Secure Blockchain Considerations for the Enterprise: Infrastructure, Blockchain Middleware, and Consensus

Published on September 22, 2016

Nitin Gaur
Director at IBM Blockchain Labs

Tech Talk

Secure Blockchain Considerations for the Enterprise:

Infrastructure, Blockchain Middleware, and Consensus

In this post, I bring a technical focus on security considerations for enterprise blockchain applications and business networks. I also seek to introduce an approach developing the doctrine of layered defense, which has been employed as a practice of combining multiple mitigating security controls to protect resources (digital assets/smart contracts in a blockchain context) and data (ledger data in a blockchain context).

The promise of blockchain stems from the vision of an Internet of Value or, in some cases, Internet of Transactions, with a foundation in the systemic, secure exchange of data leading to the trading and transference of value through smart contracts, such as business intermediaries. These foundational elements lend themselves to the rails that enable a secure movement of things of value with non-repudiation—or, at least, that is the intent.

In my previous discussion of blockchain and value networks, I emphasized the importance of a trust system in blockchain that aims to disintermediate the trust intermediaries and enables information symmetry for business network participants. This level of disintermediation relies on the provision of a computing framework to ensure the backing of computer power and proven algorithms that provide a robust trust system, thereby replacing the trust intermediaries.

Enterprises meaningfully realize the promise of blockchain, which is either

a. **Transformational cost models** – IT costs: redundant and duplicative systems and/or opportunity costs, including capital and liquidity costs from inefficient market operations due to asymmetric information flows;

or

b. **Disruptive costs models** – New business models, such a P2P value exchange platforms and crowd sourced models.

The adoption of blockchain is a balancing act for an enterprise, as it not only has to run, manage, and maintain its existing infrastructure but also pave the way to this new computational model that promises to fundamentally change enterprises and even whole industries. For regulated industries, this means a dual impact on the cost of compliance, because even a new technology platform has to adhere to well understood regulatory frameworks and proven technology architecture and design that pass the regulatory mustard test. Building upon the layered approach and sourcing from many design sessions, I'd like to transition to **secure blockchain considerations for the enterprise**, which essentially targets

a. Infrastructure

b. **Blockchain middleware**

c. **Trust systems (i.e., consensus)**

Three Layered Approach to security considerations for enterprise blockchain applications and business networks

I. **Physical: IT Infrastructure layer**

This layers addresses the fundamental IT infrastructure security elements, such as a network and instances, HW isolation, hardware security modules (HSMs) for key management and secure storage, and Crypto accelerators for offloading crypto processes. The idea is to address not only the basic building blocks and foundational elements of security to provide support for higher layers protocols and also to ensure that we are addressing the scalability requirements of a blockchain network, which is an important consideration for blockchain applications, networks, and distributed applications.

Other Infrastructure scalability Considerations

1) **Blockchain – Consensus, ACID property and CAP**

When NoSQL and distributed data-driven models became the norm, various models in which an NoSQL system solved their particular problem by understanding this CAP theorem together with the RDBMS enterprise community held steadfast to their ACID properties. There are several reasons why Blockchain could very well enable primitives to break CAP and maintain ACID. Here are some considerations:

CAP

C- Consistency: Consensus guarantees that there is only one truth of what happened and the order in which it happened;

A- Availability: The fact that all calls to the blockchain are asynchronous allows the "invoking" application to make progress while the consensus and durability (chaining also guarantees this) are getting done;

P- Network partition: Consensus again keeps us from getting a split brain with conflicts when things get back together after a network partition.

ACID Properties of a Transaction

A- Atomicity: The chain-code programming model is an all/nothing behavior, which allows one to group activity together; it either all happens, or it doesn't;

C- Consistency: Significant consideration in DAPP – Distributed application and in many cases the choice of consensus is geared towards achieving ledger consistency, and this means the same as the "C" in CAP;

I- Isolation: This means that two transactions are serialized, which is exactly what the block construction and chaining do;

D- Durability: The chaining and replication all over the network make sure that if one or more nodes go down that we don't lose the data; this is why everyone wants to bring a node, and it is also why we want to make sure that not all those nodes are not co-located.

2) **Attestation – Self-Signed Certificates – SSCs are signed and encrypted.**

The software, operating system, hypervisors, and docker container images in SSCs cannot be modified. Certificates can be included within the SSC so that it can probe itself to be genuine to a remote a party. For example, we can include an SSL certificate when we build SSCs so that later, one can be sure that we are speaking with a genuine instance, since the SSL certificate will always stay protected (encrypted) within the SSC.

3) **Use of HSMs**

An HSM is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. Wikipedia: "A Hardware Security Module Administering a high-

security device like an HSM is difficult to do with adequate security and controls. In fact, standards today mandate certain methods and levels of security for the HSM administrative (and key management) systems."

