



Technical considerations in blockchain consortia

Blockchain consortia are a rapidly growing approach that businesses are turning toward in an effort to better leverage data and information to help them remain competitive and control the cost of information.

In Part I of this series, we discussed how consortia rely on cooperation—an alliance between traditional competitors—to quickly and effectively establish unique marketplace positions by leveraging their complementary strengths to benefit each member in the consortium. Further, we discussed some of the key strategic issues that organizations should consider before joining a consortium, including who its members are, what its mission is, its operating considerations (e.g., its structure, funding, legal considerations, etc.), and how it will be governed to provide value for each participant.

In this article, we dig a little deeper and take a closer look at some of the key technical considerations that should be taken into account when joining a consortium.

Blockchain is a tool, not a magic bullet

It's a situation we see time and again, in all types of companies and in all types of industries. Executives looking to maintain a competitive edge for their organizations latch onto the latest trends in an effort to stay ahead of their competitors, even if they don't fully understand what they are getting themselves—or their organizations—into.

If their peers and the press are all talking about blockchain consortia, they figure they should join one themselves before it's too late, and they're forced to play catch-up. Sometimes, they're right. Sometimes, they're not.

The key thing organizations should keep in mind before jumping into any new venture, such as a consortium, is that technology concerns should complement and support

their work, not define it. In other words, don't join a consortium just because it's blockchain-enabled; join a consortium because its use of blockchain can help it—and your business—achieve the goals you are striving to reach.

Sharing is the key

It is important for organizations to understand that blockchains can share more than data: They can share permissions, proofs, access, and truth. So, while many early builds of blockchain only focused on data, this thinking has evolved—and so should yours.

As previously mentioned, consortia work because they rely on the concept of co-competition to bring traditional competitors together to address a common problem that is affecting their businesses or their industry. They have identified a shared pain point and, by working together, hope to devise a solution that helps them all be more successful.

It is important to note that the exact nature of the shared pain point isn't important. Consortium members could be looking for ways to reduce overhead and operating expenses, address problematic business or regulatory issues, or create new standards that allow everyone to compete on a more level playing field. It really doesn't matter, so long as all the members are working together to solve a common problem.

Oftentimes, the issue the consortium is looking to address has nothing to do with blockchain, but because it is fundamentally a distributed network, consortium members turn toward blockchain-enabled technologies because they facilitate a feeling that everyone in the group is equal. However, this is not always the case.

Organizations cannot expect to enlist the cooperation of the ecosystem into a consortium process without having thought through the incentivization model for adoption. They can't first build a blockchain ecosystem for a consortium and then mandate the formation of a consortium. It is worth noting that a viable blockchain solution generally isn't enough to incentivize

companies to enlist. There are many additional reasons why competitors might be reluctant to join a consortium, such as if they don't see enough upside potential or if they fear that certain members might monopolize the group and derive the most benefit from the initiative.

To address such concerns, there are three hosting structures that are commonly used for blockchain consortia: fully distributed, single-member hosting, and third-party hosting for a private consortium. There are technical considerations based on each hosting structure. In the fully distributed option, each organization operates a copy of the blockchain on their own infrastructure. This distributed ledger processes transactions and remains in sync with all the nodes. The second option is single-entity hosting, where one organization is responsible for the operation and maintenance of the blockchain ecosystem on behalf of all the members. A third option is third-party hosting that may also be composed of a single entity that maintains the ecosystem. The participants in this consortium may be an entity's corporate affiliates or vendors, for example. It is worth noting that cloud solutions can be successfully integrated into the three hosting structures mentioned above.

Of openness and interoperability

Businesses that are considering joining a new or existing consortium need to approach the decision with the mindset of a technology company, even if they don't truly play in that environment. What does that mean, exactly?

When joining a consortium, businesses must consider how their own technology choices will align with those of the consortium and develop an in-depth understanding of how the consortium's strategic objectives align with their own. If there's a mismatch between the business and the consortium's objectives, chances are the relationship may not provide the kind of benefits the business is looking for.

To this end, consortium members must agree on, and adopt, common

communication and data standards so that everyone is working from the same playbook and has a clear understanding of the information being provided and shared among the group. Adopting such "Ubiquitous Language," which originated from Domain-Driven Design, is therefore imperative to successful blockchain consortia.

Similarly, it is important that consortium members agree on how to deliver and receive ecosystem data so that the communication of this data may be done to a single, standardized API (application programming interface). Without clear transaction standardization in place, communication is impossible, which stops the free flow of information between consortium members and removes an individual member's incentive to participate.

Solution architects also must be clear on the process that the consortium is trying to facilitate. Understanding what value is being exchanged on the blockchain and who is involved in these transfers is necessary to determine how workflows and smart contracts are coded. If consortium members cannot articulate what they expect a transaction to accomplish, then regardless of the architect's skill, this can have serious consequences.

Thoughts on the organizational structure

Consortia don't just happen because business competitors decide they should work together to solve shared problems. They take planning and a willingness to dedicate both time and human resources to the effort to help ensure success.

One of the key problems we see with consortia is that organizations often express significant enthusiasm to participate early on in the process, only to pull back when they are called on to provide the resources they promised. Part of this is due to the fact that many organizations fail to understand the full scope of the resources they are required to provide to the consortium.

Because of this, we often see that member organizations do not dedicate enough

Technical considerations in blockchain consortia

staff, or— more importantly—the right staff to these relationships. This can cause delays and hinder key initiatives from being completed in a timely manner, as those staffers working with the consortium may not have the decision-making authority required to allocate resources or the money required.

