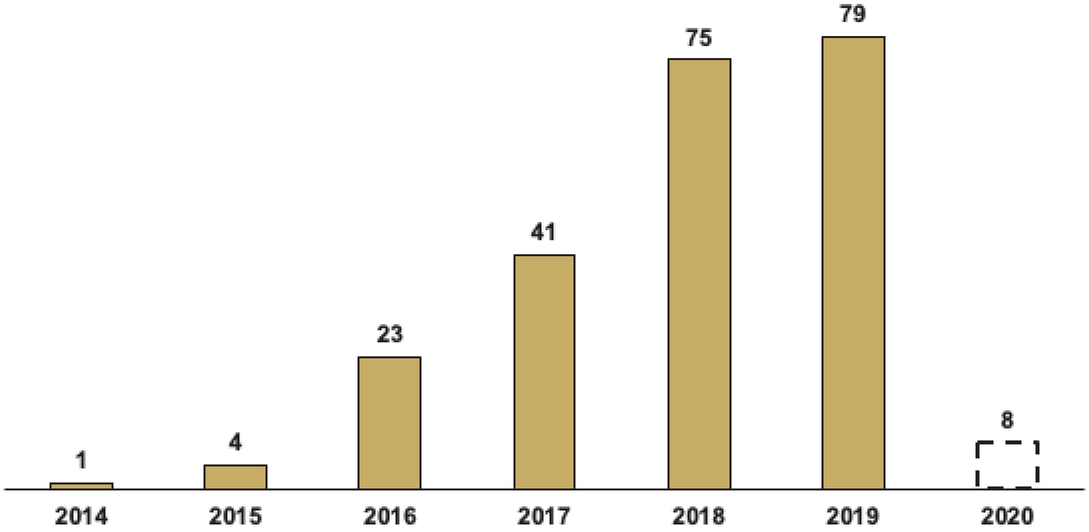


Figure 3: The number of consortia launched every year from 2014 to 2020. Source: ESG Intelligence.

However, despite growing interests, there is no killer use case yet. There is considerable uncertainty around the business values of the consortium for it to thrive. Some consortia are more successful than others, such as MarcoPolo, and We.Trade. Yet, many others struggled to create value or failed. We believe the potential of blockchain in helping firms to run more efficiently and digitally. The blockchain consortium could be used to foster trust, collaboration, or the development of specific blockchain products that are appealing to all members. In this study, we want to study why the blockchain consortium has not achieved strong business values as it was initially predicted. Specifically, we are going to answer:

What are the success factors for a blockchain consortium?

Our scope focuses on the blockchain consortium that serves business use cases for its members. The data, solutions, and infrastructure are open and administered only to and by its members. We interviewed experts to get their views on the success factors of blockchain consortia. We have conducted a survey to ask consortia and their members on the design of their blockchain consortia and the success and challenges that they face. We also draw lessons from literature, industry reports, and op-eds to identify the success factors. Based on this information, we provide recommendations on how to build a successful blockchain consortium. The results can be useful lessons to further the development of blockchain consortium.

The paper is organized as the following. Section one is the scope and problem of blockchain consortium, including introduction, problem, technical background, and landscape. Section two lays out the factors for success and failure based on case studies, qualitative interviews, and research. Section three discusses the survey results. Section four presents recommendations. Section five concludes.

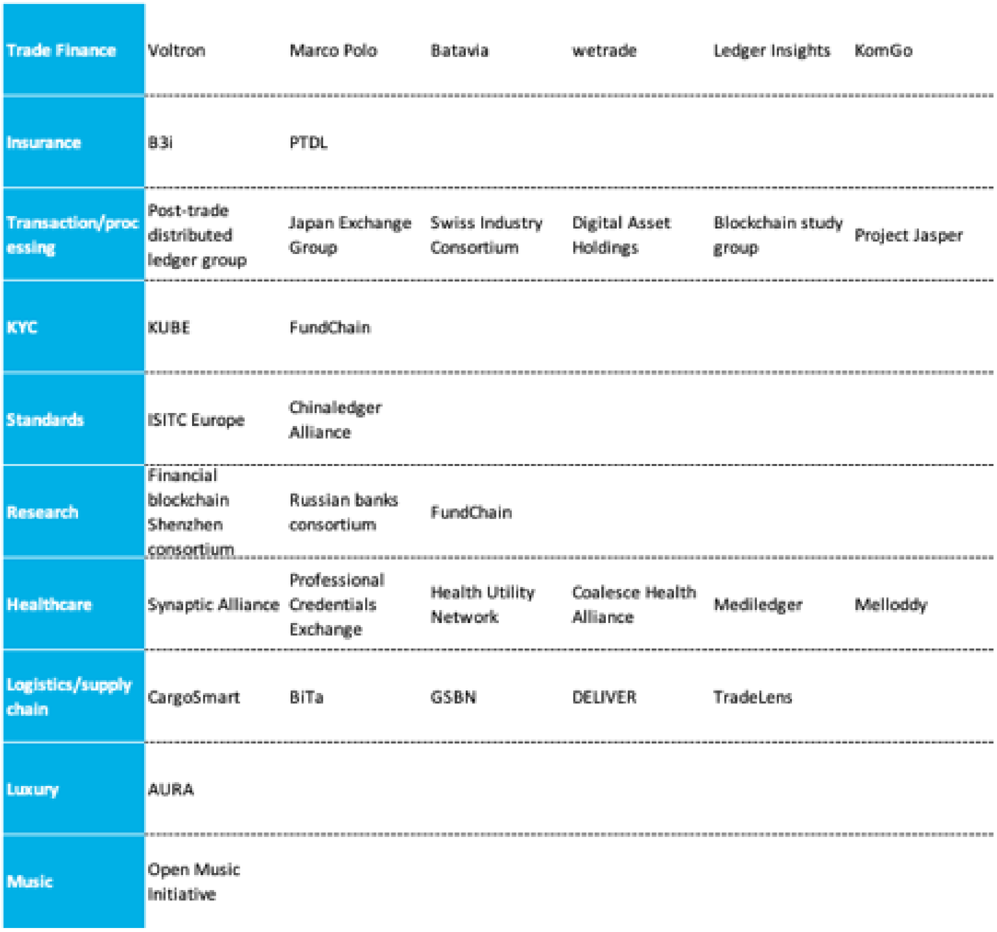
b. Landscape

It is important to distinguish between the types of consortia to understand the current state of the blockchain consortium. They can be broken into two categories: the technology development consortia and the project-based consortia. These are not necessarily mutually exclusive, and some consortia can embody both types.

The purpose of research and technology development consortia is to fund the development of open source blockchain technologies and advance the field through research projects. The best example of such a consortium is the Enterprise Ethereum Alliance, which comprises over 150 members. Members type vary and include traditional firms, other blockchain-related consortium, blockchain startups, and companies. Due to their size and the different industries of their members, they are often organized into smaller working groups collaborating on technical subjects or identifying industry-specific opportunities. Other examples of such consortia include R3, Hyperledger technical working group, or Hyperledger framework and tools.

Then, the project-based consortia - the focus of our study - are collaborations that emerge in response to an industry-specific business problem and can be solved using blockchain-driven solutions. Their focus is on co-learning as well as co-developing a blockchain project. They also often participate in defining industry standards and specifications. Their legal structure can vary a lot, for instance, Marco Polo is a fully distributed network in opposition to a standalone legal entity with equity shareholders, which is the case of Contour (formally known as Voltron) as an example. The members are generally incumbent companies amongst a single industry or sector of activities, willing to develop blockchain capabilities and implement blockchain solutions. Members can be competitors, partners, or customers, which will result in different types of collaboration, for instance, with regards to data sharing. We will explore in greater detail consortia with different types of members' relationships in the "business use cases" section. While many consortia of the sort have been created, only a handful of them has been implemented in production at full scales, such as We.Trade. The remainder is either still investigating the business opportunities, doing pilot projects, or, if unsuccessful or unable to identify a solid use case, inactive.

These consortia can be further broken down by industries, as the table below suggests. Interests have been mainly focused on finance in the past and expanded to other sectors such as health and logistics more recently.



Trade Finance	Voltron	Marco Polo	Batavia	wetrade	Ledger Insights	KomGo
Insurance	B3i	PTDL				
Transaction/processing	Post-trade distributed ledger group	Japan Exchange Group	Swiss Industry Consortium	Digital Asset Holdings	Blockchain study group	Project Jasper
KYC	KUBE	FundChain				
Standards	ISITC Europe	Chinaledger Alliance				
Research	Financial blockchain Shenzhen consortium	Russian banks consortium	FundChain			
Healthcare	Synaptic Alliance	Professional Credentials Exchange	Health Utility Network	Coalesce Health Alliance	Mediledger	Melloddy
Logistics/supply chain	CargoSmart	BiTa	GSBN	DELIVER	TradeLens	
Luxury	AURA					
Music	Open Music Initiative					

Figure 4: Examples of consortia by type of industry.

c. Technical Background

Blockchain Technology

Before diving into the success factors of a blockchain consortium, it is worth knowing what is inside of the black box of blockchain technology and blockchain consortium.

Blockchain is a decentralized, distributed ledger, where transactions are arranged in blocks, and placed in the P2P network. Blockchain is hosted on a server that resides in a data center. When you browse the web or use applications, clients traditionally request content or data from application servers. However, blockchain permits multiple clients to connect with peer [multiple] clients as well and share data with each other: this is termed a P2P network. Blockchain is a P2P network of computers that computes transactions, validates them, and stores them in an ordered form in a shared ledger. This allows for a distributed database that records all the data, transactions, and any other relevant information.

Each computer in a P2P network is called a *node*. Nodes are responsible for validating transactions, organizing them into blocks, broadcasting them to the blockchain network, etc. Upon reaching a consensus or agreement, nodes commit a block to the blockchain network and update their local ledger copy.

The blockchain technology uses cryptography and P2P (peer-to-peer) technology as well as consensus protocols, which are a fundamental part of blockchain technology. Some popular blockchain consensus protocols include PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), and PBFT (Practical Byzantine Fault Tolerance). Each consensus protocol has different strengths and weaknesses, as outlined by Shijie Zhang, Jong-Hyouk Lee (2019) in the analysis of the main consensus protocols of blockchain. Consensus protocols can help fault tolerance and security of the blockchain systems. The consensus protocols currently used in most blockchain systems can be divided into two categories: the probabilistic-finality consensus protocols and the absolute-finality consensus protocols.

Blockchain technology also has a layered architecture. It can be divided into broad categories: application and presentation layer, consensus layer, network layer, data layer, and hardware/infrastructure layer.