II. **Blockchain Middleware Laye**r – This layer includes considerations around ledger data and storage, symmetric cipher algorithm, key length, public key algorithms, choice of ledger storage and replication, crypto modules, level of encryption, encryption on data storage, transfer and data at rest, and visibility of data between network participants (see sub ledgers, below). These layers also include choice of blockchain fabric, infrastructure and supported pluggable modules, and all aspects of enterprise integration.

Note on Multichannel / Sub Ledgers – a Hyperledger design concept

The original theory behind multichannel and sub ledgers was to provide a level of isolation to chains/networks for consensus as a service. The separation would be accomplished by using different channels writing to the single common ledgers (at the time of the original idea, there was only one ledger available).

III. **Blockchain Consensus (i.e., trust system layer)** – I have always believed this to be the heart of blockchain. Consensus in the blockchain is required to guarantee very basic "data store" properties. The more players there are in the network, so we will only scale up if they bring capital or compute equity. This is about building a "shared data store" that has enterprise data qualities that they get from their internal, walled-off, enterprise—with a lower barrier to entry. Consensus, even minimal consensus, is required to guarantee this on the architecture in place.

A divide has emerged between crypto currency-based and non-crypto currency-based trust systems. Basically, permissioned ledger crypto currency-based trust systems, such as POW/PoS, drive a model that is unsustainable for enterprise use cases aspiring to create a permissioned blockchain. This is a topic in its own right for a dedicated post/paper.

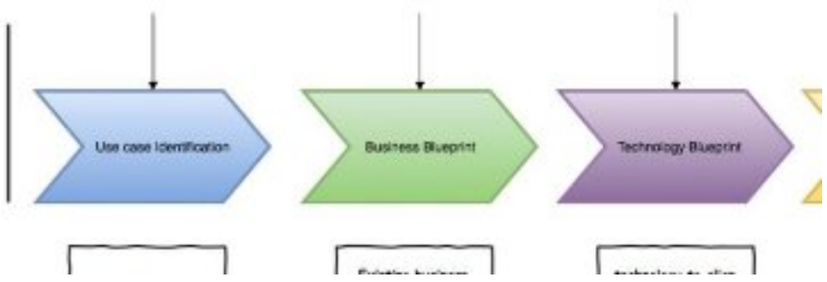
In one of my previous posts, I discussed the blockchain tenets for a permissioned ledger/network sought by regulated industries, the rules of engagement change, and the radicalized trust currency needs to be morphed into a viable trust system—which one can choose to ignore or adopt as a foundation of parts of an incentive economics based on the trust system of consensus models. As discussed earlier, much work needs to be done in this field, as there is not a single consensus model that will address all use cases (there is Byzantine Fault Tolerant [BFT], PoW, PoS or Practical Byzantine Fault Tolerant [pBFT], RAFT, Paxos, etc.). An enterprise needs to understand these. They will also drive investment into the underlying resources (people, power, and time).

Conclusion

The adoption of blockchain will be a balancing act for an enterprise, as it will not only have to run, manage ,and maintain its existing infrastructure but also pay the way to this new computational model that promises to fundamentally change enterprises and even whole industries. For regulated industries this means a dual impact on the cost of compliance, because even a new technology platform has to adhere to well understood regulatory frameworks and proven technology architecture and design that pass the regulatory mustard test. Enterprises can take a pragmatic approach to **secure blockchain considerations for the enterprise** by adopting the doctrine of layered defense, which involves combining multiple mitigating security controls to protect resources (digital assets/smart contracts in blockchain context) and data (ledger data in blockchain context).

Nitin Gaur
Director at IBM Blockchain Labs
19 posts

Don't miss more posts by Nitin Gaur

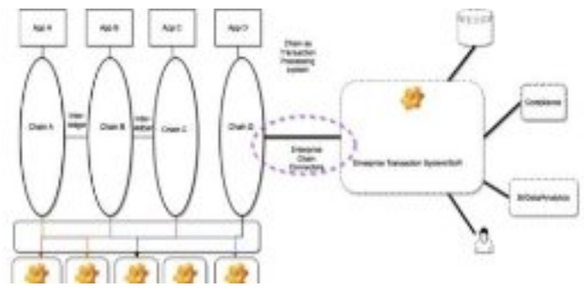


Path to blockchain enterprise adoption: A prescriptive approach

Nitin Gaur on LinkedIn

Blockchain for Enterprise – Focus on KYC, AML, and Regulatory…

Nitin Gaur on LinkedIn



Blockchain for enterprise? Not so fast!

Nitin Gaur on LinkedIn

Looking for more of the latest headlines on LinkedIn?

Discover more stories