LTI Let's Solve | solar

A Larsen & Toubro Group Company

Whitepaper

Blockchain Consortium Approach

Author: **Ravi Raj Singh, Steen Madsen**

Table of Contents

1. Introduction 3

2. Key challenges in construction industry 4

3. Consortium approach - key considerations 6

3.1 Collaboration 6

3.1.1 Consortium's purpose, vision and mission 6

3.1.2 Use-case design and development 8

3.1.3 Initial network setup 9

3.1.4 Incentivization 13

3.2 Governance 14

3.2.1 Roles and responsibilities 14

3.2.2 Participation rules and guidelines 15

3.2.3 Participation management 17

3.2.4 Dispute resolution 18

3.2.5 IP management 18

3.3 Operating considerations 20

3.3.1 Node hosting 20

3.3.2 Data management 21

3.3.3 Dispute resolution – blockchain network 22

3.4 Financial considerations 23

3.4.1 Expenses 23

3.4.2 Funding 23

3.5 Security 26

3.5.1 Risk assessment 26

3.5.2 Threat modelling 27

3.5.3 Data privacy 27

3.5.4 End-point security and key management 28

4. Conclusion 29

Introduction

Since its inception, Blockchain technology has evolved beyond cryptocurrencies and steadily gained mainstream attention due to its potential to disrupt business models and operating processes across a variety of industries. The technology brings with it the promise of traceability, immutability and transparency, thereby reducing disputes and helping foster trust among stakeholders transacting on the network without unnecessary intermediaries.

An emerging trend in the exploration and adoption of new technologies like Blockchain is to form a consortium with like-minded organizations to develop, deploy and scale industry-wide solutions. This coopetition model allows organizations to quickly and cost-effectively establish unique positions within an evolving marketplace by leveraging their complementary strengths. This could eventually lead them to deliver better services to clients and customers in addition to benefiting themselves.

In this whitepaper, we discuss the approach to building a viable Blockchain consortium, tuned to the needs of the construction industry and how member organizations may leverage Blockchain to create decentralized networked solutions to solve industry-wide issues.

2. Key Challenges in Construction Industry

A single construction project generally involves several Contractors, Original Equipment Manufacturers (OEM), Suppliers, Logistics partners, and these are just actors in the supply chain alone. Besides these, a typical project may also involve Banks, Insurers, Designers and Regulators.

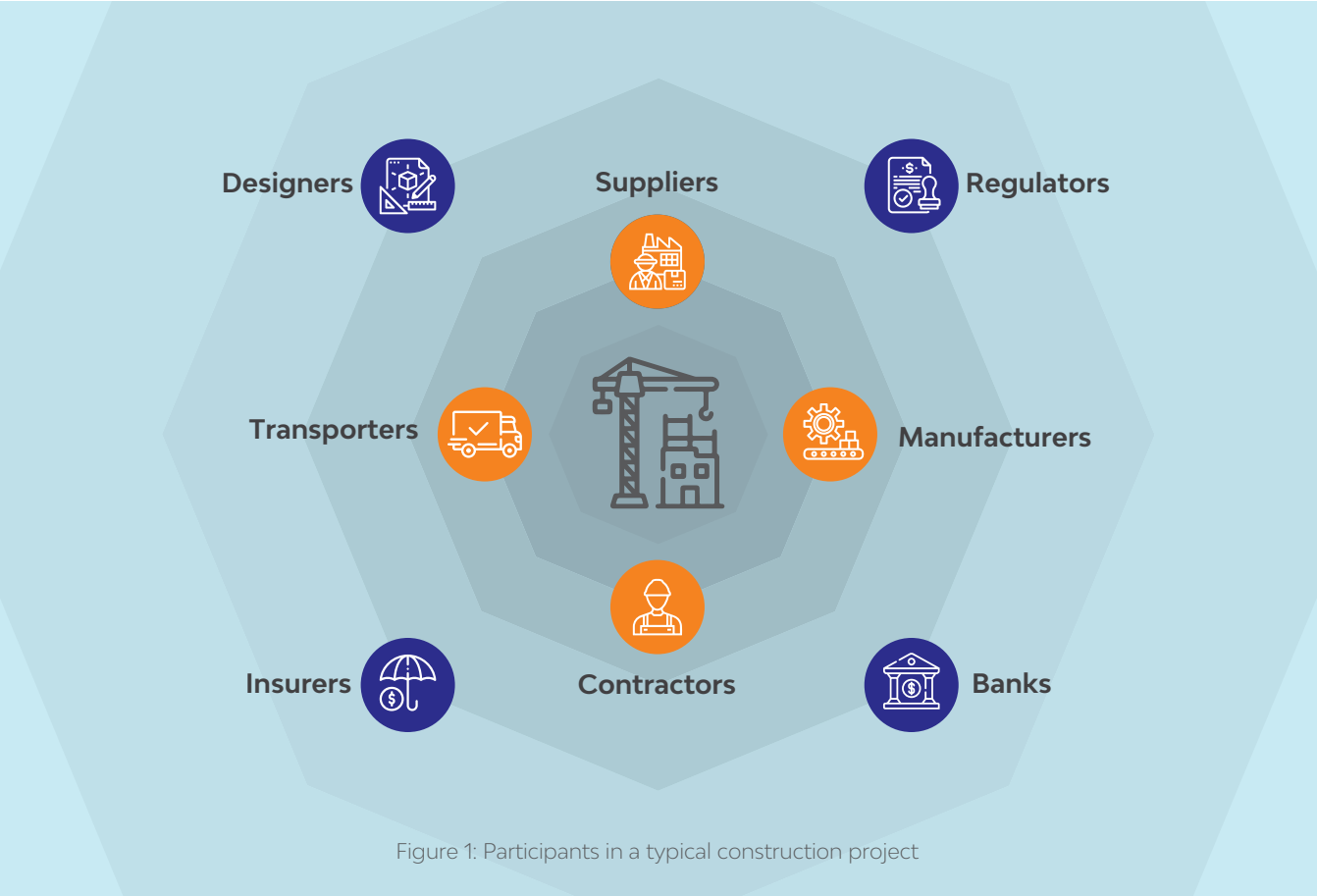


Figure 1: Participants in a typical construction project

Managing timelines, inventory, budget and work-in-progress with so many actors becomes a challenging task since these actors generally have their own IT service providers and often operate in informational silos. Additionally, much of the communication still happens over phone calls and emails. This hinders real-time information sharing, making it very difficult to keep track of updates and make timely adjustments. Real-time updates are especially critical in the case of logistics, where deliveries to the construction site must be made in a given time slot and for inventory management, so that items can be replenished on time.

