Featured

Guidelines for blockchain adoption in the How to compare frameworks

Nitin Gaur
Created on May 11, 2017

0

In any enterprise, the driving principles are the business blueprint, the technology blueprint, and integration in t
walk through the essential considerations for choosing a blockchain framework according to these principles. A
handy worksheet to help you size your adoption effort based on these considerations.

Business blueprint

Blockchain's promise is to create a business network of value that is based on trust. And in order to reinvent a
system, it's important to understand how different blockchain frameworks address network interaction patterns
vulnerabilities.

Technology blueprint

For technology to align with business imperatives, you need to make the right technology and architecture cho
as TPS (transactions per second), enterprise integration, external system integration, and regulatory and comp
these decisions are the technical due diligence needed to budget properly for an enterprise blockchain project

Enterprise integration

Enterprise integration, especially with an adjacent system, is an important consideration and cost point. It's a b
as a technology consideration, because downstream transaction systems affect critical business systems. In m
system integration has a significant cost impact on blockchain projects, and if not focused on early in the plann
enterprise adoption.

Business considerations for choosing a blockchain fram

1. **Open platform and open governance**:
   The choice of technology standards paves the way for enterprise adoption, compliance, governance, and th
2. **Economic viability of the solution**:
   The focus is on cost alignment to business models, charge backs, compute equity, and account manageme
   by the advent of crypto-economics due to game theory constraints and accounting of such. This flows into
3. **Longevity of the solution**:
   As we aspire to build a trusted network, we need to ensure that the cost and operation are sustainable so th
   scale to accommodate additional participants and resulting transactions.
4. **Regulatory compliance**:
   This includes events like industry-specific reporting, analysis, and costs of compliance –- in terms of busines
   automated and human-centric. These tasks are tightly linked with transaction processing in a business netw
5. **Coexistence with adjacent systems**:
   This refers to the impact of the blockchain network on the enterprise and on the participants of the business
   to the existing system, which may have overlapping and complementary functions.
6. **Predictable costs of business growth**:
   Business growth relies on predictable metrics. Historically, industry has focused on transaction per second,
   transaction per second differs from system to system based on system design, compute costs, and busines
7. **Access to skills and talent**:

Access to skills and talent affects costs and also the maintenance and longevity of the solution with respect innovation.

8. **Financial viability of technology vendors**:
   This is an important consideration when it comes to long-term support and solution longevity. Vendor/busin be based on their long-term vision and the sustainability of their business model.
9. **Global footprint and support**:
   Blockchain applications and solutions are about business networks with global footprints, and the associate the expansion of the business network with the least disruptive adoption path.
10. **Reliance on technology and industry-specific standards**:
    Standards play an important role not only in standardizing a common technology stack and deployment but communication platform between industry experts and technologists to solve important industry problems a Standards also lead to low-cost technology that can be rapidly consumed with widely available skills.

Blockchain vendors offer different specializations, including:

- Variant trust systems: Consensus, Mining, proof of Work, etc.
- Lock in to a single trust system
- Purpose-built infrastructure components for a specialized use case
- Design that is field-tested via proof-of-concepts

The risk is a fragmented blockchain model for the enterprise.

Conversely, the open-standards based approach, commercialized by IBM, is different in these ways:

- Open design
- Flexibility with a pluggable and modular trust system
- Open for specialized blockchains, such as Ripple
- Trust intermediary, which is a trust-system provisioning layer
- Enterprise blockchain concept
- Separate business domain with technology that supports it

Technology considerations for choosing a blockchain fr

> *Start with the premise that this is NOT ANOTHER APPLICATION you're choosing. This*
> *NETWORK with risks and costs to ensure upkeep and maintenance that cannot use e*
> *development, infrastructure, and common services.*

1. Identity management

This is an involved and complex topic, especially in regulated industries where identities NOT ONLY need to be
business consequences around activities such as Know Your Customer (KYC), Anti-Money Laundering (AML),
analytics functions.

1. **Permissioning** is the notion of eCerts (member enrollment certificates) and tCerts (transaction certificates fo
   allow for an entity to be permissioned and be identified as transactions are complete.
2. **End use identity** is the mapping of the LDAP/User registry to the tCerts or transaction ID for the sake of tra
   as well as Know Your Customer's Customer), but this mapping is maintained by the participating entity in th

Other identity management considerations include:

- LDAP or existing user registry will not go away and must be considered as a design point, since Authenticat
  systems are mature with significant investment as well as enterprise security policies.
- Blockchain trust systems are the heart of the technology and need to provide an avenue to induce trust with
  cases that require the transactional traceability).
- Identity on blockchain
- Identity for blockchain
- Identity acquisition, vetting, and lifecycle
- Alignment with trust systems based on use cases

2. Scalability

Scalability is both a business consideration and a technology consideration, due to downstream transaction sy
business systems. Technology choices for scalability, such as database choices for the shared ledger, adjacent
encryption, and consensus, lead to system design that can accommodate the predictable costs of the growth
and/or the growth in transactions.