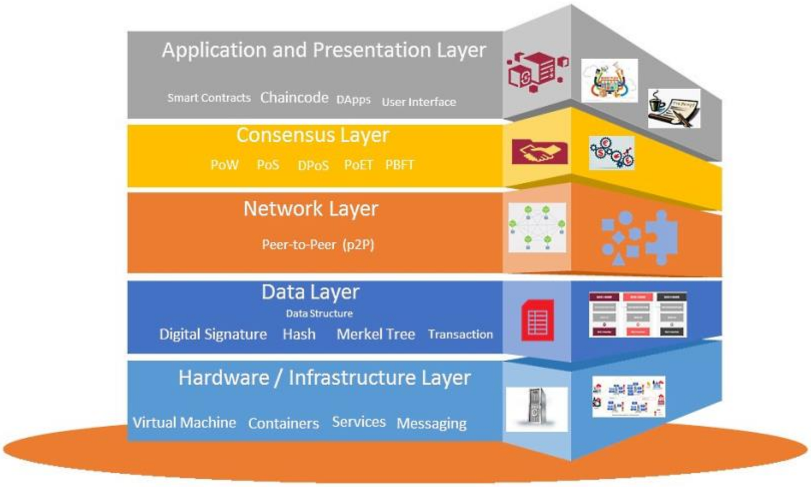


Figure 5: Blockchain layered architecture. Source: Dib et al. 2018.

Each of these layers has specific functions:

Hardware/Infrastructure Layer: This layer mainly allows for virtualization: the creation of virtual resources such as storage, network, servers, etc. Nodes are the core of this layer.

Network Layer: The network layer, also known as the P2P layer, or propagation layer, is responsible for internode communication. It takes care of discovery, transactions, and block propagation.

Application Layer: This layer includes smart contracts, chaincode, and decentralized applications. The app layer can also be broadly divided into two sublayers: the application layer and the execution layer. The application sends instructions to the execution layer such as chaincode in the case of the HyperLedger fabric, which performs the execution of transactions and ensures the deterministic nature of the blockchain (such as permissioned blockchain like hyperledger fabric).

Consensus Layer: The consensus layer is the core and most critical and crucial layer for any blockchain. The consensus is responsible for validating the blocks, ordering the blocks, and ensuring everyone agree on it. Consensus methods vary for different types of blockchain. In a permissionless blockchain such as Bitcoin, there is a probabilistic consensus. This kind of consensus guarantees the consistency of the ledger, but participants remain vulnerable. Permissioned blockchains, such as the hyperledger fabric, have deterministic algorithms/consensus. These blockchain networks have specific nodes called ordering nodes; blocks validated by these ordering nodes are considered as final and true.

Data Layer: The data structure of a blockchain can be represented as a linked list of blocks, where transactions are ordered. There are two primary components to a blockchain's data structure—pointers and a linked list. The pointers are the variables, which refer to the location of another variable, and linked list is a list of chained blocks, where each block has data and pointers to the previous block. Depending on the type of blockchain, data is stored in blocks. A hash is a unique digest of the data. A cryptographic hash algorithm (such as the SHA 256 algorithm) can generate a fixed-length hash value of the data. These hashes help identify blocks and detect any changes that are made to the blocks. Any new node connected to the blockchain will receive a copy of the blockchain network. Only upon consensus are blocks added to the local blockchain. Transactions are digitally signed on the blockchain to ensure the security and integrity of the data stored on it. They secure information about the block, transactions, transacting parties, and so via a digital signature, which uses asymmetric cryptography. Transactions are signed using a private key, and anyone in possession of the public key can verify the signer. As the data is already encrypted, it cannot be detected. Even if it is detected, it cannot be tampered with. Hence, the "immutability" characteristic of blockchain. Without a common consensus among notes, data cannot be altered.

Blockchain Consortium

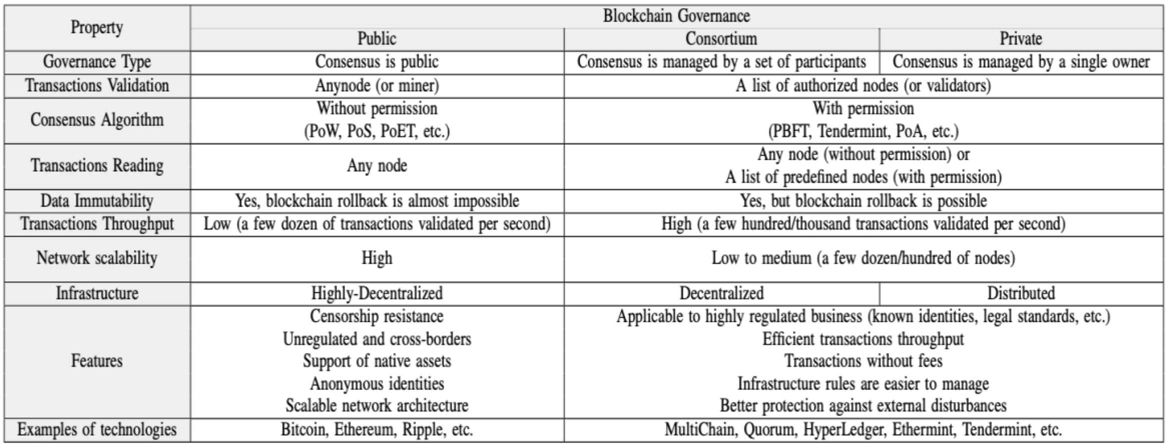
Public blockchains have proven to be useful and successful to process transactions in a secure manner in trust-less environments. However, they exhibit limitations when used in industrial settings as the dynamics between the participants are not necessarily the same as in the aforementioned environments (Dib et al, 2018). This has allowed for the emergence of consortium blockchains for enterprises, whose goal is to tackle these issues and is intended for restricted members. The consortium blockchain is a hybrid between the 'low-trust' entity given by public blockchains and the 'single highly-trusted entity' model of private blockchains. It is a permissioned blockchain platform with a deterministic algorithm and consensus.

The distinction between the consortium and permissionless and open blockchain platforms comes down to the infrastructure along with the governance scheme.

Infrastructure:

One of the main differences in the infrastructure and mostly the data layer is that consortium members can come to an agreement and alter previous blocks.

In a blockchain consortium, members share the authority among them. Blockchain consortia are deployed in a decentralized manner on multiple hardware managed by different members. Moreover, data is not always homogeneous among consortium nodes since some blockchains allow private transactions leading to knowledge fragmentation (commonly known as off-chain data). This ensures data privacy on a need-to-know basis and increases trust in using the system.



Property	Blockchain Governance		
	Public	Consortium	Private
Governance Type	Consensus is public	Consensus is managed by a set of participants	Consensus is managed by a single owner
Transactions Validation	Anynode (or miner)	A list of authorized nodes (or validators)	
Consensus Algorithm	Without permission (PoW, PoS, PoET, etc.)	With permission (PBFT, Tendermint, PoA, etc.)	
Transactions Reading	Any node	Any node (without permission) or A list of predefined nodes (with permission)	
Data Immutability	Yes, blockchain rollback is almost impossible	Yes, but blockchain rollback is possible	
Transactions Throughput	Low (a few dozen of transactions validated per second)	High (a few hundred/thousand transactions validated per second)	
Network scalability	High	Low to medium (a few dozen/hundred of nodes)	
Infrastructure	Highly-Decentralized	Decentralized	Distributed
Features	Censorship resistance Unregulated and cross-borders Support of native assets Anonymous identities Scalable network architecture	Applicable to highly regulated business (known identities, legal standards, etc.) Efficient transactions throughput Transactions without fees Infrastructure rules are easier to manage Better protection against external disturbances	
Examples of technologies	Bitcoin, Ethereum, Ripple, etc.	MultiChain, Quorum, HyperLedger, Ethermint, Tendermint, etc.	

[1]

Figure 6: Blockchain classification. Source Dib et al. 2018.

[1] To clarify the point on data immutability and rollback in private blockchain: "Data immutability is generally put forward when referring to blockchain technologies. However, […] the written data could still be tampered and the blockchain rebuilt as long as the majority of the participants (or miners) have reached a consensus. This is

Governance Scheme:

In a private blockchain, the governance addresses the power distribution amongst the consortium members by assigning authority and responsibility. Concretely, it determines a set of rules such as which nodes will be able to "create blocks, read/write data, contribute to the consensus mechanism and/or to participate in decisions, software updates, allow new nodes to join the system and so on" (Dib et al, 2018). As the governance has an impact not only within the system but could also on the business model of the use case, it should be determined accordingly (Dib et al, 2018). It should depend on the participants' dynamics (vertical vs. horizontal) as well as the specific purpose and business use case of the consortium.

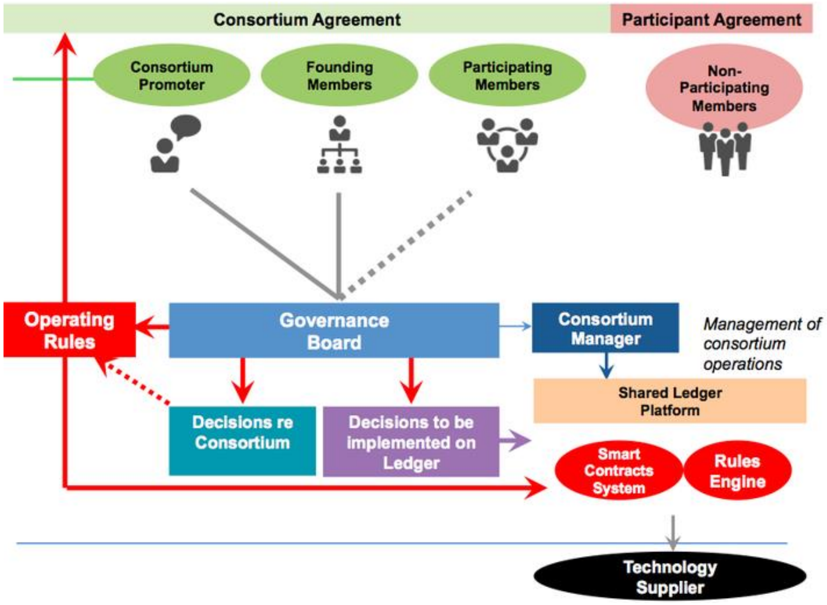


Figure 7: Consortium Blockchain Strategy. Source: Medium.

There are two main forms of governance in consortia: off-chain and on-chain. Off-chain governance refers to either of two things: contracts and rules members might have outside of the blockchain technology, or it can mean sub-rules within the on-chain governance that only certain members abide by when they share data amongst themselves and not the larger consortium. They operate without telling the global ledger or consortium. On the other hand, on-chain governance is the established rules that the consortium members agree upon to effectively work together to effectively build something useful not only to each of its members but to the community as a whole, and they have to abide by these rules.

especially true in consortium and private blockchains where the number of miners is generally limited in comparison with public blockchains". (Dib et al. 2018.)