Furthermore, much of the data that is captured during the project course is either difficult to access (if not lost) or is inconsistent, decreasing its usability to solve issues and drive decisions for current as well as future endeavours.

Also, many processes still require manual intervention, or are dependent on paperwork, which is both inefficient and prone to errors. Thus, there is a lack of complete and reliable data making it very difficult to ascertain liability when something goes wrong and is generally the cause of disputes and delay in payments.

These are some of the major challenges due to which construction projects are so complex, and therefore, are considered very risky. According to the Dansk Byggeri* (Danish Construction Association), this is the primary reason why construction companies in Denmark, struggle to acquire bank credit, which amounts to approximately 70% of their total credit supply.

Blockchain's unique capabilities can help alleviate aforesaid pain points by bringing transparency in the processes and provide much-needed visibility to involved stakeholders. Owing to its immutable nature, the data captured on the underlying ledger can be trusted as a single source of truth by all stakeholders, which would not only reduce discrepancies and disputes, but also enable better management of project workflows. We firmly believe that all organizations in the construction space stand to benefit greatly by collaborating on use-cases in areas such as project management, supply chain, inventory management, payments, to name a few.

3. Consortium Approach - Key Considerations

In the following sections, we discuss some of the key considerations that organizations may find useful in forming a viable ecosystem.

3.1 Collaboration

Generally, the idea of forming a consortium starts organically between few organizations without any formal contractual agreements and rarely as a separate legal entity. This can be termed as the 'pre-consortium' stage. To begin the dialogue, each organization typically nominates representatives who would act as the interim 'governing body' of the 'to-be' consortium. Their primary objective would be to forge the Memorandum of Understanding (MoU) with partnering organizations, based on which they would collaborate initially. Key decisions that need to be taken by them include:

1. Consortium's purpose, vision and mission
2. Identifying & developing viable use cases
3. Initial network setup, governance and funding

These are discussed in detail in the sub-sections below.

The endgame of these discussions is to create a legally binding consortium contract. Therefore, it is advisable that each organization nominates someone who has decision-making authority or at least direct access to someone with decision-making authority in their respective organizations. This will ensure that the consortium's functioning is not hindered in the time to come because of the representative's inability to drive decisions in their organization.

3.1.1 Consortium's Purpose, Vision and Mission

Consortia are of many types and run on different models tailored to the specific needs of the member organizations. For a consortium to be effective, the founding members should approach the development of the 'to-be' consortium with clearly defined goals and a shared vision of how the consortium would promote its strategic objectives and those of its fellow members, both in the short as well the long term.

To start with, the primary question to be considered is, will the consortium be:

Technology-focused

Aimed at building a neutral Blockchain platform that can be used across industries, essentially driving technical standards and best practices. E.g. R3 Corda, Hyperledger, etc.

Business-focused

Aimed at building solutions for cross-industry or industry-specific problems using available Blockchain platforms with the intention of driving cost-saving, efficiency, and so on. E.g. TradeLens, a supply chain platform built on Hyperledger; etc.

Note: We will be focusing on Business-focused consortia for the remainder of this document.

Next, members must agree on which use cases to pursue, which participants would be involved, and in what capacity. These decisions are largely driven by the consortium's vision i.e. the kind of network that is being built and the magnitude of change that this consortium plans to bring about. Members must decide whether they are trying to build a network that would solve problems only for their businesses and the parties they engage with, such as their suppliers and customers; or would it be a network where even competitors can collaborate to solve problems collectively as an industry and drive change. For example, we can track and perhaps reduce carbon emission in construction projects with the help of reliable data provided by suppliers, logistics partners, construction companies, etc.

Early alignment is essential as each member's willingness to invest would depend on what they hope to achieve through this collaboration. For example, while some members may be looking to bring benefits to their business such as operational efficiency or cost savings, others might just want to build solutions that can be monetized.

Lastly, it must be kept in mind that since there are no formal agreements at this stage, things tend to move slowly. Therefore, members must set up and adhere to, strict timelines regarding activities that need to be undertaken. This must be clearly defined in the Memorandum of Understanding (MoU), including what exactly is expected from each member.

3.1.2 Use-Case Design and Development

Building an ecosystem would entail designing a solution road map of sorts. A typical approach to this is depicted below:

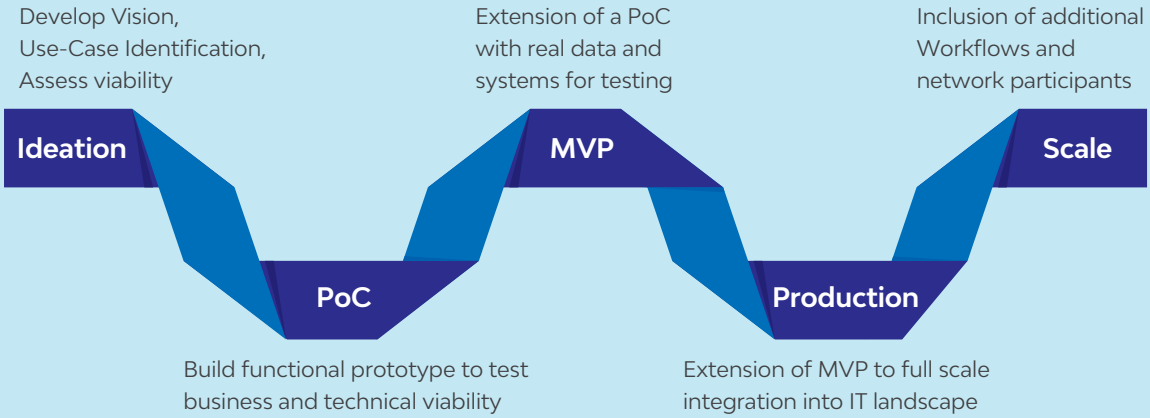


Figure 2: Commercialization Road Map

In the ideation phase, members will be required to map their current processes and identify common pain points. Next, they must identify where and how Blockchain can help in improving said processes and alleviate pain points.

For example, in a typical construction project, the flow of information is often restricted or not in sync, as there is a lot of point-to-point integration between different entities. This information asymmetry often leads to delays and disputes, costing all the involved stakeholders dearly in terms of time, resources and revenue. Therefore, a good use case could be about building a distributed application, that would provide access to real-time updates, like changes in the delivery schedule or order status thereby, acting as a single source of truth for all participating entities.