To combat this, participating businesses need to do more than just pay lip service to the concept of the consortium. They need to involve empowered decision makers in the exercise and come together to make key decisions. This is one reason why blockchain solutions architects and experienced developers with 10 to 15 years of experience in the field are now in such high demand.

The devil is in the details of the technology, and businesses really need to understand those details to implement blockchain properly. Organizations that are unfamiliar with blockchain technology are often scared of it and reluctant to act for fear of doing something “wrong.” That’s why solutions architects, and the people implementing this technology, must be experienced enough to understand those subtleties of implementation.

Organizations that are serious about their participation in a consortium should also consider assigning at least one full-time facilitator to the effort. Empowered to make key decisions on the organization’s behalf, and working in concert with the solutions architect, this person should be tasked with managing the day-to-day concerns surrounding the firm’s participation in the consortium, such as ensuring that meeting minutes and agendas are maintained and overseeing the necessary prep work for meetings and working sessions. It is important to note, however, that key decisions ultimately will be made by the board of the consortium, and facilitators from each participant in the ecosystem should be in place to work with consortium management.

Who owns the data?

Another key consideration that companies must address when joining a consortium revolves around the data and its ownership.

This is often a significant obstacle that consortia must overcome. Blockchains create unique data through the consensus that exists on the blockchain. When forming a blockchain consortium, it must be decided early on who owns this unique data, who has the right to possibly monetize it, and, if monetized, how the proceeds are distributed. It is also important to consider data ownership should new nodes be added to the ecosystem in the future.

To help alleviate some of the worries related to data ownership, companies must decide if ecosystem data needs to be on the blockchain in the first place. In the next evolution of consortium blockchains, the blockchain can act as a proof for data controlled by individual members of the consortium. In the past, many organizations designed blockchains as the endpoint or repository of data. This is not the most effective use of the technology. When integrated properly, data doesn’t necessarily need to go on-chain but can remain in off-chain repositories. The chain can then facilitate access to these repositories and data to provide proofs that they “are what they are supposed to be.”

Take on the hard work up front

Once you know that you’re going to participate in a consortium, don’t hesitate to bring your company’s lawyers and your solutions architects into the conversation. Why? Because hammering out all of the minute details surrounding data, ownership, and IP take time and effort, and addressing these key points as early as possible will help to streamline the consortium’s decision-making process later.

By addressing and resolving potential sticking points early on, potential consortium members should have a better understanding of their roles, responsibilities, and rewards for participation before they invest financial and human capital into the project. In short, getting the lawyers involved early will help to increase transparency and to prevent larger disagreements around issues like data sharing and IP from arising in the future.

Blockchain solutions architects/experienced blockchain developers hard skills:

Front end

- JavaScript (Angular, React, Meteor)
- Web3
- Python (Django, Flask)
- CSS and Modules

Back end

- NodeJS, Python (API server development), Java, Kotlin
- Database and interface experience (MongoDB, GraphQL)
- OpenSSL
- Docker
- Kubernetes
- Blockchain
 - Private Ethereum, Quorum, Corda, Hyperledger Fabric for blockchain platforms, etc.
 - Solidity (Ethereum’s smart contract language)
 - Understanding event-driven development
 - Truffle (Smart contract deployment process)
 - Geth, Parity
 - Puppeth
 - Distributed systems
 - Familiarity w/ InterPlanetary File System (IPFS)
 - Familiarity w/ permissioned functions (visibility & execution modifiers)
 - Familiarity w/ basic cryptography (fundamentals of hashing)

Conclusion

Consortia succeed and fail for a variety of reasons. Most often, however, problems arise because participants do not feel like they are being treated equally or receiving equal returns on their investments into the group. This often occurs when consortium members fail to agree upon important decisions early in the process.

We have seen time and again that consortia that provide unilateral benefits to one or two key members don't work, except in rare and exceptional cases where the primary members are so large and powerful that other participants have no choice but to follow their lead. In general, however, consortium members want to play an active part and want their points of view to be incorporated into the consortium's decisions.

As such, it is critically important that members—and potential members—develop a deep and thorough understanding of the consortium's ground rules, technologies, operating standards, and overall objective before they agree to participate. By putting in the necessary groundwork early in the process, participants can help to ensure that they are operating on a level footing with other members and are receiving all of the benefits they are entitled to from the consortium.

It is vital that organizations understand that blockchain is a technology with a particularly steep learning curve, especially when it comes to proper design and integration. Unfortunately, businesses often will attempt to force a blockchain solution without having the proper resources to do so. Even with a seasoned development department and IT staff, without a blockchain specialist, a blockchain build is likely to fail.

Organizations should expect a degree of disruption when it comes to blockchain consortia. The technology can affect not just technology in general, but also a company's culture, HR, revenue models, and other vital moving parts of the organization.

Of course, there are other considerations to ponder before joining a blockchain consortium, and in our next paper, we will take a more detailed look at the various issues of governance that members should address as part of their participation.

Acknowledgments:

Authors

Peder Mueller

Specialist Leader
Deloitte & Touche LLP
pemuel@deloitte.com

Sanjiv Maewall

Specialist Leader
Deloitte Consulting LLP
smaewall@deloitte.com

Antonio Senatore

Director
Deloitte Ireland
asenatore@deloitte.ie

Dr. Paul Sin

Partner
Deloitte Consulting, China
psin@deloitte.com.hk

Kenny Brown

Senior Manager
Deloitte Consulting LLP
kebrown@deloitte.com

Contributors

Jonathan Holdowsky (Deloitte Services LP),
Linda Pawczuk (Deloitte Consulting LLP),
Mike Prokop (Deloitte & Touche LLP),
Lisa Simpson (Deloitte Consulting LLP)

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.