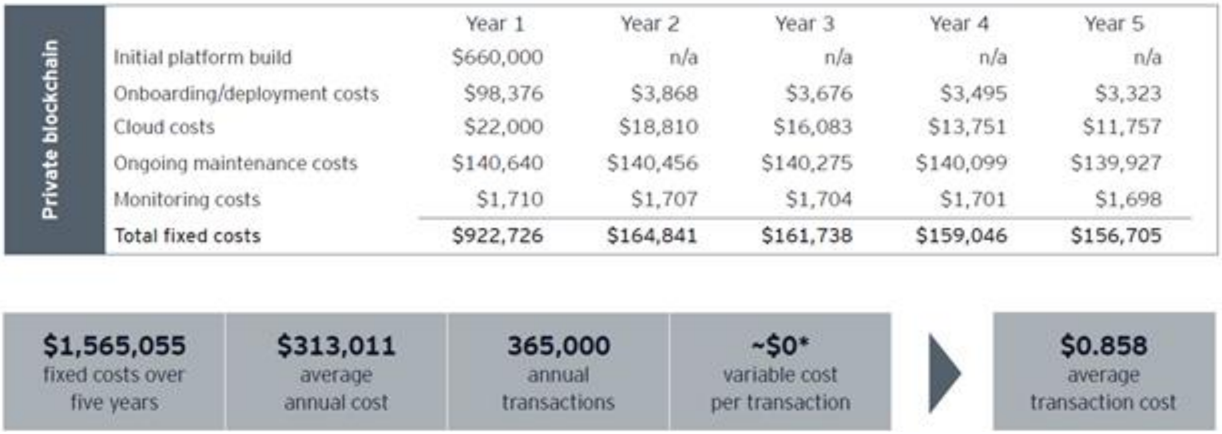
Governance is fundamentally intertwined with the viability and business model of a consortium. It affects and is affected by not only the blockchain technology but the consortium members. For example, the more companies join a consortium, the more durable it can become. However, it also dilutes the power to a certain extent.

II. Case studies and Literature on Key Success Factors

Research and expert interviews have suggested that success factors of a blockchain consortium include (1) strong business use cases, (2) robust governance, (3) operations, (4) data and privacy, and (5) regulatory environment. Each with different weight in terms of its importance.

a. Business Use Case

"Successful consortium is a business challenge, not a technology question," a remark from our expert interviews. Business use case is identified as the most important factor for the success and the continuity of blockchain consortium. Participants need to ensure that the consortium's goals are critical to the industry and solving an actual problem with real economic rationale. Namely, questions such as how it is improving business efficiency, or how much it reduces costs are essential for members to remain engaged and contributing. Moreover, they must make sure that blockchain technology is critical to solving the business problem since it is usually costly. The average cost of maintaining a private blockchain ranges between 150K to 250K. For a blockchain with 1000 daily transactions, costs $0.858/transaction (E.Y.). Thus, structuring the consortium in a way that has real business benefits is crucial.



Private blockchain	Year 1	Year 2	Year 3	Year 4	Year 5
Initial platform build	$660,000	n/a	n/a	n/a	n/a
Onboarding/deployment costs	$98,376	$3,868	$3,676	$3,495	$3,323
Cloud costs	$22,000	$18,810	$16,083	$13,751	$11,757
Ongoing maintenance costs	$140,640	$140,456	$140,275	$140,099	$139,927
Monitoring costs	$1,710	$1,707	$1,704	$1,701	$1,698
Total fixed costs	**$922,726**	**$164,841**	**$161,738**	**$159,046**	**$156,705**

$1,565,055 fixed costs over five years

$313,011 average annual cost

365,000 annual transactions

~$0* variable cost per transaction

$0.858 average transaction cost

Figure 8: Private blockchain costs analysis. Source: E.Y., 2019. Total cost of ownership for blockchain solutions. Dataset can be found here: https://github.com/EYBlockchain/fundamental-cost-of-ownership/blob/master/Total%20Cost%20of%20Ownership%20of%20Blockchain%20Solutions.xlsx

However, more concrete business use cases, whether it was pre-defined at the establishment of the consortium and developed as part of the consortium purpose, are sometimes hard to achieve. The budget and resource concerns increase when there is no clear business use case.

Our survey suggests that the digitization and standardization of data, learning, and access to information are the main benefits of a consortium. While these are beneficial, businesses might look for more direct business values such as cost reduction and revenue increase to stay committed and engaged. For example, the research-oriented consortium might be good for learning but might be too remote from creating direct and quick business values and make the consortium successful.

Blockchain consortium is still in its early development. Business solutions that consortia try to address are sometimes vague and evolving overtime. For example, R3 was a consortium with nine world's largest banks in the world when it first started on September 15th, 2015. It was designed as a learning platform for banks to learn about blockchain. The consortium quickly drew interest, and an additional 33 banks joined within three months. Four years later, the R3 consortium has led to a blockchain ecosystem R3 Corda and many businesses spin-off, such as other consortia (MarcoPolo) and software business for members. This is not what they had anticipated.

Here, we will deep dive into the business cases and literature to draw lessons from. We will, therefore, break down our analysis of the use cases in two parts according to different dynamics. First, we will investigate use cases where participants are business partners, and then we will focus on use cases where participants are traditionally competitors. We will finish the section with lessons learned from the literature to provide some more insights.

Lessons from case studies

Vertical Dynamics

Let us now turn our attention to consortia with vertical dynamics. We will focus on two specific cases in different industries, namely Komgo in supply chain and Aura in Luxury goods.

- Example 1: KomGo

Trade finance is known for its long, opaque, prone to fraud, and paper-based process. From initiating an export deal, shipping, to receiving the goods overseas, it involves a large number of parties, including clients, exporters, importers, logistic companies, their banks, corresponding bank(s), customs, and any other documentation related parties. A typical single commodity trade involves 36 original documents and 240 copies from as many as 27 parties (Gtreview). The burdensome and paper-based process prolonged the process for weeks, even months to complete.

KomGo is a trade finance consortium that was launched in December 2018 by 15 shareholders consisting of banks, trading companies, and oil giants to digitize the paper-heavy process and improve trade finance efficiency through blockchain enabled solutions. The consortium designed a blockchain based open platform that allows all parties to monitor progress in real-time, easy data verifications, reduce fraud, and shorten cash cycles. It reduced the processing time from 10 days to 1 hour on average, increased gains from cash flow by 30-40 percent, and is expected to reduce the operation cost by 20-50 percent if having industry-wide adoption (Consensys KomGo Case Study).

The consortium designed several business applications. First, it allows companies to perform KYC requirements on the blockchain and solve the challenge of exchanging KYC documents with the encryption and need-to-know basis. Each company maintains the ownership of its own data rather than KomGo and can choose who can retrieve a copy. The blockchain technology also ensures the immutability of the data stored.

Secondly, the platform digitized Letters of Credit through smart contracts. In January 2020, MUFG, a consortium member, issued the first letter of credit in London on KomGo's platform for a commodity trading company (MUFG). Users can store transaction documents with cryptographically verifiable notarization. Therefore, the users can show verification documents with relevant parties that both can trust without sacrificing data privacy.

Additionally, the consortium made the platform interoperable with third parties through API. It adds flexibility in service for its members ranging from fully managed service to self-hosted options. KomGo also put all these functions on a dashboard that is user-friendly and easy to navigate. Flexible and good user experiences increase their business values for the users. The technology plays a critical part in its success.

KomGo managed to have successful business use cases through a combination of addressing the existing business needs, the right incentives to get participation, the network effect, and the user-friendly design. The use case of the blockchain-enabled KYC addresses the current needs on KYC compliance. Yet, facilitating data sharing among relevant parties and streamline the operations alone is not enough to make the case successful. The solution also needs to address the privacy and competition concerns among the participants. KomGo successfully leveraged the unique feature of blockchain that keeps the data private and immutable while improving data transparency among relevant parties. Immutability and transparency of data and yet privacy control in data sharing make companies more comfortable in storing and sharing the data on the platform without worrying about losing control of the data ownership. Lastly, the open platform started with a right mixture of players in the industry (banks and corporates) and backed by 15 world's largest banks to get enough muscle so that the rest will follow, according to the CTO of KomGo.

- Example 2: AURA

Counterfeit is a big issue for the luxury market. The fake luxury merchandise is estimated at around 2.7 trillion to 3.2 trillion dollars a year. LVMH, a luxury goods conglomerate from France, spent 17 million dollars annually on anti-counterfeiting legal actions, but the actions were not very effective in stopping the counterfeits (Harvard Business Review).

LVMH and Microsoft launched the blockchain consortium in 2019. The consortium aims to design a tool to (1) document the information of the luxury goods throughout the production and distribution process on a blockchain; (2) the buyers can access the information and authenticate products. The consortium also plans to use the platform as a communication and loyalty tool for customers. It is planned for other luxury producers to join in the future. The permissioned platform is based on JP Morgan's Quorum, the same as KomGo. Quorum is the enterprise version of Ethereum and built on an open standard that is more widely accepted. Each item is tokenized with a unique or non-fungible token based on the ERC721 standard (Ledgerinsights).

There is a clear business case, which is to fight against the counterfeit luxury merchandise. The blockchain technology has shown some success in anti-counterfeit in luxury goods (Arianee) and supply chain (Fashion Nework). AURA strengthened the use case by adding decentralized, independence of the consortium from the LVMH group, and a more open access structure to encourage other brands to follow and achieve scale. While it has attracted lots of attractions and prototyped solutions in its subsidiary brands, the consortium has only existed for under a year and is too early to tell its success.

Horizontal Dynamics

We shall now focus on the consortia where members are traditionally competitors and investigate the successful use cases. Indeed, one may wonder why competitors in the same industry would collaborate and to what extent, as well as what are the key drivers behind a successful collaboration. We will do so by exploring two specific cases: We.Trade and Marco Polo.

- Example 1: We.Trade

We.Trade is a blockchain consortium and started initially by nine banks and joined later by four others, which traditionally are competitors. It uses blockchain technology from IBM Fabric.

We.Trade is a digital platform facilitating trade transactions between small and medium enterprises (SMEs) by allowing users to manage, track and protect their trades and linking all stakeholders – namely, the seller, the seller's bank, the transporter, the buyer, and the buyer's bank. The main customer segment is the European SMEs. The platform distinguishes itself not only by its technology but also by its user-friendliness. We.Trade is solving two main problems persistent within trade finance. First, the issue of late payment, indeed, it is reported that only 42.8 percent of companies across the European Union respect payment terms. The second recurrent issue is the slow processing of trades, usually due to the physical exchange of documents. The platform solves the former pain point by allowing to track the evolution of the trade and guarantees that the payment is processed according to settlement conditions defined beforehand, once all contractual agreements have been met, which is enforced through smart contracts. To address the latter hurdle in the current trade finance system, We.Trade platform is fully automated and available at all times, resulting in quicker order-to-payments process than the traditional exchange of documents.