Another important aspect of identifying a potential use case is also to look at its potential Return on Investment (ROI). This can be done by comparing the potential benefits against the investment required in terms of effort, time and funding to productionize a solution. This can be a bit tricky as organizations tend to focus more on the financial benefits of the proposed solution. While having these discussions it is important to understand that benefits may not always be tangible resulting in financial gain, but could also be intangible, such as increased trust among entities resulting from transparency.

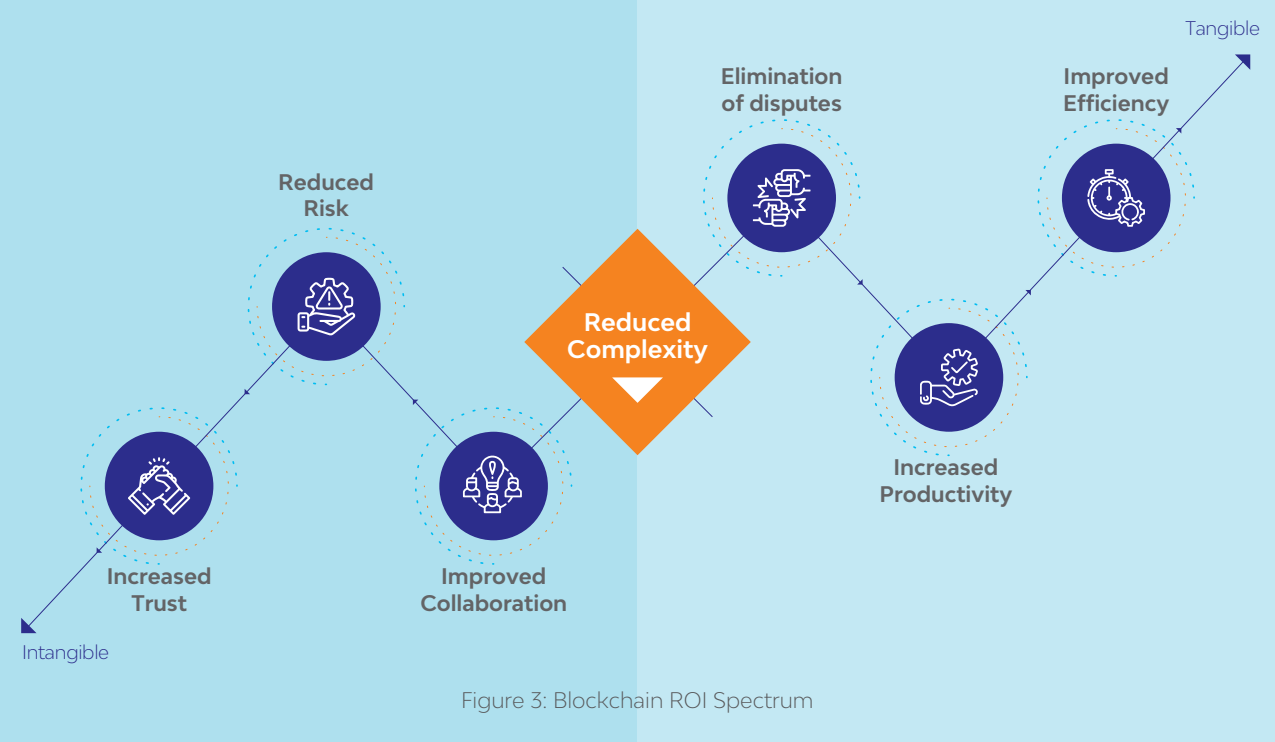


Figure 3: Blockchain ROI Spectrum

Taking the above into consideration, members can home on to prospective use-cases. These can be tested through a simple Proof of Concept (PoC) exercise involving fewer participants. The scope of the PoC must be limited so that the performance of the proposed solution can be measured easily. At this stage, the key focus should be on testing and understanding the underlying technology and discerning the viability of the use case.

For the PoC to be deemed successful, it is rather important to define and agree on realistic success criteria and timelines based on which definitive decisions can be taken.

It is also worthwhile to consider the risks that may be introduced due to the implementation of such a solution and if these should ever materialize, how they would be mitigated. These are discussed later in this document, under the section titled 'Security'.

3.1.3 Initial Network Setup

Once a viable use-case has been identified, a suitable Blockchain platform should be selected. This decision should not only take into account the PoC but also the needs of the consortium in the long term. Key considerations while selecting an appropriate Blockchain platform include:

Privacy **Scalability** **Costs**

Privacy

Essentially there are 2 types of Blockchain networks:

Public and Permissionless

- Anyone can join the network
- Rules and permissions are the same for everyone, therefore transaction privacy cannot be configured

Private and Permissioned

- Participation is invite-only
- Rules and permissions can be set by the members, hence access to the network and transaction privacy can be configured easily

Scalability

Mainly refers to the platform's ability to support a growing number of transactions as new nodes and workflows are added to the network. A use case that is transaction-intensive like payments, would require a high TPS (Transactions Per Second), whereas a non-transaction intensive use case like supply chain tracking, may not require a high TPS rate. In most Blockchain networks, performance is inversely proportional to the number of participants on the network and the amount of data that is being stored on it.

Costs

Permissionless Blockchains run on open source software and usually charge transaction fees to commit transactions to the network. These fees are generally in the form of the underlying native cryptocurrency. A good example would be that of the Ethereum platform, where a user must pay a certain amount of 'ethers' to post a transaction on the network. The only catch here is that these cryptocurrencies are highly volatile, which introduces financial risk to the transacting parties.

On the other hand, Permissioned Blockchains generally run on licensed software and may or may not have transaction fees associated with them. A good example would be R3 Corda which comes in both open source, as well as enterprise versions and does not have any associated transaction fees. A more detailed view of the costs involved is discussed in the section 'Financial considerations'.

