A Strategic Framework Checklist
For Evaluating Blockchain Solutions

October 2016
Agenda

- Overview
- Business Concerns
- Legal Concerns
- Risk / Regulatory Concerns
- Technical Concerns
- Mercator’s Key Findings
- The Strategic Framework Matrix
- The Product Evaluations
  - Evernym
  - Guardtime
  - Ripple
CO-OP Financial Services (CO-OP) and The Members Group (TMG) commissioned Mercator Advisory Group to develop a decision framework to be used to evaluate Blockchain/Distributed Ledger use cases.

The framework is designed to assist in the understanding of how well each use case aligns with a Blockchain implementation and specifically identify areas where misalignment is most frequently discovered.

Three specific blockchain product offerings were evaluated:

1. Evernym, a Self-Sovereign Identity solution that enables users to collect personal information from multiple sources and then share the collected information or simply validate the truth contained in that information to a requester.

2. Guardtime, a product of KSI, claims to utilize a blockchain but research suggests the claim is exaggerated. Guardtime uses an immutable ledger to verify the integrity of system files, applications, and databases but does not operate across multiple nodes in a blockchain configuration.

3. Ripple, a solution from Ripple Labs which uses blockchain technology to settle cross-currency payments efficiently by directly connecting banks
The Strategic Framework for Evaluating Blockchain Solutions consists of 63 individual questions across five strategic areas. Every solution under consideration should be evaluated across all of these, but Mercator discovered that just a few strategic questions were those that suppliers had the most difficulty answering.

Those issues are paraphrased in the slides that follow in these four general categories:
1. Business Concerns
2. Legal Concerns
3. Risk / Regulatory Concerns
4. Technical Concerns
Key Business Issues to Consider:

Business Concerns

1) A single contract that is binding to all participants lowers cost and effort, but if the Ledger does not incorporate required data, bilateral arrangements are required.

2) How does the contract and technology enable new data to be added to the ledger or new functions added to the software?
   - Software updates are challenging to implement and typically can’t be mandated.
   - Technologically, even mandated, can’t be forced across all operating nodes today.
   - Is it acceptable that changes to ledger and transactions takes months to deploy?

3) Does the implementation share data inappropriately, enabling others besides regulators to determine your partners, customers, transaction volume and transaction details?

4) Is your business protected from errors or outages that result due to systemic failure?

5) Is the company’s revenue model sustainable and will it support all business operations?

6) Is settlement finality clear and does solution eliminate two sets of accounting books and reconciliation between ledger and internal books?
Key Legal Concerns:

**Legal Concerns**

1) Does the operating company have legal standing to deliver binding contracts across all participants and users, including consumers if involved?

2) How does the solution address data residency and confidentiality issues if ledger is distributed across multiple legal boundaries?

3) Are participants operating in a well defined legal structure?
   a) Who is responsible if incorrect data results in negative actions to you or your customers?

4) Are controls in place to assure distributed partners consistently meet all legal hurdles?

5) If involved, are consumer T&Cs capable of being clearly articulated in the distributed ledger environment and various potential consumer claims vetted.

6) Is the institutions legal position clear in case of systemic failure?
Key Regulatory Issues to Consider:

Risk / Regulatory Concerns

1) Is solution compliant to OFAC and other funding restrictions?
2) Is colocation of data in the ledger permissible?
3) Is pseudo-anonymity of participants acceptable?
4) Are appropriate tools in place to enable regulatory supervision?
5) Are data residency requirements met despite data distributed across geographies?
6) Will legal entity deploying and managing infrastructure meet 3\textsuperscript{rd} party management requirements?
7) Is institution unaffected if there are significant delays in transactions?
8) If customer data or interaction is involved, is solution compliant, including UDAAP?
9) What is the institutions responsibility If ledger data, or meta data, is misused?
Key Regulatory Issues to Consider:

Technical Concerns

1) Will solution deliver performance required despite increased volume, DoS attack, or major geographic disaster or brownout?
   a) How seriously is transaction finality time jeopardized by above?
2) Is trust algorithm sufficiently capable of preventing collusion?
3) In what countries will trust algorithm be run and by whom?
4) Are data access permissions sufficiently granular to support the intended task?
   a) Will permissions need to be changed frequently and what is impact on solution?
5) Are keys properly managed and protected and by whom?
6) Does design enable crypto module to be replaced in 20 to 30 years for all data in ledger?
7) Can the ledger replace existing transaction logs or must reconciliation be performed?
8) What data will be distributed across geographic boundaries?
Mercator Key Findings

Blockchains deliver a unique set of new features, but these features also introduce technical limitations that cause new risk and legal concerns. Blockchain developers are rushing to solve these technical limitations but are slowly discovering that mitigation should be done for each specific solution. Most blockchain solutions today have followed the technical design process shown on the right hand side of the figure below instead of the Fast Path delivery model diagrammed on the left.

This is critical because modifying a deployed blockchain is much more difficult than modifying any other software solution.
The Strategic Framework Matrix

Mercator Advisory Group created a matrix with the key attributes needed to align an application with the functions delivered by blockchains, as well as attributes that indicate a misalignment with blockchain’s functions or associated with deployment. The matrix evaluated five areas:

1. **Adherence to Blockchain Conceptual Framework**
   7 attributes measured

2. **Transactional Data Elements Utilized**
   14 attributes measured

3. **Data Access Privileges and Data Availability Utilized**
   17 attributes measured

4. **Regulatory & Risk**
   19 attributes measured

5. **Settlement**
   5 attributes measured
5 Key Attribute Areas to Evaluate  (slide 1 of 3)

1. **Adherence to Blockchain Conceptual Framework**
   Blockchain implements an immutable ledger that maintains a shared view of time-ordered transactions across multiple independently operated nodes managed by some coordinating entity.
   
   • If these capabilities are not required, then perhaps other technologies will prove more appropriate for deployment.

2. **Transactional Data Elements Utilized**
   The blockchain ledger structure has limited flexibility compared to other data distribution technologies such as cloud computing and traditional distributed databases. This area evaluates the applications needs for complex data structures that are not easily implemented with existing blockchain technologies.
   
   • If the use case requires sophisticated transactional capabilities, then other technologies may prove more appropriate for deployment.

*continued*
3. Data Access Privileges and Data Availability Utilized
Blockchains implement privacy and immutability utilizing public/private key pairs and a trust algorithm (proof of work, or PoW, proof of stake or PoS, etc.) that time orders transactions and propagates that order to all nodes. This approach makes complex data access controls difficult, if not impossible, to implement. Also, transaction availability across the network may be difficult or impossible to predict.

- If the use case requires rapid sharing of data or complex controls over which entities have read or write access to the transactions or atomic elements of the transaction, then other technologies may prove more appropriate for deployment.

4. Regulatory & Risk
Blockchains are deployed across multiple nodes, and the trust algorithm and the data contained in the ledger may be made available to any entity interested in executing a node, in any geography. That entity may be a participant or nonparticipant in the ledger use case, and the entity may or may not receive compensation.

- The structure controlling how the proof-of-work algorithm is deployed will have a major impact on how regulatory agencies perceive risk and compliance to existing regulations.
5 Key Areas to Evaluate (slide 2 of 3)

5. Settlement Requirements

Blockchains utilize a trust algorithm that requires time to propagate the shared perspective on transaction acceptance and ordering. If the blockchain includes its own currency, or is linked to an external form of compensation, it is likely that finality will take time to be achieved. When the currency is not native to the blockchain, external exchanges will be required to settle between participants of a finalized transaction. Exchanges fall outside of the trust algorithm and have been proven to represent significant risk.