Let us now describe the different roles of the banks and explore their incentives to remain engaged within the consortium. First, the banks must verify their respective clients before the trade settlement details can be set up. The incentive for the banks to provide a thorough KYC analysis stems from the fact that the bank is either undertaking the payment or financing the trade, which shifts the counterparty risk to the bank. Thus, the bank has skin in the game, which in turn, strengthens the incentive for businesses to use the platform.

While this system results in the aforementioned positive effects, it may also lead to trust issues within the participants of the consortium. Indeed, HSBC, who is part of We.Trade and responded to our survey listed "trust amongst participants" as one of the consortium's main challenges. We may also wonder why banks are participating in this initiative at all. One possible answer could be the structure of the trade industry. Indeed, as no bank has a monopoly over all the SMEs or the entire trade finance process, the banks must collaborate anyways to process trades, and using an efficient and secure system provides them with a competitive advantage as well as increase their attractiveness in the eyes of clients. Participating in the consortium, in this case, seems like a Nash equilibrium – no bank would benefit from not participating, given that some of its clients are SMEs engaging in trading activities. Overall, the perks of the platform – namely security, user-friendliness, and trade processing system, as well as the structure of the trading industry, stem strong incentives for competitors to actively participate in We.Trade. It is important to note that without blockchain technology, the solution would not be as performant.

- <u>Example 2: Marco Polo</u>

Marco Polo is made up of over thirty banks and corporations. It uses technology from R3's Corda network as well as TradeIX trade finance solutions. The main business problem that Marco Polo is trying to solve is related to inadequate working capital, which limits firms' growth perspectives and investments. Indeed, the leading reason mentioned by companies for rejecting trade finance transactions is the lack of additional collateral to finance the trade. Similarly to We.Trade, Marco Polo main customers are SMEs. To address the aforementioned problem, Marco Polo launched a solution named Payment Commitment. They introduce a new digital instrument for trade settlement called Irrevocable Payment Unit (IPU). The way the system works is the following: the seller and buyer agree on a transaction, the goods are then purchased by the buyer, and the goods are sent by the seller. At the same time, relevant information from the three parties – namely purchase order, invoice data, and shipment tracking - is exchanged on a blockchain-based network, allowing all parties to access this information. Once the trade data is matched and reviewed, the buyer's bank provides an IPU to the supplier to mitigate the non-payment risk – the counterparty risk is shifted. Moreover, suppliers can also sell their IPU to other banks in exchange for early payments, achieving risk mitigating and accelerated cash flow, solving both working capital and counterparty risk issues.

Similarly, as the previous example, the value for the banks is derived from the attractiveness of the solution to corporate clients. Indeed, as more transactions are done using this automated system, the incentive for banks to take part in it grows as it would result in more business for them. We also observe in this case that the banks transact between one another and do not deal directly with the other end of the trade. Such collaboration is facilitated by the platform and legally enforceable, entirely digital, and self-executing smart-contracts for digital payment commitments, resolving the trust issues. Furthermore, the Marco Polo network allows participants to join their research and development efforts and investments in trade finance and blockchain. Such a collaborative and fecund environment fosters innovation in the field and could benefit participants as well as their clients. This consists of another incentive for banks to join, especially if competitors are also onboard as they would lag behind if they do not.

The vertical and horizontal cases share a commonality that the solution addresses the existing business pain point. Having a strong business use case set a good start of the consortium, but that is not enough. The blockchain technology should also be a critical part in its business solution by leveraging its transparency, decentralized structure, and data privacy protection features. Furthermore, a consortium should also focus on making the products user friendly and open standards to encourage industry-wide adoption in order to make the business solutions more valuable for the members and increase its network effects.

Lessons from literature

We are drawing lessons from the literature on how to build a successful business case, especially in the context of the consortium. This would be complementary to the lessons learned from the case studies.

Jap (2001, p.96) noted different goals and culture among private sector players and government agencies in a consortium. It noted that for firms, return on investment and process efficiency is critical for them to stay in a consortium, whereas the government agencies expect firms would take the technology and apply in its product development.

Coelho & Valente (2017) conducted a survey, asking 414 developers of open-source software projects (OSS) that were able to gain traction, attract attention, users and significant contributors, and failed, to understand why they failed. A project is considered to have failed when the project is no longer under maintenance, and the developers have no plan to relaunch the development, or they explicitly mention that the project is definitely paused, and not complete. They found that the biggest reasons explaining the failure of an OSS project are usurpation by a competitor, obsolescence, lack of time, lack of interest, outdated technologies and low maintainability. When grouped by categories, the main reasons are project characteristics then followed by the project team, and finally, environmental reasons. This is an interesting framework for blockchain consortium. The finding further emphasizes the importance of creating tangible business values to the success of a consortium.

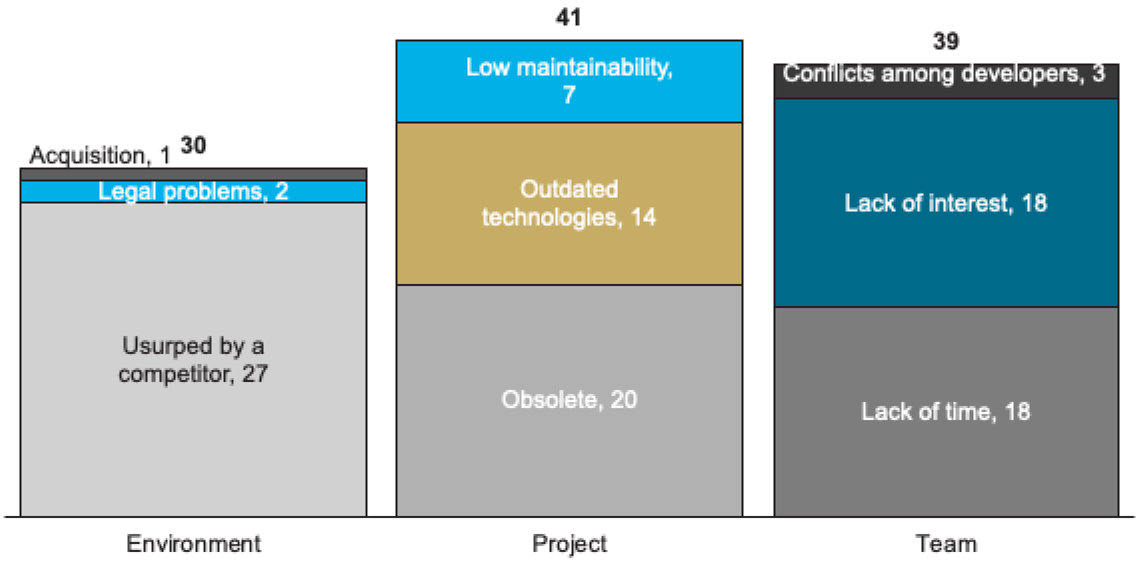


Figure 9: Main reasons for failure. Source: Coelho & Valente (2017).

Updegrove (2019) emphasized the need of business considerations to form a successful consideration. The business consideration should clearly identify the deliverables that it should create in order to achieve its mission. Different members might have different interests in the deliverables. The deliverables could be designed considering different segmentation of the members with varying interests. For example, some members are interested in cutting costs and adapting it to their operations. Others might be more interested in the learning experience. The deliverables should prioritize the most important interests while putting fewer resources on the less important ones. The deliverables could be differentiated in terms of who would be contributing to the development of the product and who would be contributing to the adoption of the product as well to take care of different interests.

Acharya (2019) proposed a quantitative way to identify and justify the need for blockchain for its use case. It proposed an equation called blockchain justifying equation (BJE) to quantify the need for blockchain includes critical factors and satisfaction factors. The critical factor refers to 'is reconciliation between parties critical? The satisfaction factor refers to 'is the current reconciliation between parties satisfactory? The use case factors are assigned with a score and put into the equation to get a binary outcome (justified or not justified). Justified is when "the use case is critical to the firms but is not well-served currently." Not justified is when "the use case is not critical to the firms, and it is currently well served."

$$\textit{blockchain need} = \textit{criticality factor} + (\textit{criticality factor} - \textit{satisfaction factor})$$

This resonates with the findings in the case studies that we need both conditions for a successful consortium: (1) there is a need to change existing solutions, and (2) blockchain technology is critical for the new solution in addressing the existing gap.

b. Operation, Governance, and Trust

The governance structure is a master agreement agreed by all members. It should include but not limited to the membership, the business case, the decision rules, the verification, the rules regarding the code, the management, the operation rules, the finance, the legal ownership and liability, the I.P., and the exit. R&D consortia set a good example for Blockchain consortia, as it operates exactly like any type of consortia.

We have interesting evidence provided by Olk & Young (1997) on US-based consortia. They targeted 110 consortia of 3+ members but had a low response rate (around 20 percent). They found that membership continuity doesn't always imply good consortium performance. Performance influences participants to stay in the consortium, but there is a more complex relationship between performance & continuation. Other factors are the conditions of membership: the decision to continue depends on the nature of the relationship among members, but the performance of the consortium is also determined by the condition of membership & learnings from the consortium.

Is it necessary to have an equal say for all members to have a successful consortium? Evidence from cases suggests both. The biggest companies do not end up dictating the consortium. On the other hand, success can be seen by governance and the presence of a powerful player.

There are often tensions among private sector players – competition vs. cooperation. Firms that form strategic alliances often have a difficult time balancing competition and cooperation (Jap 2001, p.96). The impact of vertical and horizontal relationship on competition and cooperation is also mixed. Several studies suggest that the competition issue is more pronounced among horizontal players (OECD 2010, Medrano 2001, Cecere et al. 2015). Some other studies suggested that the horizontal ties enable joint product innovation and efficiency gains while maintaining both competition and cooperation (Mesquita and Lazzarini 2009, Bengtsson and Kock 1999)

Moreover, Branstetter & Sakakibara (2002) tested the success factors of Japanese R&D consortia. Indeed, a lot of consortia were founded in Japan during the 90s, mainly focused on semiconductors. They focused on the operating parts of these consortiums and operational metrics. They found that success factors rely on the following points:

- Level of R&D spillovers within a consortium
- Ex-post level of product market competition

This means that successful consortia allow significant cost savings for all participants and that participants have a limited level of competition. The underlying mechanism that allows a successful consortium to survive is that it allows each participant to realize a positive return on their investment and that they can reinvest it. Indeed, a highly intense level of competition will force all the participants to offset their cost savings by a product price decline. They will not see any additional profit, and R&D spillovers will translate into an increased price war. Firms will thus reduce participation in consortia, and the consortium ends disbanded.

c. Data Privacy

One of the most prominent concerns regarding consortium is privacy and the distribution of data between members, as also suggested by our survey results. Blockchain is often preferred over non-blockchain solutions for a variety of reasons: blockchain can be a data registry, and it has certain privacy and security principles operated by different members. These interactions occur peer to peer, so there are no scaling issues the traditional blockchains have.