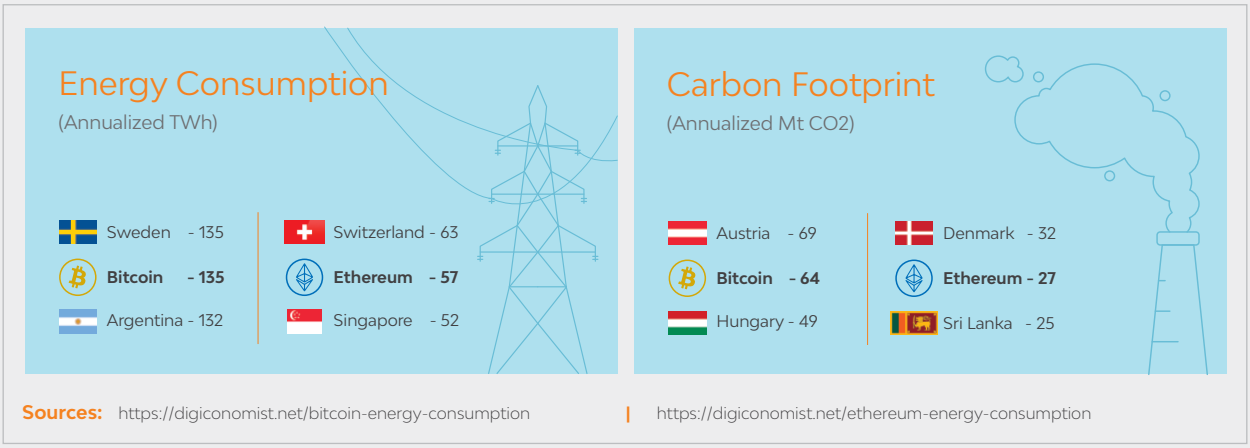
Note: It may also be worthwhile to consider that multiple use-cases may require different types of Blockchain platforms, and that the consortium may not need to stick to only one.

Environmental cost

While deciding on the Blockchain platform (Public or Private), organizations must also consider the impact that their solution might have on the environment. In recent times, there has been a growing concern about the energy consumption of Blockchains especially the public ones like Bitcoin and Ethereum, with many studies bringing to light their power-hungry nature and consequentially their contribution to carbon emissions.

The primary reason for this huge energy consumption is attributed to the consensus mechanism based on which these decentralized networks function. Currently, most Public Blockchain platforms use the 'Proof of Work' consensus mechanism, which is dependent on 'mining'. It is with this mechanism that transactions are validated and verified on the Blockchain network. Here miners on the network, have to solve trivial albeit complex, computationally intensive cryptographic puzzles in order to commit the next block of transactions on the chain. The miner(s) who solves the puzzle first, adds the next block and is rewarded in the underlying cryptocurrency for the work done. The work of other miners, however, goes to waste. This process along with the rising cryptocurrency prices, incentivizes miners to deploy increasingly powerful systems to improve their chances of getting the reward. Overall, this results in the network consuming more and more energy every day.

Today the power consumption of these networks has grown to epic proportions, surpassing that of many nations. Additionally, many studies have revealed that most of the energy used by mining operations comes from fossil fuels and therefore contributes significantly to carbon emissions. To help put this in perspective, the energy and carbon footprints of two of the world's most prominent networks - Bitcoin and Ethereum are illustrated below:



As alarming as this may seem, it does not mean that Blockchains are inherently unsustainable. We can limit the power consumption by using alternate consensus mechanisms such as 'Proof of Stake' or by using Private Blockchain platforms which by design are more efficient.

Once a suitable Blockchain platform has been selected and PoC has been conducted successfully i.e. viability of the solution has been proven, the next step would be to build a Minimum Viable Product (MVP). This is the stage where members must start formalizing the 'consortium contract'. The first order of business for the founders would be to estimate the minimum number of network participants required to set up a viable ecosystem in the short term. These could be any of the vertical participants (upstream or downstream) or horizontal participants which have the same function(competitors).

It is advisable to start small, with 3 to 5 members depending on the use case, and then scale accordingly. Involving too many organizations at the start would just complicate and probably delay decision-making. Equally important is to choose the right organizations to partner with, in the beginning. While approaching potential participants, careful thought must be given to what these organizations can bring to the table in terms of technology, funding, market power, and even more so, if they have the right intent and motivations to be part of the platform.

Once appropriate partners have been identified, discussions regarding 'to-be' consortium's policies can begin. This would include its governance (both in the 'real world' and on the 'Blockchain network'), as well as its funding. These are covered in subsequent sections.

While designing these policies, it must be kept in mind that one of the most common reasons such ventures fail to take off is because the initial set of members often design the consortium policies in a way that tends to favour them. This may work in the short term, but is likely to undermine collaboration in the long run.

Once these policies are defined and agreed to, by all the initial members, a legally binding consortium contract must then be signed. Completing these activities promptly would greatly reduce the consortium's 'time-to-market'. It is advisable that only after the consortium contract has been signed, MVP development may commence.

3.1.4 Incentivization

For the consortium to function and grow successfully, members must be adequately incentivized to join the consortium, adhere to its rules, and perform assigned duties. This begins firstly by understanding their interests and aligning these with that of the consortium. Listed below are some of the important aspects that organizations look at, when they are considering joining a network:

- **Consortium's Organizational structure**
- **Quality of the current members and their influence in the industry or geography**
- **How well it's funded**
- **Fairness and inclusivity of governance policies**
- **Participation cost v/s benefits**
- **Maturity of the solution(s)**
- **Adoption of the Blockchain platform being used**

The consortium should be able to clearly communicate to existing and potential participants about the benefits they would enjoy by being part of the consortium and being early adopters. Listed below are some of the direct benefits:

- **Additional revenue and/or cost savings brought in by solving common pain-points**
- **Accelerated learning and development, where all participants pool resources and experience to bring innovative solutions to the market, which they may not be able to do alone**
- **Having a role in influencing industry standards and best practices**
- **Sharing the risk that comes with experimenting with new technologies**
- **Networking opportunities and access to a wider set of audience**

Additionally, to attract and incentivize members, the consortium could also:

- **Offer a stake in the IP being developed or a percentage of profits that may be generated from it in later stages**
- **Extend participation in consortium governance roles**
- **Allow and empower members to design and execute their own use cases**
- **Provide access to historic data and resources developed by the consortium such as research reports, whitepapers, etc**

Finally, it is of utmost importance that the network must be designed in such a way that it offers the same set of benefits to a group of participants. For example, all the suppliers on the network must benefit equally by being part of the ecosystem and not just the larger ones.