• Understanding systemic risk and transactional risk associated with the settlement mechanism is critical.
Questions:
Adherence to Blockchain Conceptual Framework

1. Does implementation adhere to Blockchain Conceptual Framework?
2. Is distributed data critical to this use case?
3. Is operation of nodes in an untrusted environment critical to this use case?
4. Is immutability of data critical to this use case?
5. Is private key control of entire transaction appropriate to this use case?
6. Is management of the software appropriate to the use case?
7. Will all nodes operate in the same geography operating under the same regulatory construct?
Questions:
Transactional Data Elements Utilized

1. Yes indicates there is no requirement for record locking.
2. Yes indicates no field-based data access controls and privileges are needed.
3. Yes indicates no record-based data access controls and privileges are needed.
4. Are permissions to data static?
5. Yes indicates that no extremely large record size is required.
6. Yes indicates that all participants share a common field structure.
7. Yes indicates that field level secrecy is not required.
8. Yes indicates that only record / transaction level secrecy is needed.
9. Yes indicates that no revocation of a record is required.
10. Yes indicates assets are created by algorithm and not externally generated.
11. Yes indicates records inter-related and that slow write speeds to the ledger is acceptable.
12. Is average and peak frequency of data element additions low?
13. Is average and peak frequency of data element changes low?
14. Yes indicates there are no data retention requirements that require deletion of data.
Questions: Data Access Privileges and Data Availability Utilized

1. Are there a limited number of actors?
2. Are there a limited number of roles?
3. Are there a limited number of access dependencies?
4. Yes indicates that latency on local nodes is irrelevant.
5. Yes indicates that latency on remote nodes is irrelevant.
6. Will complex data sharing be minimized?
7. Will shared data not require licensing arrangements?
8. Will private keys be held by individuals?
9. Yes indicates Private key does not need to be shared.
10. Yes indicates Private key does not need to be shared across multiple organizations.
11. May data ownership be visible to participants?
12. Are all access controls maintained internally to the blockchain?
13. Is it acceptable if participant transaction volume is disclosed?
14. Does a mechanism exist to re-encrypt data in 20 years?
15. Is risk acceptable if private key is lost or stolen?
16. Yes indicates that reports will not be generated from the ledger data.
17. Yes indicates there will not be a high frequency of access privilege changes.
Questions:
Regulatory, Data Ownership, and Residency Requirements

1. Are there likely to be any encumbrances on the data elements?
2. Yes indicates there is no need to assign liability for error or failure.
3. Are OFAC funding restrictions avoided?
4. Is pseudo-anonymity sufficient?
5. Is data residency addressed for each data element?
6. Will bank be indemnified for information misuse?
7. Will bank be indemnified for inaccurate data?
8. Will bank be indemnified for information loss?
9. Will consumer services delivered meet UDAAP?
10. Are participants operating in a defined legal structure?
11. Is solution auditable per regulatory entity responsible?
12. Is solution auditable per CFPB (full recounting of all entity interactions)?
13. Will software update and management meet third-party risk management requirements?
14. Will operational entity pass OCC third-party risk evaluation?
15. Is collocation of data acceptable?
16. Yes means that implementation does not utilize miners for proof of work outside U.S.
17. Does solution address Gramm-Leach-Bliley Act, Section 501(b)?
18. Does solution adhere to Federal Deposit Insurance Act – section 36?
19. Are the risks regarding Consumer Claims understood?
Questions:
Settlement Requirements

1. Is solution devoid of all involvement in funds movement?
2. Will settlement be made based on a transaction that is properly verified?
3. Will settlement be made outside of the blockchain?
4. Will solution avoid any possibility of settlement revocation?
5. Yes indicates that settlement finality is not required.
The Strategic Framework Matrix – Excel Tool

Double Click Graphic Below to Access Matrix in Excel Format

<table>
<thead>
<tr>
<th>Does Solution Require The Blockchain Conceptual Framework</th>
<th>Is The Solution A Good Fit For The Blockchain Data Structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are distributed transactions a fundamental need (i.e., a centralized approach is improbable) Are the partners untrusted Is the immutability of data a primary requirement Are all participants prepared to operate a node</td>
<td>Is the transactional data structure static Is data typically accessed as a full transaction Can all transactions be visible to all participants Is each transaction final and rarely changed Is each transaction permanent, deletions not required Does solution run in a properly managed environment under US legal structure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does Solution Meet Regulatory And Settlement Needs</th>
<th>Can Solution Operate In A Limited Access &amp; Throughput Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the solution approved by appropriate regulators Does solution meets KYC, data residency, &amp; UDAAP needs Is liability (for error / failure) understood (in US law) Is there no need for settlement or Does solution settle over existing networks, or If settlement uses cryptocurrency, is it acceptable to the US Government</td>
<td>Are access controls simple or not required Is slow transaction validation acceptable Is low throughput acceptable Is data ownership visible to all participants acceptable Is it acceptable everyone knows your transaction volume Can transactions be re-encrypted when needed</td>
</tr>
</tbody>
</table>