Consortiums want to standardize data and share it among each other efficiently and privately. Some want the data to be immutable, but, as we have seen, the blockchain consortium fabric allows for the mutability of blocks and as such data. This, in return, allows for the risk of losing "control" of the data, even though the ledger marks the changes and letting others have copies of the data. In order to mitigate these trade-offs that come with the mutability of blocks and data in a consortium, practices have been put in place: governance structures have been defined on- and off-chain, sharding, data arrangements, and further encryption of the content that shows the validity of the data.

If you divide a blockchain or partition it, integrity is still based on the data. The necessity for all members to download all data is more to show that privacy. The off-chain protocol allows hiding data that participants wish to exchange privately, to increase privacy over the data they wish to share. Another important characteristic of what consortiums are designing is that you create your connections and are in control of the keys that establish a connection with the peer, there's no account service in between: they are able to tackle the weakness in client-server architecture, which is rooted in peer to peer architecture.

One interesting technical tool to increase trust in a single database and acquire locks is the Key Event Receipt Infrastructure (KERI), developed by Sam Smith. It could aid in solving the trust and governance issue. The main concept is that as records are being added to the database, each time, you're creating a linked list in parallel to the database that is the length of the hashes of the records that are being added, so it's kind of like its own little blockchain. You can make that information public or not, but you can also make it available only to the set of members that need to see it. It's similar to having a witness. Later on, members can recreate that linked list and see if you've altered anything (Samuel M. Smith 2019).

Although some members or consortium prefer the immutability of data that comes with public blockchains, the mutability with comes with private blockchains and consortium can be a real asset and should not be dismissed so quickly: if there's a bug in the data that was allowed to be written in the ledger, it can later be fixed.

d. Regulatory Challenges

Regulatory support is important for the success of the consortium. For example, finance is a highly regulated space with certain reporting, data storage, and legal requirements. Members might face different rules based on their jurisdictions. Different regulatory regimes might make it more challenging for the consortium members to find a common solution and join the consortium.

R3, is one of the earliest consortia, claimed that it was extremely important to get the buy-in from regulators since the beginning. Axoni, another consortium for standardizing and sharing trade data, collaborated closely with the regulators and made sure the data solution is compliant and useful for the reporting and supervising. The consortium joined by Samsung and Korean banks were not successful due to the regulatory concerns.

Regulations that are particularly relevant to consortia include AML/KYC, data privacy rules, the antitrust, legal issue regarding smart contracts, the right to modify personal data, and accountability and governance rules. For example, KYC blockchain consortium faced the potential problems of who is liable for the erroneous data that has been shared among the members in detecting frauds. The consortium can establish its internal rules on holding members liable for their own data quality. But the regulators of AML/CFT in practice might just hold whoever missed the fraud detection accountable even though it was due to the wrong data input shared by another member in the consortium (IFC). This creates uncertainty and concerns among members to participate in the KYC consortium, according to our discussions with regulators. Data privacy is another key area with an uneven regulatory regime. The E.U. has the GDPR, and the U.S. has similar rules CCPA only in Washington and California. The GDPR has already influenced the architecture of blockchain solutions that has E.U. personal data (Barnes & Thornburg). In the case of a consortium with data from different jurisdictions, different treatments would be needed and might prevent the standardization of the data.

Additionally, there are overlapping and gaps in the regulatory framework that it is sometimes unclear for blockchain consortia to know what the rules are and who is responsible for what. For example, the U.S. has the federal and state-level regulatory structure for financial services. There are competing interests among regulators. The rules for emerging technology such as cryptocurrency are not clear, which brings some compliance risks for consortium members.

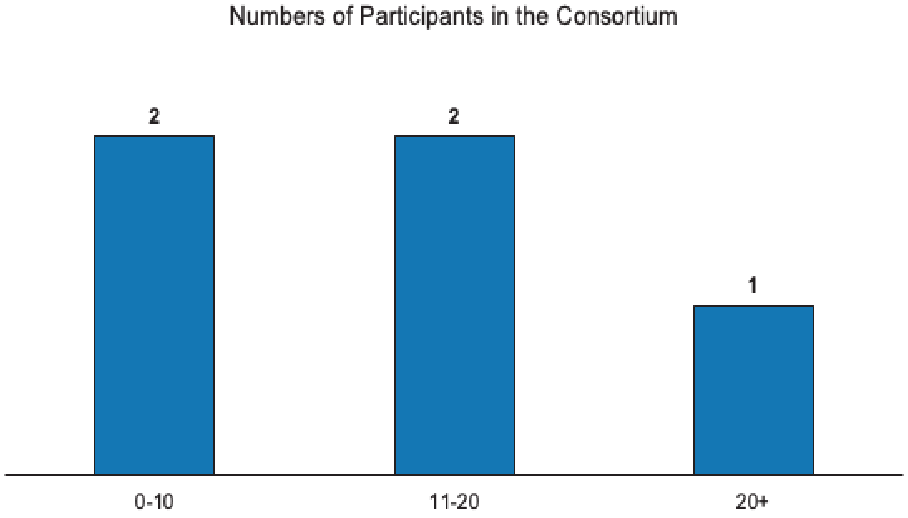
III. Survey results on Key Success Factors

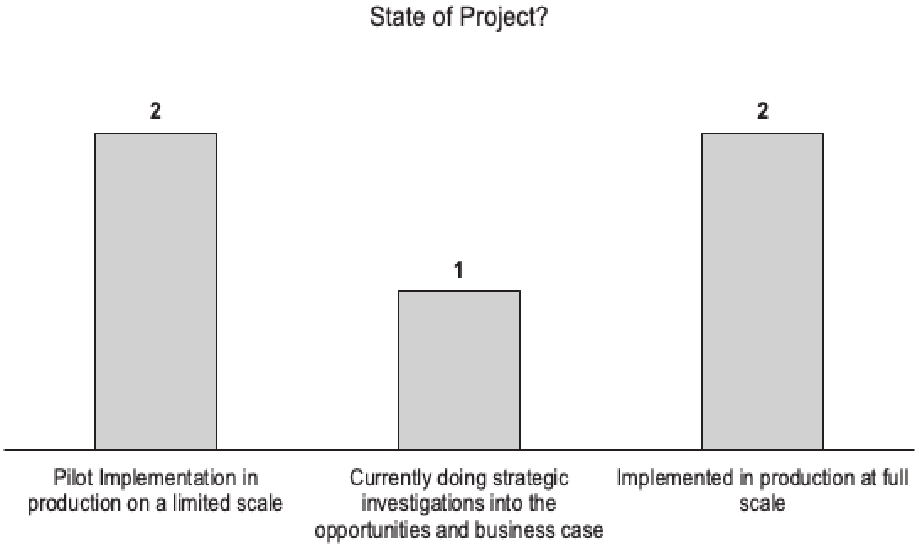
a. Survey Presentation

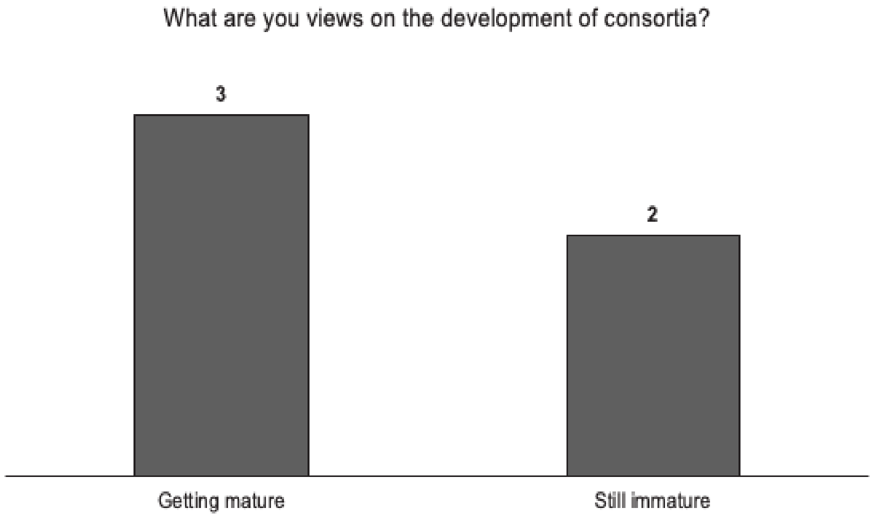
After having identified the relevant scope and issues that our survey should be targeting, we set up a 34-question survey. The survey covers nine specific topics: size, market & growth, business model, firm & competition dynamics, governance, blockchain technology, privacy & data, regulatory impact, and performance. Our survey respondents include 29 different companies involved in consortia (consortium platforms or member companies). However, the response rate is quite low (5 respondents, around 18 percent response rate). This low response rate is in line with the response rate from the R&D consortium literature. Due to the very low absolute number of respondents, we are unable to do a statistical analysis of our answers. Nevertheless, the descriptive analysis provides some insights into the state of consortia and success factors.

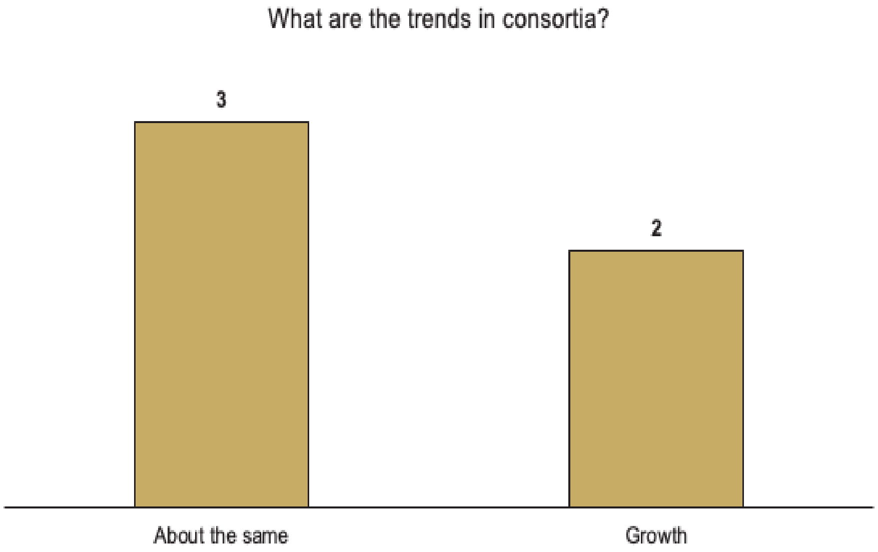
b. Preliminary Results from the Data

We identified that the longer the consortium has been around, the bigger it is. We had answers from 2 "old "consortia" (founded around 2015), and 2 "new consortia" (founded after 2019). This result is intuitive. There is probably a survivorship bias, as the "old" consortium are the ones that survived and continued to grow. However, older consortia are not necessarily mature and/or fully implemented, and they are all at least in the process of getting mature. This could be explained by the fact that consortium is a relatively new concept, and even the older ones have only been around for 5 -6 years.