3.2 Governance

Governance is unquestionably the most important aspect of a well-functioning consortium and could give it, its competitive advantage. Creating the framework for organizations to effectively work together is just as important, if not more, as building the technology solution itself. Like with any joint venture, it can be expected that member organizations will have dissimilar needs, interests and priorities, that would need to be aligned in order to form the consortium policies. Therefore, it is essential to plan who will be involved in the decision-making process, what roles and responsibilities each member will have, and how differences in opinion will be resolved. Additionally, as new members join, these policies would have to be amended to accommodate their interests and goals as well. Hence, an appropriate amendment mechanism must also be put in place.

As discussed in the sections above, forming these policies would initially fall on the shoulders of the consortium's interim governing body. Once the consortium is up and running, these duties can then be transferred to the appointed steering committee.

Another important decision that needs to be made is with regards to the kind of engagement under which, the consortium will operate. Would it be only through contractual agreements among participating entities or would the consortium operate as a separate legal entity altogether.

Discussed in the below sections are some of the important considerations related to the consortium's governance.

3.2.1 Roles and Responsibilities

Outlining the roles and responsibilities for each type of member early on is essential to the success of the consortium. The governing body must contemplate the following:

- **How many committees/teams would be required and what function would they perform?**
- **What would be the strength of each committee/team?**
- **Which member organizations would be allowed to take part in the committee/team?**
- **Can these committees/teams have non-member participants?**
- **How would members of these committees/teams be selected? Would it be through voting or would it be a rotational power structure?**
- **How long will the term of these members last in a specific role?**

Provided in the table below are some of the common roles and their respective responsibilities that generally exist in consortia:

Role	Key Responsibility
Steering Committee (Preferably C-suite executives from member organizations)	• Consortium governance • Fund raising and deployment • Selecting technology, business and legal partners
Project Management Team(s) (Project Managers and Business Analysts)	• Developing Project/Use Case plan and managing deliverables • Day-to-day management of project schedule, budget, quality and team members • Regularly report to Steering committee
Development and Support Team(s) (Developers Blockchain, Cloud, etc.)	• Blockchain implementation, testing, deployment and integration activities
Security and Architecture Review Group	• Develop consortium's data security policies • Implement and periodically assess consortium network security
Dispute Resolution Team	• Develop dispute resolution framework • Arbitration and mediation
Advisory Board (Business, Technology, Tax and Legal specialists)	• Provide counsel on issues raised by Steering Committee and Dispute resolution team • Monitor consortium's performance

Again, the organizational structure of the consortium would have to evolve as the consortium grows. For example, in the initial stages, the decision-making power may be limited to the founding members, but as the scope, the number of projects, and members increase, the consortium's governance could be opened up to other members also. However, it must also be kept in mind that decision-making may become cumbersome if the governing body becomes too large. Therefore, it is advisable that sub-committees be formed, and decision-making be distributed accordingly.

3.2.2 Participation Rules and Guidelines

While deciding on the rules and guidelines for membership, the governing body must keep in mind that all the members of the consortium, old and new, must be represented reasonably. These must be designed in a such way that does not allow any member to dominate the network, even if they are founders or big industry players. As mentioned earlier, fair play and inclusivity, especially in a Blockchain consortium, are paramount to the growth of the ecosystem.

It is also worthwhile to categorize the membership into various levels or types. This would entail defining the benefits participants would enjoy at each level, such as decision-making authority, stake in IP being developed, etc; and what support would be expected from them in terms of funding, technology, and/or governance to fulfil the goals of the consortium.

Once the membership levels are decided, eligibility criteria for each type of member must be worked out. As an example, a list of membership levels is provided in the table below:

Membership	Benefits	Expectation
Founding Member	• May be given a permanent seat on the steering committee. • General membership benefits • Could be allowed to execute use cases independently	• Provide seed funding (upfront and/or annual) • Provide vision, support and governance • Use case identification and participation • Contribute infrastructure and data
Exclusive Member	• Right to run for a seat on the steering committee for a specific time period • General membership benefits • Could be allowed to execute use cases independently	• Buy in: Same level of investment as that of the founding members • Assist in governance • Participation in use case execution • Contribute data and infrastructure
Standard Member	• General membership benefits only • May or may not be allowed to execute use cases independently • Access to Consortium data and resources	• Buy in: Less than Exclusive members (e.g. annual fees could be 1/3rd that of exclusive members) • Contribute data and infrastructure
Open Member (Non-profit / Academia / Startups)	• Access to historic datasets, reports, etc. for research purposes or validation	• Buy in: Could be given free membership for a specific period • Participation in use case identification and execution
Regulatory Member	• Right to run for a seat on the steering committee. • General membership benefits	• Buy In: Could be free • Assist in governance • May participate in use case identification and execution • Help drive adoption and standardization in the industry
Contract-based Participant	• Non-members • No membership benefits	• Buy-in: Not Applicable • Contracted for a limited time and specific purpose only, e.g. technology providers

It is important to differentiate between members of the consortium and the participants on the network. All members of the consortium may not be part of the blockchain network (eg. investors) and vice versa. On the blockchain network, each participant must be categorized based on their function. For example, in a construction supply chain use case, all suppliers would fall under a single group. Similarly, other actors such as logistics partners, contractors, OEMs would fall into separate groups. Here, each group of actors on the network would be governed by the same rules, have the same set of responsibilities and enjoy the same benefits.

3.2.3 Participation Management

It is important for any consortium and more so for a Blockchain network to have a well-defined criteria that clearly states which entities can and cannot become participants. Once the membership levels are decided, eligibility criteria for each type of member must be worked out. Membership criteria may be bifurcated into 'general', applicable to all members and 'specific', applicable to each membership level or group. Setting up these criteria would fall under the purview of the governing body. Other than conducting a due diligence process, wherein participants identity is checked, it is important to consider whether participants are required to:

- **Have certain licenses, e.g. to certify compliance with consortium's data security standards**
- **Meet certain financial thresholds, to ensure consortium's funding is not compromised**
- **Have certain regulatory qualifications, as adding participants in new jurisdictions, may subject the consortium to additional regulatory obligations**

Once such criteria are set, a process to determine whether a potential new participant meets these criteria needs to be put in place. An important thing to remember is that these criteria are not set in stone and may change as the consortium matures.

The governing body must also prepare similar guidelines for a scenario when members leave the consortium. This could be voluntarily due to misaligned goals, insolvency, etc, or involuntarily due to security breach or misuse of data, etc. The governing body should clearly define in advance the conditions under which a member will be offloaded forcefully. This needs to be communicated to all participants to avoid any disputes and\or litigations at later stages when such situations arise.