3. Enterprise security

Enterprise security includes three layers to consider:

1. The **physical IT infrastructure layer** includes use case-specific considerations such as the requirements o infrastructure isolation.
2. The **blockchain middleware layer** includes considerations around crypto modules, the level of encryption, transfer and data at rest, and visibility of data between network participants.
3. The **blockchain consensus (trust system layer)** is the heart of blockchain technology.Consensus in the bl guarantee very basic “data store” properties. When more players are in the network, they must bring capital building a “shared data store” that has enterprise data qualities from the internal, walled-off enterprise, at a l Consensus, even minimal consensus, is required to guarantee this on the architecture in place.A divide betw trust systems and non-cryptocurrency-based trust systems has emerged. The model based on cryptocurre such as POW/PoS, is unsustainable for enterprise use cases that aspire to create permissioned blockchains

4. Development tooling

Development tooling considerations include:

1. Integrated Development Environment
2. Business modeling
3. Model-driven development

5. Crypto-economic models

This term roughly means a decentralized system that uses public key cryptography for authentication and econ that it keeps going and doesn’t go back in time or incur any other alterations. To fully understand the blockchai cryptography in computer science, we need to first understand the concept of “decentralized consensus,” a ke computing revolution.

6. Tenets of decentralization with systemic governance

Decentralized consensus breaks the old paradigm of centralized consensus, in other words, when one central
transaction validity. A decentralized scheme transfers authority and trust to a decentralized network and enable
and sequentially record their transactions on a public “block,” creating a unique “chain” — the blockchain. Cryp
used to secure the authentication of the transaction source and removes the need for a central intermediary. Th
cryptography and blockchain technology together ensures there is never a duplicate recording of the same tran

> *Blockchain system design should embody this concept to be adapted and preserved*
> *network while centralizing some aspect of regulatory compliance and maintenance ac*
> *preserving the decentralized digital transaction processing.*

7. Robust and secure blockchain infrastructure

Considerations for a robust and secure blockchain infrastructure include:

1. Global presence
2. Industry acceptable certification

Enterprise support

Enterprise support is an important component for the same reasons as the reconsideration of estimation effort.
premise that this is NOT ANOTHER APPLICATION you’re choosing. This is a production NETWORK with risks
and maintenance that cannot use existing applications for development, infrastructure, and common services.

Use case-driven pluggability choices

Considerations for use case-driven pluggability choices include:

1.
    1. **Shared ledger technology** leads to a choice of shared ledger and database technologies driven by the

imperatives of the business network and problem domain being addressed.

2. **Consensus**

> *Consensus is heart of blockchain technology as it not only dictates the trust syst*
> *technology investment in blockchain application infrastructure. Also, no one cons*
> *cases. Use cases define the interaction between participants and will suggest a*
> *system via consensus models.*

Consensus is a method for validating the order of network requests, or transactions (deploy and invoke),
The correct ordering of transactions is critical, because many types of network transactions have a depe
transactions (account debits often have a dependency on prior credits, for example).

On a blockchain network, there is no single authority that determines the transaction order; instead, each
has an equal say in establishing the order, by implementing the network consensus protocol. Consensus
quorum of nodes agree on the order in which transactions are appended to the shared ledger. By resolvi
proposed transaction order, consensus guarantees that all network nodes are operating on an identical b
consensus guarantees the integrity and consistency of blockchain network transactions.

Broadly, all consensus algorithms are grouped into one of the three classifications:

- No-Master – PoW
- Multi-Master – PBFT/BFT
- Single-Master – HA manager/RAFT

1.
1. **Crypto algorithms and encryption technology**:The choices in blockchain system design include the c
encryption technology. Use case requirements will dictate this choice and drive the technology investmen
infrastructure.

- Asymmetric: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, KCDSA, Elliptic Curve Cryptograph
with named, user-defined, and Brainpool curves

- Symmetric: AES, RC2, RC4, RC5, CAST, DES, Triple DES, ARIA, SEED
- Hash/Message Digest/HMAC: SHA-1, SHA-2 (224-512), SSL3-MD5-MAC, SSL3-SHA-1-MAC, SM3
- Random Number Generation: FIPS 140-2 approved DRBG (SP 800-90 CTR mode)

1. **Use case-driven pluggable choices**:Use cases define the interaction between participants and will sugges system via consensus models.