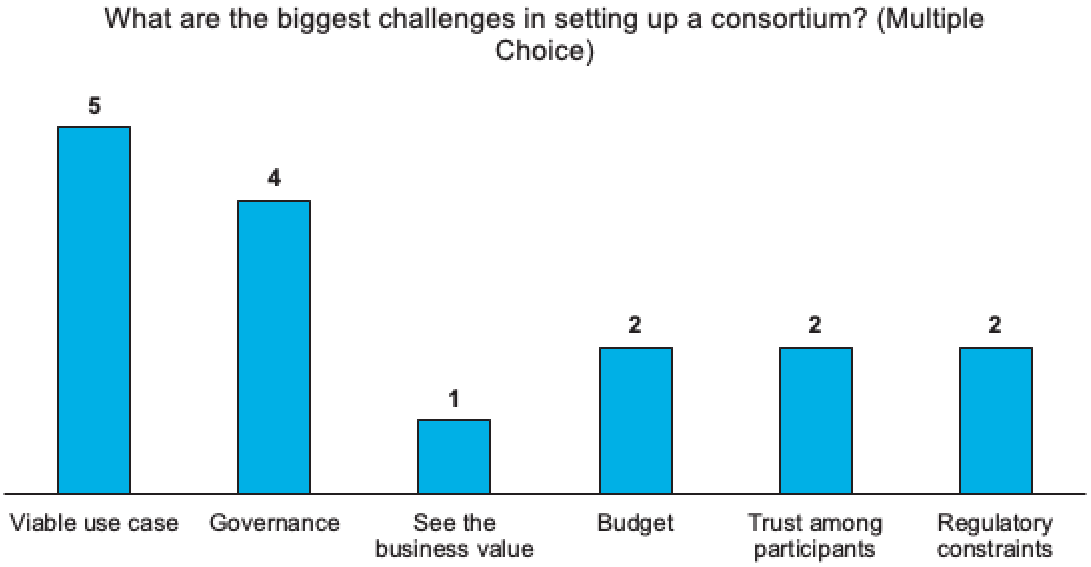






Furthermore, we identified relevant variations in the data regarding the value proposition. All respondents identified economies of scale as a motivation for them to join, as participants can pool problems together and solve them more efficiently. Some participants also mentioned network effects as a big motivation to join. We also identified standardization of data and automatization of wasteful processes as drivers for respondents to join consortia. Finally, access to analytics and additional channels to reach out to customers (both revenues and insights) are motivations for players to join.

Other big important issues raised by respondents are viable use case, governance, budget, regulatory constraints, and trust. Indeed, they identify the business use case as a critical criterion for consortium success, while governance is secondary. The budget is a reasonable concern, given the expensive annual contribution to join the consortium (ranging from 200K to 2M). The bigger the consortium, the higher the contribution.



Moreover, we found an interesting variation in the survey data regarding trust. The high level of competition between participants seems to imply a high level of trust within the consortium, while low level of competition seems to imply low trust between participants (especially more vertical consortia, with a dominant player). It is an interesting finding in terms of "cooptation" dynamics. That might resonate with the fact that the horizontal consortium is often designed to have competitors join forces to advance product innovation, also as Mesquita and Lazzarini 2009 indicated in its findings.

Indeed, in a horizontal consortium with intense competition between members, cooperation seems to be inevitable, and all participants are driven by the same initiatives. Let $x_1, \dots, x_t$ be the industry participants, let $NI_1 \dots NI_t$ be the profit margin of the industry participants, and $r_1, \dots, r_t$the return on asset of the industry participants. Let $I_c$be a subset of the industry participants, such as $x_i \in I_c$can join a consortium. If $x_i \in I_c$, then there is an opportunity ϵ_i such as x_i profit margin is now $NI_i' = NI_i + \varepsilon_i$. These participants will have an excess income that it can reinvest in new assets, and further increase its income by $\varepsilon_i r_i$.

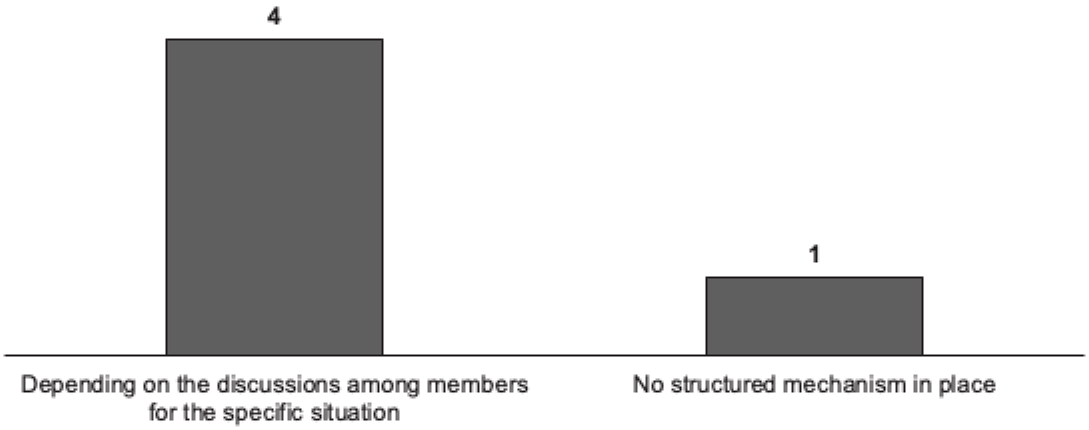
A highly competitive industry would have $r_i \simeq r_j$and $NI_i \simeq NI_j$, at a relatively low level. If $x_j \notin I_c$, then participant j would see its profit margin not benefit from the increased opportunity, a situation they will avoid. Knowing this, all industry participants would join a consortium opportunity, as it would not change its relative profit margin (Osarenkhoe 2010).

The lack of trust among the verticals adds an interesting dimension to our findings from literature and case studies. We previously found that vertical consortia had higher efficiency gains and lower competitions compared to the horizontal ones. Yet, the vertical ties do not translate into higher trust. One explanation is that the verticals are easier to create synergies as it improves the efficiency of existing supply chain, but the trust level might be lower among the players because not everyone knows each other along the supply chain. So, there are three different concepts involved: efficiency gains, competition, and trust. Alternatively, as all industry participants know it is mutually beneficial, they have a higher level of trust, explaining why we observe that. On the opposite side, participants from different industries have different returns on assets, and different potential profit margin increases, which translates in different incentives, and a low level of trust between participants. This might warrant further research.

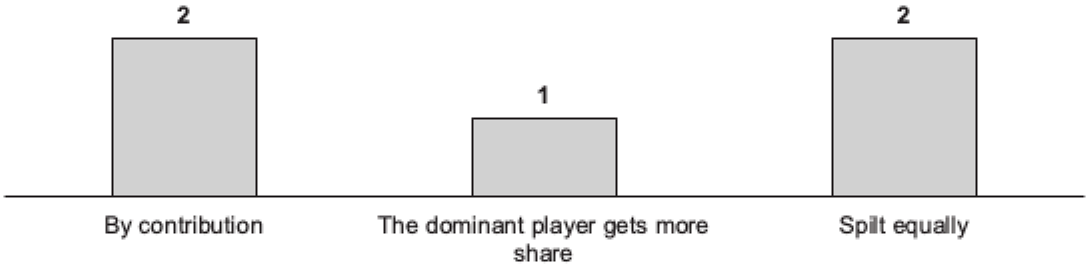
Regarding the governance design, all participants use an off-chain governance system. Cited decision mechanisms include discussion among members, with equal voting rights, or by contribution. Some have a dominant leader having all the decision power. There is no clear reason why a certain type of governance structure is preferred to another. It is highly dependent on the verticality of the consortium, the history of its formation, its business use case, etc.

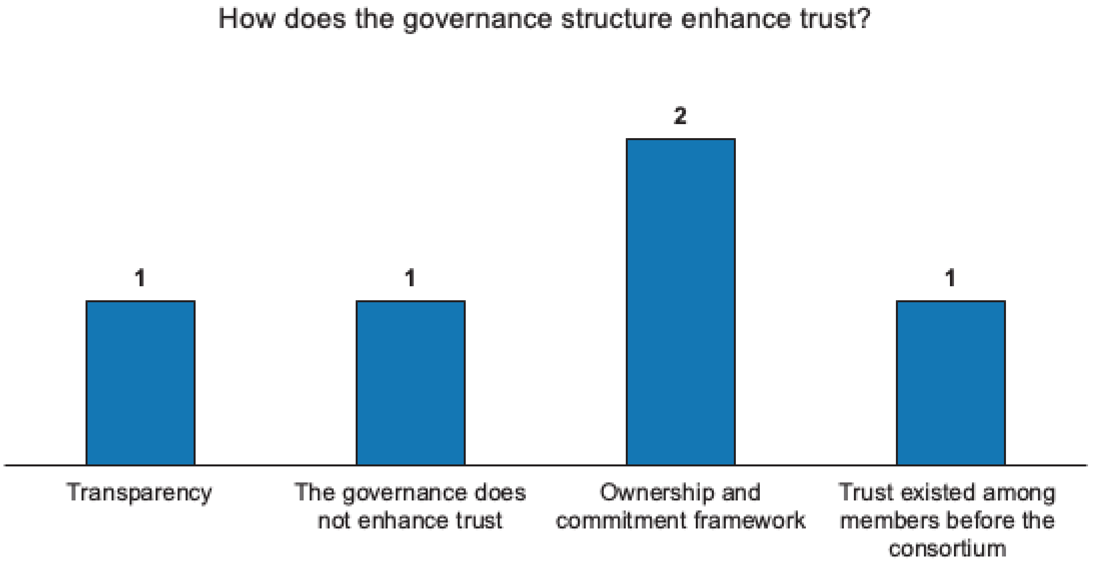
The governance structure could increase trust by enhancing transparency or setting ownership and commitment framework. There are respondents who also claimed the trust existed before the consortia and were independent of the governance. Getting commitments from the members is the biggest challenge in governance facing respondents, followed by trust and transparency. This is an understandable concern, as not all members can control each other’s contributions and good faith. In addition to that, open and rule-based governance structure are mentioned as secondary concerns. The governance structure could facilitate trust, but it needs to secure strong commitments from the members and increase transparency. Otherwise, the trust would have to be gained from outside of the governance premises such as pre-existing relationship among members.