Equally important is to prepare a transition plan to ensure that after a participant has been offloaded, functioning of the consortium is not hampered or compromised. This plan should take into consideration:

- **Who would take up the roles and responsibilities of the ex-participant (especially if it's a founding member)?**
- **What would happen to their stake in the IP (if any)?**
- **What would happen to the consortium-related data that they possess?**

3.2.4 Dispute Resolution

Disputes in the 'Real world' may arise due to:

- **Inactivity of a member organization**
- **Specific decisions taken by a committee on policy or membership, and so on**
- **Compliance or legal violations; etc.**

An internal dispute resolution mechanism aimed at solving such disputes between members must be formulated. These disputes could be tricky and may result in an unfavourable outcome, such as members pulling out of the consortium or at worst, litigations, which would be both time-consuming and costly. Initially, the governing body could be responsible for resolving disputes, but as the consortium grows, it is advisable that a separate dispute resolution body be formed, so that any disputes may be resolved fairly and as quickly as possible. The following must be considered while deciding the strength and composition of such a body:

- **Should members of this body include independent/neutral third-party individuals or only representatives from member organizations?**
- **Would the team comprise of a fixed set of members or would it be on a case to case basis?**
- **What would be the qualification criteria to be on this team?**

The dispute resolution mechanism must be transparent to all consortium participants in order to ensure decisions are viewed as impartial.

Disputes may arise on the Blockchain network as well. This is covered in a separate sub-section under 'Operating considerations'.

3.2.5 Intellectual Property (IP) Management

It is advisable that members identify and understand IP assets that will be created in the pre-consortium stage itself. These may include software or new processes being developed as part of this collaboration. The IP assets may not hold much value in the beginning, nevertheless it is very important for members to discuss and agree at the earliest on:

- **How members can and cannot use these assets within their own organization?**
- **Who all would have a stake in these assets?**
- **What would happen when new members join the consortium, would they be given a stake in the IP being developed?**
- **What would happen to the stake of the members that leave the consortium?**
- **Will the IP assets be owned by the members through contractual agreements or would they be attached to the consortium entity (in case one has been formed)?**

The first step here would be to create and agree on a mechanism based on which IP assets will be allocated and transferred (as and when required). A straightforward approach could be to assign ownership to only those members who were involved in the development of the asset. They should be given an appropriate stake based on their contribution, whereas other existing members and the new ones who join can be allowed to use it for a fee. In case a member leaves the consortium, their stake can be bought by members or be distributed among the ones who already have a stake in it. Having these types of procedures set in the beginning would save the consortium from disputes at later stages once these IP assets become more and more valuable.

The next step would be to determine the potential value of identified IP assets. This exercise would not only help in formulating the licensing agreements and appropriate fees once the assets are developed but may also be leveraged to attract new participants and investors to the consortium. Additionally, knowing the value of IP assets would help in deciding what course of action is to be taken in case there is a dispute among members or due to infringement by an external party. For example, is the value of the IP large enough to initiate a lawsuit or would it be better to settle the matter outside of court. It is advisable that each organization involve its legal team in such discussions.

Furthermore, it may also happen that some of the member organizations as part of their contribution to the consortium, bring their own IP assets to the table. Careful consideration must be given to how these 'background' IP assets can be protected while being shared. Lastly, a review of the IP valuation and any related policies must be conducted on a regular basis. This can be done by the governing body or a separate team may be formed.

3.3 Operating Considerations

In this section, we discuss key considerations relating to the management of the Blockchain network itself.

3.3.1 Node Hosting

Members are hosted as logical nodes through which transactions and updates are posted on the Blockchain network. Some of the nodes take up the role of validating the transactions that are getting executed on the network. Additionally, these nodes can be used to query the underlying ledger for information relating to the transactions posted by participants for audit purposes. Different Blockchain platforms have different kinds of node structures:

Permissionless Networks
(e.g. Ethereum) have

Full nodes – Post and verify transactions and maintain consensus in the network

Light Nodes – Post transactions only, while relying on full nodes for verification

Permissioned Networks
(e.g. Corda) have

Notary Nodes – Responsible for confirming transactions on the network

Standard Nodes – Post Transactions while relying on notary nodes for verification

In reality, node structure of Blockchain networks are much more complex, the above is just an oversimplification for ease of understanding and is beyond the scope of the whitepaper.

As discussed in earlier sections, addition of new nodes can only be restricted in a permissioned network, where rules and permissions can be set by the governing members. Hence, the consortium members can decide on how to grow the network and provision for the required level of privacy. Therefore, for ease of understanding, this section is limited to permissioned networks (R3 Corda in particular) only.

Now each logical node has its own enclaved ledger and privacy features, which ensures that data exchange between nodes is permissioned and protected, and that user-specific rules regulate the accessibility of information exchanged between member nodes. The logical nodes can be hosted separately as individual Blockchain nodes, or they can be provisioned as user member accounts within each independent Blockchain node.

Listed below are some of the key considerations regarding node hosting:

- **Who will participate via a node vs a member account?**
- **What kind of permissions (read/write/query) will each node have?**
- **Who would be allowed to post/update smart contracts on the network?**
- **Can an existing member add nodes independently, or would this need to be cleared with the consortium first?**

It is important to understand that owning a separate node is good for maintaining the integrity of the Blockchain network, but it also comes with its own obligations. It might happen that some members may be reluctant to join the network just because they have to own a separate node. An example could be that of a small logistics partner who may lack the capital or infrastructure that may be required to own a separate node; or may have a very limited role and/or upside to be on the network, and therefore is not able to justify such expenditure. In cases such as these, participation of these members can be provisioned via member accounts. As an example, the logistics partner could be added to the network as a member account under the supplier node. With this the logistics partner need not bear the full cost of owning the node.

3.3.2 Data Management

It is important for consortium members to decide on the degree of control they want over the data that is shared by them on the Blockchain network. Keeping data confidential could be:

- **A mandatory requirement, like in the case of PII (Personally identifiable information)**
- **Essential to protect the competitive advantage of a company i.e. protecting critical information such as pricing details or identity of their suppliers and buyers from others on the network**

In this section, we examine two strategies that may be employed to protect such information on the Blockchain network, without diluting its value proposition.