Other considerations

1. Consensus, ACID property, and CAP

The consensus model will never go to 0, and here is why. When NoSQL became the norm, various NoSQL sys by understanding this CAP theorem, and the RDBMS enterprise community held steadfast to their ACID prope well provide the 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 and durability (chaining also guarantees this).
- **P – Network partition**

  Consensus again prevents split brain with conflicts when things get back together after a network partition.

ACID

- - **A – Atomicity**

    The chaincode programming model is an all-or-nothing behavior, which allows you to group activity toge doesn’t.

- **C – Consistency**

  I think the new world of NoSQL fudges this one. I believe that 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 chainin

- **D – Durability**

  The chaining and replication all over the network make sure that if one or more nodes go down, you don everyone wants to bring a node. It’s also why all those nodes should not be not co-located.

2. Attestation – SSCs are signed and encrypted

The software, operating system, hypervisors, and docker container images in secure service containers (SSCs) Certificates can be included within the SSC so that it can probe itself to be genuine to a remote a party. For exa certificate when building SSCs helps us be sure that we are speaking with a genuine instance since the SSL ce protected (encrypted) within the SSC.

3. Use of HSMs

> *According to Wikipedia, a hardware security module (HSM) is a physical computing d and manages digital keys for strong authentication and provides cryptoprocessing. Th traditionally come in the form of a plug-in card or an external device that attaches dire network server.*

Administering a high-security device like an HSM is difficult to do with adequate security and controls. In fact, s certain methods and levels of security for the HSM administrative (and key management) systems.

Sample of work estimation

> *Remember the fundamental premise that this is NOT ANOTHER APPLICATION you're*
> *production NETWORK with risks and costs to ensure upkeep and maintenance that c*
> *applications for development, infrastructure, and common services.*

Front end components: Java, Tomcat

Web front end

Mobile front end

Middleware that integrates with existing enterprise information systems

Databases design:

Database design and admin skills

API management design:

API design and component design

API management design

API development

Admin

Enterprise connectivity:

Enterprise security

Enterprise integration

Enterprise API integration and management

Key management:

Key management design

Key management implementation and admin

Identity management design and development:

ID management design

ID federation strategy

ID management – integration and implementation

ID audit and operations

Content Management System (CMS) design and development:

CMS design and strategy

CMS implementation and development

CMS installation/management and administration

CMS audit and operations

Blockchain framework migration

Current and future design

Chaincode development and implementation

Chaincode design and development

Chaincode test and deployment

Infrastructure:

System architecture and design

System (and component) provisioning

DevOps strategy and design

HSBN (V1) design and provisioning

Cloud services (Bluemix and other components) – provisioning and admin

Operation and monitoring:

Operation Center – design and admin

Change management strategy

Monitoring – Infrastructure and application components

Network operations – HSBN and Cloud components

Performance and SLA management:

Performance design and strategy

SLA design and Strategy

Performance management and tuning

Network monitoring and tuning

Security:

Overall security design

Network security design and implementation

Blockchain infrastructure security design and implementation

Blockchain middleware security design and implementation

Front end application security design and implementation

Security testing – design and implementation

Security auditing – key metrics and test (application and penetration testing, etc.)

Additional services:

Business analysis and design

Technical architect

Project management

Project execution

Risk analyst

Project documentation (business and technology requirements and decisions)

Learn more

- Start building with IBM Blockchain on Bluemix. Your Bluemix trial is free for 30 days.
- IBM Blockchain 101: Quick-start guide for developers

Read more by Nitin Gaur

- 7 principles for designing a blockchain network to power and sustain your business
- Blockchain for enterprise? Not so fast!
- Blockchain for Enterprise – Focus on KYC, AML, and Regulatory Compliance – Are we Calling it RegTech
- Path to blockchain enterprise adoption: A prescriptive approach
- Secure Blockchain Considerations for the Enterprise: Infrastructure, Blockchain Middleware, and Consen

---

Share this:

Related

7 principles for designing a blockchain network to power and sustain your business
January 1, 2017
In "Featured"

The Force Awakens
December 15, 2015
In "Featured"

Lessons from one y
gang!
October 3, 2016
In "Featured"

TAGS BLOCKCHAIN ADOPTION, BLOG

Join The Discussion

Your email address will not be published. Required fields are marked *

Enter your comments...

Name *

Email *

Website

Notify me of follow-up comments by email.

Notify me of new posts by email.