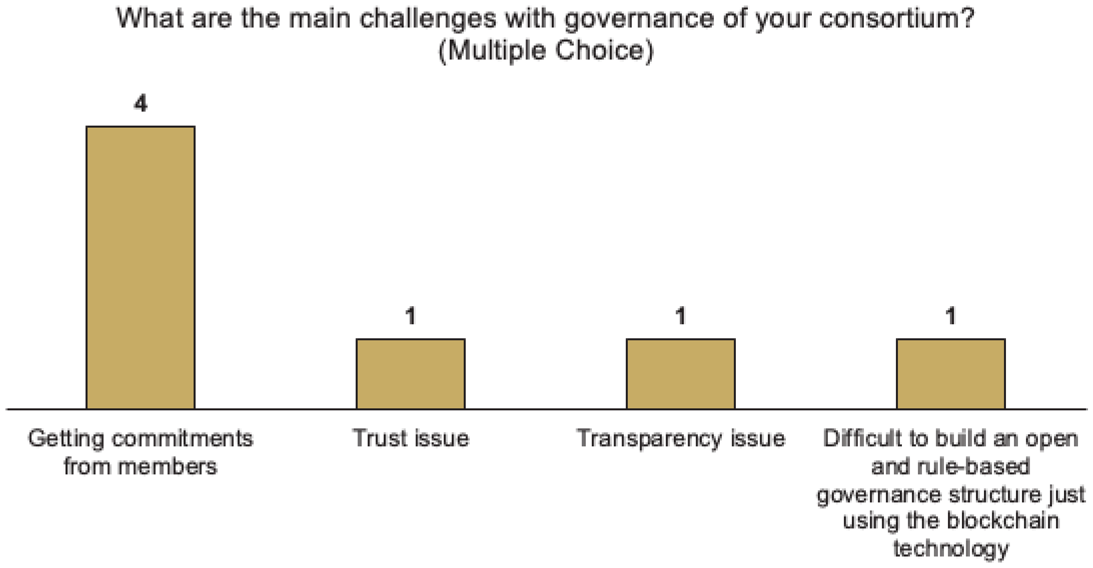
How are decisions made?



How is voting share for each member decided?

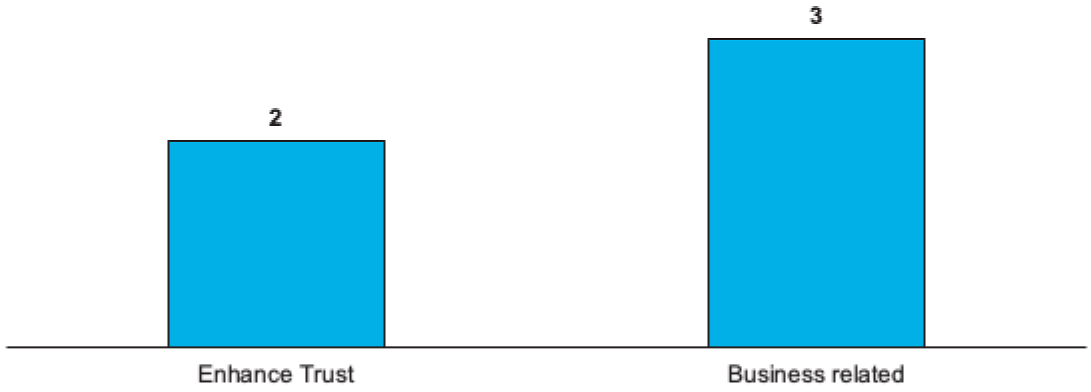




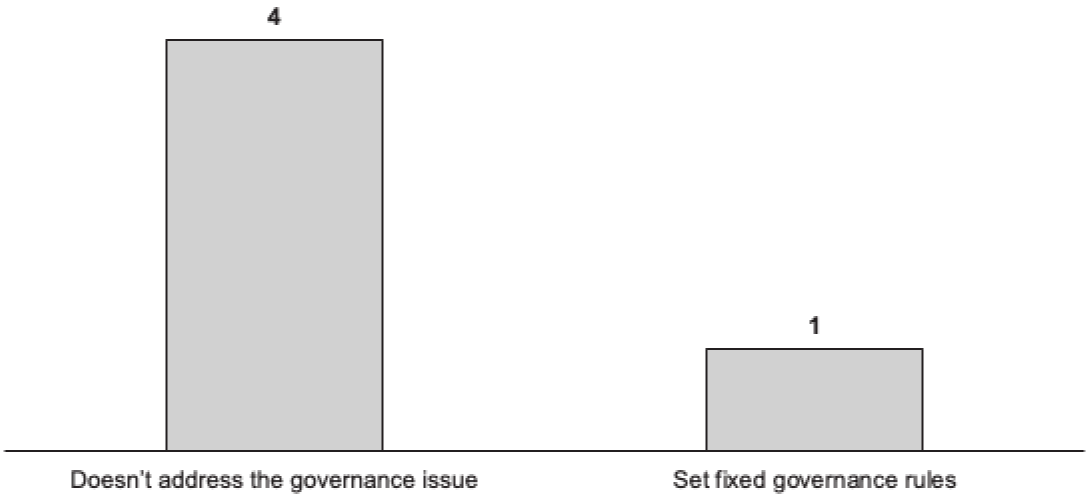


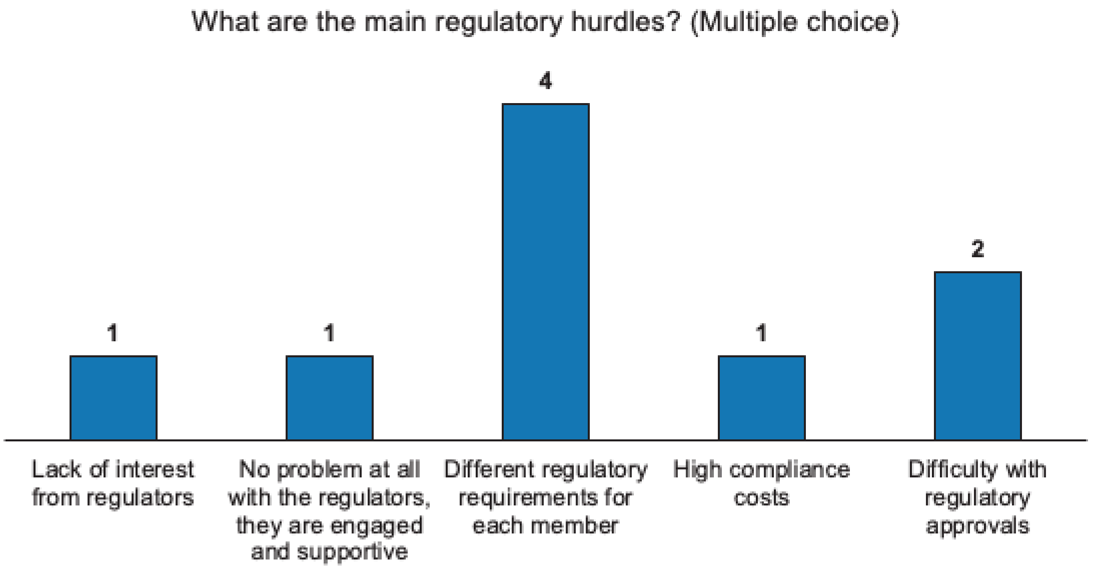
Furthermore, all participants claim that blockchain technology is necessary for their consortium. Reasons evoked include trust and operational efficiency. They also claimed that it is the best technology suited for the specific problem solved by the consortium. However, they most affirmed that the blockchain technology does not address governance. Few said that blockchain was needed to set fixed governance rules. This is an interesting point to see that the blockchain has limited applications on governance so far but there are some potentials in establishing fixed governance rules.

Why is blockchain technology needed for the consortium?



How exactly is the blockchain addressing the governance issue?





Privacy has been raised as a big concern for most of the participants. Indeed, despite having mechanisms to protect access to data, blockchain does not seem to be able to solve the privacy issue completely. Regulation seems to be another issue as each member faces different requirements, which is consistent with our findings from the literature. They do not have a clear mechanism to solve many issues implied by regulation.

Finally, the respondents all claimed to be satisfied by the level of learning through the consortium, despite their unwillingness to disclose revenue and cost performance in the survey.

c. Limits and Next Steps

The survey study shows interesting results but also comes with great caveats. As alluded earlier, the response rate is quite low. It is clearly not sufficient to make statistically significant inferences. Secondly, we have no mature consortium in our sample to study from. Thirdly, we got almost no response to the financial performance questions. For future research, it would be useful to continue the survey and increase the response rate. Additional questions can be considered based on the findings, such as the reason for lack of on-chain governance and the trust level for the horizontal and vertical consortium. Once we have more observations, a statistical analysis such as the partial least square method used by Olk & Young (1997) could be done.

IV. Conclusions

Business use case, governance, operation, data privacy, and regulations are all vital success factors for blockchain consortium with different weights. These factors facilitate trust, corporations, and efficiency gains in its way that are critical in translating the alliance into success. Based on our findings, we were able to rank the factors by its importance, as well as draw the transmission mechanisms among the success factors.

Success factors by rank

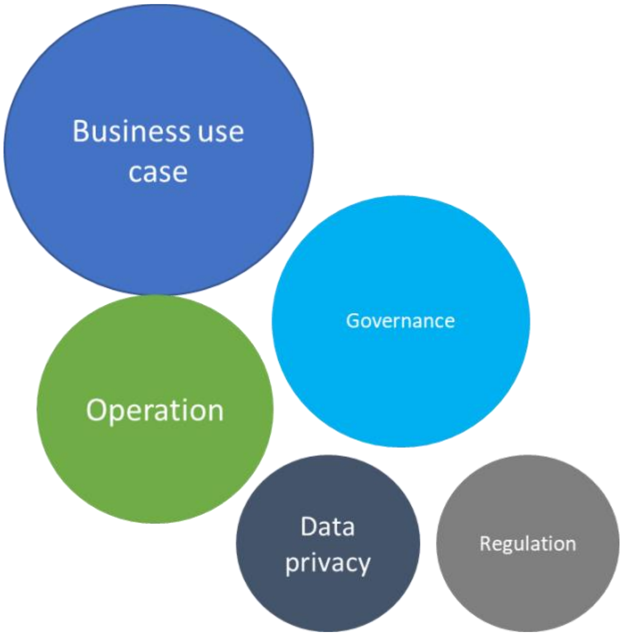


Figure 10: Success factors by rank.