One of the strategies could be to segregate data into two buckets namely 'sensitive' and 'non-sensitive'. Only the non-sensitive data can be put on the Blockchain network. The sensitive data can be kept 'off-chain' and only it's hash can be stored on the network. In case data kept 'off-chain' is manipulated, then its resultant hash would not match with the one on the Blockchain network, thus guaranteeing its authenticity. Keeping data 'off-chain' has other benefits as well:

- **Storing data-heavy files such as documents, photos, videos etc. 'off-chain' would keep the network from being over-burdened, therefore not impacting the throughput**
- **To conform with any regulation that prohibits sharing or retaining user data without or against their consent. For example, in some countries, sensitive data such as PII is required to be deleted once its intended purpose is fulfilled ('Right to be forgotten')**

Another strategy could be to provide role-based access to relevant participants wherein information related to a transaction is visible only to entities privy to that information. This can be easily provisioned in permissioned networks, where access rights to data in a transaction can be coded down to a single field in the transaction. In the case of permissionless networks however, this is not possible. A workaround with Zero Knowledge Proofs may be used to provision privacy, but this solution is still maturing and slows down the network significantly.

3.3.3 Dispute Resolution – Blockchain Network

Disputes may arise between participants on the Blockchain network due to a variety of reasons such as:

- **Incorrect inputs entered/captured on the underlying ledger (e.g. Manual errors)**
- **Defects/Vulnerabilities in the Blockchain code and/or smart contracts that may be exploited by a network participant to cheat the system**
- **Incorrect or inept translation of 'Real-world Contracts' to 'Smart Contracts'**

As an example, consider the case where a certain contractor is supposed to release payments to a designer on 'delivery of work'. Coding this condition in a smart contract can be tricky, since the 'delivery of work' can be challenged based on quality. Disputes may arise if the contractor is not satisfied with the quality of designs delivered and refuses to release payments.

In a consortium setting, there could be two ways in which disputes like the above could be resolved. One could be through the traditional dispute resolution process as discussed in one of the sections above, wherein the appropriate procedures set up by the consortium's governing body would be invoked and a resolution can be reached among concerned parties. Another way however could be to resolve this dispute on the Blockchain network itself, achieved by provisioning a dispute resolution clause in the code or smart contract.

Continuing with the above example, a provision can be made on the code wherein any transacting party, if they wish to do so, may trigger a dispute process on the network which would randomly select a defined number of network participants, who would be notified and tasked with assessing the dispute. Based on their findings, each one could vote in favour of either party and depending on the tally, payment may be held or released to the designer.

3.4 Financial Considerations

Like any other business, success of a consortium is tied to its initial and ongoing funding. It is the duty of the governing body to decide the financial commitment each participant will be expected to make and how these funds would be utilized to achieve the goals of the consortium. Discussed in the following sections are the costs involved in setting up the Blockchain network and how funding may be managed in the consortium.

3.4.1 Expenses

To estimate the amount of funding that would be required, members must identify the different cost elements of building a consortium and the Blockchain network. Below is a breakup of the costs that the investors would incur:

Upfront Costs

Infrastructure – Third-party licensing costs would include Cloud consumption (if deployed on cloud), specialized tools and software, Blockchain platform license fee (only applicable for enterprise versions), etc.

Development – Typical manpower costs related to Blockchain application design, development, deployment, integration, migration, and code audits to assess vulnerabilities in the code (especially in smart contracts). This will also include the costs associated with project management activities.

Administrative – These are costs associated with hiring external consultants for business, technology, tax, and legal support.

Operational Costs (On-going)

Infrastructure – Depending on the Blockchain platform transactional costs may be added, which must be borne by the party posting transactions or submitting new/updated smart contracts onto the network. This will also include the cost associated with owning a separate node.

Maintenance and Support – Manpower costs related to performing maintenance and support activities including future enhancements, integration with new systems and so on.

Administrative – Typical expenses related to day-to-day operations and business administration.

Infrastructure and Development costs would largely depend on the scope, approach, complexity of the use case(s), and the timeframe in which they are to be productized. Whereas Administrative costs would depend on the kind of arrangement consortium members operate in, i.e. through contractual agreements or as a separate legal entity.

3.4.2 Funding

Based on the costs discussed in the previous section, members can now start to build a realistic budget to fund the consortium activities. Funding of the consortium may be divided into two phases:

Initial/Seed Funding **Funding post-commercialization**

Initial/Seed Funding

This phase includes funding required for all activities until the consortium produces a commercial solution. Here, the members must decide on how costs (discussed in the previous section) would be spread among the investors. For example, if the total estimated cost to reach commercialization in 2 years' time is about EUR 1 Million, and there are 5 founding members, then each of them would be committing EUR 200K each.

Two prevalent models commonly seen in consortia are:

Founder-led Consortia

In this model, a founding member or a group of members take onto themselves, the responsibility of establishing the consortium. They fund all or at least most of the activities, associated with setting up the initial infrastructure, governance, etc., and therefore have all the decision-making authority in these matters due to which these consortia are easy to set up but may prove to be difficult to grow.

Co-owned Consortia

As the name suggests, this is a more collaborative approach wherein all members are co-owners and share the costs of setting up the consortium from the very beginning. This also means that decision-making authority is distributed among many members due to which finding common ground becomes a challenge. But when they do find common ground, they are more likely to grow fast due to network effects.

Depending on the funding approach taken up by the consortium, members must set realistic milestones for obtaining, as well as deployment of funds. This would mean clearly outlining in detail, what part of the fund will be allocated to which activity.

Additionally, a contingency plan must be prepared, in case additional funding is required. Now, this could be due to investors pulling out of the consortium pre-maturely or in case if expected goals are not met in the given time. The governing body must be prepared to deal with these kinds of situations well in advance to ensure consortium activities continue uninterrupted.

While deciding on these key issues, the governing body must keep in mind that the decision-making authority and especially the benefits must be reasonably distributed among the members and not be skewed heavily towards some of the participants. This will not only discourage new members from joining but may also result in existing members pulling out, subsequently impeding the consortium's growth in the long term.

The consortium may also consider or switch to, an annual membership model even before a commercialized solution is in place, provided that many organizations are willing to join the ecosystem.

Funding post-commercialization

Once a commercial solution is in place, members should discuss and decide on the best possible way to charge their customers. The following product monetization models could be considered:

- Subscription-based Model
- Transaction-based Model
- Licensing Model

Additionally, since Blockchain enables selective sharing of information i.e. users get to choose how much of their data is exposed to the outside world and the fact that data captured on immutable Blockchain ledgers can be considered authentic, opens up a variety of interesting opportunities for the consortium. Firstly, aggregated user-generated data could be directly monetized in its raw form. Secondly, this data can be used to derive superior insights. These can be further monetized and used internally by consortium members to enhance their own businesses.