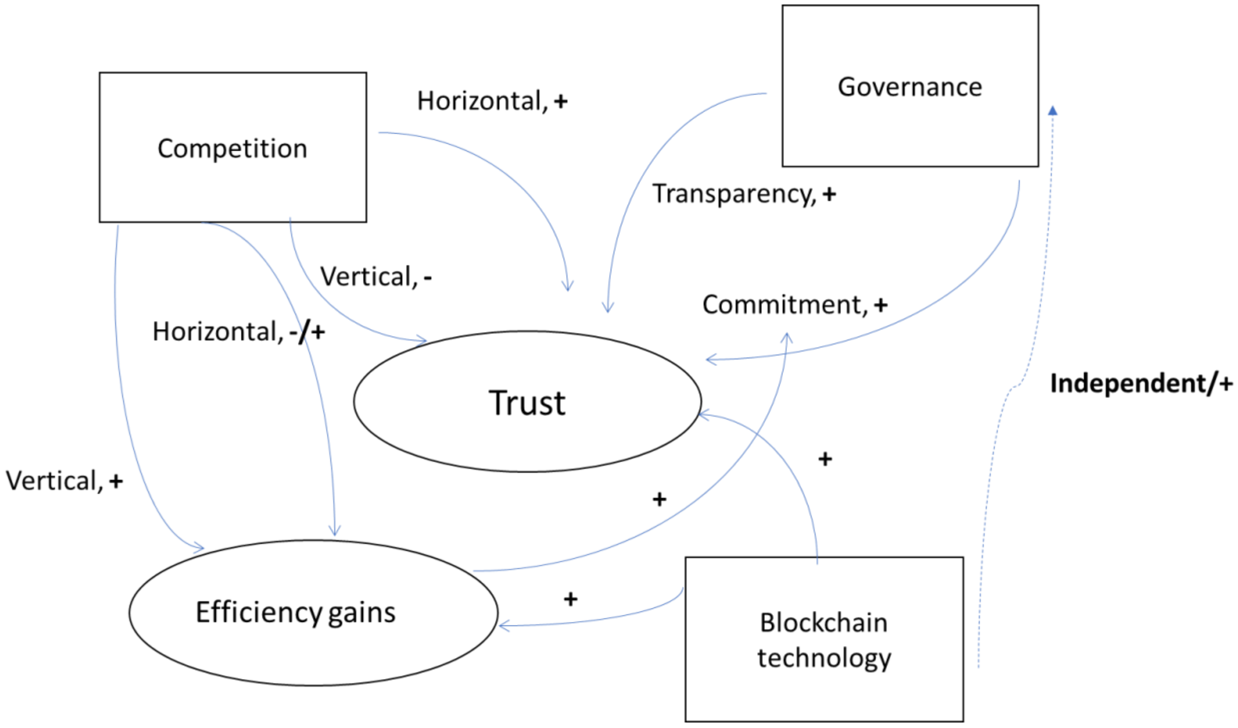
1. The identification of a clear business use case for all participants seems to be the major success factor. It helps to get commitments from participants, aligning incentives, and justifying the investment in such initiatives. Business values are more important in securing a commitment from members than governance, as suggested by our survey and literature. The importance of value creation in securing commitment and budget during the post-COVID would be even more important as firms are cutting down on capital expenditures.

2. Governance is another critical success factor, less so than the business use case. Interviews with experts, research, and our survey all suggested the importance of governance. It is related to promoting transparency and trust. However, governance seems to be mostly done off-chain rather than on-chain among consortia. This is probably

due to the early development and lack of capability of consortium, as the on-chain government typically is harder to do. Furthermore, with the capability to conduct on-chain governance, the consortium would still run into the governance issue of setting the standard and consensus for writing the rules coded on the blockchain. Our study shows that getting commitments from members is the biggest challenge for governance, rather than the trust, transparency, or democratic governance structure. We think to start by having a strong business use case would help secure commitments and create synergies with governance.

3. Data privacy and regulations are somewhat easier to manage than the creation of business use cases and governance.

Transmission mechanisms



Blockchain technology alone is not a success factor for a consortium. It enhances trust and is absolutely needed for the blockchain consortium solution, but it seems to be independent of governance effectiveness.

Trust has convoluted relationships with different success factors. Blockchain technology, governance, and competitions all could facilitate trust. We identified competition as a vector of trust between participants, instead of a cause for failure. This is counter-intuitive, and it would be interesting to estimate spillovers from consortia to confirm or not that trust translates into success. Governance could enhance trust, but it is very difficult. It would require the governance structure encourages commitment and enhance transparency to establish trust. Otherwise, governance is considered independent of the trust. As we have learnt, efficiency gains are the most effective in securing commitments and interests. So, the governance would need to work together with strong business use case to achieve trust.

References

Acharya, V., Yerrapati, Anand Eswararao, author, & Prakash, Nimesh, author. (2019). Oracle blockchain quick start guide a practical approach to implementing blockchain in your enterprise. Birmingham.

Anon, MUFG executes first transaction on komgo, a blockchain based commodity trade finance platform. MUFG EMEA. Available at: https://www.mufgemea.com/media/mufg-executes-first-transaction-on-komgo-a-blockchain-based-commodity-trade-finance-platform/ [Accessed May 18, 2020].

Bengtsson, M. and Kock, S. (1999), "Cooperation and competition in relationships between competitors in business networks", Journal of Business & Industrial Marketing, Vol. 14 No. 3, pp. 178-194. https://doi.org/10.1108/08858629910272184

Baumert, M., 2019. Blockchain Consortia A legal roadmap to a dynamically changing regulatory landscape: Media Mentions: Barnes & Thornburg. Blockchain Consortia A legal roadmap to a dynamically changing regulatory landscape | Media Mentions | Barnes & Thornburg. Available at: https://btlaw.com/insights/news/2019/blockchain-consortia-a-legal-roadmap-to-a-dynamically-changing-regulatory-landscape [Accessed May 18, 2020].

Cecere, G., Corrocher, N. and Battaglia, R.D., 2015. Innovation and competition in the smartphone industry: Is there a dominant design?. Telecommunications Policy, 39(3-4), pp.162-175.

Dib, O., Brousmiche, K.L., Durand, A., Thea, E. and Hamida, E.B., 2018. Consortium blockchains: Overview, applications and challenges. International Journal On Advances in Telecommunications, 11(1&2).

Ernst & Young, 2019. Total cost of ownership for blockchain solutions. https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf

Fontana, R., Girod, S.J.G. & Králik, M., 2019. How Luxury Brands Can Beat Counterfeiters. Harvard Business Review. Available at: https://hbr.org/2019/05/how-luxury-brands-can-beat-counterfeiters [Accessed May 18, 2020].

Goldstein, D., 2019. Enterprise Blockchain: Understanding the Landscape. sci.smithandcrown.com. Available at: https://sci.smithandcrown.com/research/enterprise-blockchain [Accessed May 18, 2020].

Gogan, J.L., Jr., U.J.G. & Rao, A., 2007. Learning in a consortium: a longitudinal case study. International Journal of Technology Management, 38(1/2), p.90.

Insights, L., 2019. LVMH unveils luxury industry blockchain with Microsoft, ConsenSys. Ledger Insights - enterprise blockchain. Available at: https://www.ledgerinsights.com/lvmh-luxury-blockchain-microsoft-consensys/ [Accessed May 18, 2020].

Marco Polo, 2020. Payment Commitment on the Marco Polo Network. Marco Polo. Available at: https://www.marcopolo.finance/payment-commitment/ [Accessed May 18, 2020].

Manders, S., 2017. Banks unveil roadmap for we.trade blockchain platform. Global Trade Review (GTR). Available at: https://www.gtreview.com/news/fintech/banks-unveil-roadmap-for-we-trade-blockchain-platform/ [Accessed May 18, 2020].

Medrano, L., 2001. On the agency insurers role in competition among insurance companies.

Mesquita, L.F. and Lazzarini, S.G., 2009. Horizontal and vertical relationships in developing economies: Implications for SMEs' access to global markets. In New frontiers in entrepreneurship (pp. 31-66). Springer, New York, NY.

Morris, N., 2020. Automated trade payments prove popular for we.trade blockchain. Ledger Insights - enterprise blockchain. Available at: https://www.ledgerinsights.com/wetrade-blockchain-trade-finance-automated-payments/ [Accessed May 18, 2020].

Osarenkhoe, A., 2010. A study of inter-firm dynamics between competition and cooperation–A coopetition strategy. Journal of Database Marketing & Customer Strategy Management, 17(3-4), pp.201-221.

Salmon, J. & Myers, G., 2019. Blockchain and Associated Legal Issues for Emerging Markets. ifc.org. Available at: https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F [Accessed May 18, 2020].

Samuel M. Smith Ph.D, 2020. KEY EVENT RECEIPT INFRASTRUCTURE (KERI) DESIGN1, v2.24 2020/05/05 v1.62 2020/02/11 v1.60 2019/07/03.

Shijie Zhanga, Jong-Hyouk Leeb, a Protocol Engineering Lab. 2019. Analysis of the main consensus protocols of blockchain, Sangmyung University, Republic of Korea b Sejong University, Republic of Korea.

Team, E., 2020. Blockchain consortia need good governance: but how? Finextra Research. Available at: https://www.finextra.com/blogposting/18543/blockchain-consortia-need-good-governance-but-how [Accessed May 18, 2020].

Thompson, F., 2020. Trade finance blockchain consortia: where are we now? Global Trade Review (GTR). Available at: https://www.gtreview.com/magazine/volume-18-issue-2/trade-finance-blockchain-consortia-now/ [Accessed May 18, 2020].

Updegrove, A., 2007. ConsortiumInfo.orgYour online research resource for Standards and Standard Setting. The Essential Guide to Consortia and Standards. Available at: https://www.consortiuminfo.org/essentialguide/forming1.php [Accessed May 18, 2020].

Van de Voorde, E. and Vanelslander, T., 2010. Market power and vertical and horizontal integration in the maritime shipping and port industry.

Wass, S., 2019. komgo unwrapped: Financing commodity trade on blockchain. Global Trade Review (GTR). Available at: https://www.gtreview.com/magazine/volume-17-issue-1/komgo-unwrapped-financing-commodity-trade-blockchain/ [Accessed May 18, 2020].