3.5 Security

Blockchains by design are robust and secure, but the external components that it interacts with, may induce vulnerabilities in the overall solution. Moreover, each member would have their own IT infrastructure and data security policies. Before they start exchanging data on the network, robust network security features must be implemented so that organizational or regional regulations are not violated. To that end, a 'Security and Architecture Review Group' (S&ARG) should be formed. Each member organization must appoint a representative from their data security team who would work with or be a part of the S&ARG. These representatives would be required to examine member organization's systems and data policy to develop a generic data model for the network. This group will also be responsible for conducting periodic assessment of the network's workflows and data artefacts needed to support them.

Additionally, permissioned Blockchain network must adhere to security standards that permit only permissioned participants to be privy to the data being exchanged. The Blockchain network should allow for implementation of organization-specific data privacy features and information security models. In principle the consortium's security policy must cover the below aspects to ensure security compliance.

3.5.1 Risk Assessment

The first order of business would be to assess the kind of risks that might be bought in due to the deployment and integration of a Blockchain solution in existing systems and processes. Each member organization must prepare an exhaustive list of risks that they think their organization and the consortium might face both initially and as the solution matures. Below are some of the risks that might help kickstart such a discussion:

Business Risks

- Due to addition of new participants/nodes on the network, which are hosted in different geographical regions and therefore may be governed by a different set of regulations.
- Due to inappropriate use of IP assets or data by an internal member or external party.
- Due to an inadequate exit strategy, for when members leave the consortium (willingly or otherwise).
- Due to lack of a sound business continuity/disaster recovery plan in case the Blockchain platform or any of the dependent components (such as cloud) are compromised.

Technology Risks

- Due to inaccurate data/transactions being recorded on Blockchain.
- Due to integration issues between the Blockchain platform and IT systems of different organizations.
- Due to the inability of the Blockchain platform to cater to the scalability needs of the consortium.
- Due to vulnerabilities in the Blockchain solution design which could compromise confidentiality and integrity of data, especially important for use cases, where sensitive information is being captured.
- Due to vulnerabilities in smart contracts which could compromise the network or the enforcement of business contracts.
- Lastly, there might be an aspect of technical debt, i.e. having to refactor code to switch to a different platform altogether. Though this can't be eliminated completely, solutions that are more modular can help lower the impact of such changes.

Once the risks are identified, suitable controls and response plans must be discussed and put in place to eliminate or limit them to a minimum.

3.5.2 Threat Modelling

Threat modeling techniques such as STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service attacks, and Elevation of privilege) or PASTA (Process for Attack Simulation and Threat Analysis) may be used by the S&ARG in order to identify and assess likely security vulnerabilities and threats (e.g. due to improper certificate management). Accordingly, a suitable mitigation and response plan must be developed. Additionally, the S&ARG would be required to assess, as well as track threats and risks regularly, through simulation and live data analysis. The consortium should also consider engaging a third-party security evaluation partner for these tasks.

3.5.3 Data Privacy

Every organization's data policy is structured to protect and safeguard data that is sensitive or critical to its operations. Consortium must clearly define policies that protect such critical information. This would also include strategies to provide appropriate access to a network participant and masking critical information before including it in transactions.

As an example, consider a purchase order raised by a contractor for procuring certain materials from a supplier. The supplier would most likely not want to share the pricing details with its OEM or logistics partners. In this case, the pricing information should be categorized as critical and these details must be masked from the OEM and logistics partners. As discussed in the section titled 'Data Management', members may choose not to store such data on the Blockchain, just storing the hash of this data would be enough.

3.5.4 End-point Security and Key Management

The user accessibility of information on the Blockchain network is governed by the access permissions and user certificates. The S&ARG must define a secured endpoint policy that is in line with the end-point security software selected. Usually, a cloud-based endpoint security software is preferred, as it helps add a security layer over the cloud infrastructure making the platform more robust against security threats.

Furthermore, Blockchain relies heavily on Public Key Infrastructure (PKI) to securely associate cryptographic keys (Private and Public) with a given participant. These keys are used to digitally sign transactions and enable secure exchange of data among participants on the blockchain network. Consortium could consider one of the below key management approaches:

- **Hardware Security Modules (HSM)**
- **Private Key Seeding**
- **Decentralized Public Key Infrastructure (DPKI)**

Given the importance of private keys in a Blockchain network, a mechanism for users to recover these keys must be set up in case they are lost or compromised.

Conclusion

While cryptocurrencies remain susceptible to wild speculation, the underlying technology i.e. Blockchain continues to retain its prominence as a lever in delivering transformative benefits to organizations. Interest in Blockchain has been growing steadily over the years, with many organizations making significant investments in exploring viable use cases. But in order to unlock its true potential, it needs to be supported by a robust ecosystem of participants. Forming a consortium seems to be a logical way to achieve that. To that end, this whitepaper is devised to help organizations navigate through the various intricacies of forming a viable consortium, as they pursue their collective interest and exploit what this ground-breaking technology has to offer.

Building a consortium from the ground up may seem like a daunting task at first, but if done right, can result in significant benefits for its members and the industry as a whole. Organizations must keep in mind that creating this kind of ecosystem is more about collaboration and finding common ground than leveraging the technology itself.

Finally, organizations must be ready to have a long-term vision when approaching consortium building as it would take a lot of deliberation, time and resources before any significant benefits are realized.

Authors

Ravi Raj Singh

Senior Consultant - Blockchain Practice, LTI

Ravi have been working in the capacity of a Senior Consultant with the Digital Transformation group at LTI for over a year and is responsible for driving projects centered around Blockchain Technology across industries. He has a total of 5+ years of experience, having worked as an Associate Consultant with Capgemini India in Banking Domain prior to joining LTI.

Steen Madsen

Enterprise Architect – Solar A/S

Steen has been an IT Professional for more than 30 years, primarily being leading digital transformations within wholesale & distribution. Driving more than 200 successful projects/programs, ranging from huge ERP implementations to innovative leading edge initiatives like introducing E-business late 1980's, global warehouse management setup mid '95, and commercial mobile apps in 2011. Currently holding a position as Enterprise Architect at Solar, with focus on driving business value by information and technology.