Yes

Yes

Yes

Likely Fit For A Blockchain!
Evernym Use Case Evaluation
Evernym: Application Evaluation Status

- Research Solution
- Fill In Excel Matrix, Identify Areas of Uncertainty
- Establish Open Questions
- Interview Company
- Create Interview Notes
- Update Excel Matrix
- Update PowerPoint
Evernym Solution Overview

Evernym has designed and is currently implementing an immutable ledger that will deploy nodes in a multi-tier trusted distributed infrastructure. The design utilizes the multi-tier structure to address both performance issues and governance issues.

To make the solution broadly available, Evernym gifted the underlying distributed identity ledger technology to an International Non-Profit Organization called the Sovrin Foundation, which will be responsible for the worldwide governance of the Sovrin Network. Importantly, the Foundation will initially consist of a Board of Trustees with a minimum of nine members, plus a Technical Governance Board that reports to the Board of Trustees. Launch of the Sovrin Foundation was announced at the Personal Information Economy Conference on September 29, 2016, in London.

This solution structure was designed to deliver governance and accountability across multiple geographies and will control software development and management to meet those goals. It is unclear that this is possible given potentially conflicting regulations on privacy and data residency on a worldwide basis.

Given the large scope of this effort, Mercator Advisory Group estimates that fully funded, it will require at least 18 to 24 months before the first public product release.
Evernym: Sectional Results

Overview

Evernym has designed and is implementing an immutable ledger using nodes to be deployed in a multi-tier trusted distributed infrastructure. Solution is designed for performance and to address regulations, but software and legal structure remain under construction. Sovrin Foundation, an international not-for-profit, will control deployment to trusted entities and design organization and technology to meet regulations worldwide.

Mercator Advisory Group estimates that fully funded, first public product release will require 18 to 24 months.

- Adherence to Blockchain Conceptual Framework 29%
  - Poor Fit
- Transactional Data Elements Utilized 14%
  - Poor Fit
- Data Access Privileges / Data Availability Utilized 47% (65% if Maybe = Yes)
  - Moderate Fit. Many issues depend on implementation.
- Regulatory, Data Ownership and Residency Requirements 26% (74% if Maybe = Yes)
  - Moderate Fit. Many issues depend on implementation.
- Settlement Requirements NA
  - Not Applicable to Identity
Evernym Observations By Section

Adherence to Blockchain Conceptual Framework 29%
  • Given the technical effort required to modify a blockchain to support a self sovereign identity solution suggest that traditional technologies could have been utilized with less cost and faster execution. P/P keys are available on traditional databases and when operated in the cloud are capable of shredding data across multiple disks and geographies that would make re-construction via a hack inconceivable.

Transactional Data Elements Utilized 14%
  • An identity solution will need complex data structures that will require extraordinary effort to achieve because access privileges will change frequently (you may now access my ID).

Data Access Privileges / Data Availability Utilized 47%
  • Rapidly changing read privileges to records and fields is very difficult using P/P Keys.

Regulatory, Data Ownership and Residency Requirements 26%
  • Only a good fit if the Sovrin Foundation can manage the technology and organizational structure appropriately. Difficult if trying to satisfy multiple geographies.

Settlement Requirements NA
  • An identity solution has no settlement requirements.
Guardtime Use Case Evaluation
Guardtime:
Application Evaluation Status

- Research Solution
- Fill In Excel Matrix, Identify Areas of Uncertainty
- Establish Open Questions
- Interview Company
- Create Interview Notes
- Update Excel Matrix
- Update PowerPoint
Guardtime is a software security company founded in Amsterdam shortly after the April 2007 Russian cyber attack on the Estonian parliament, banks, ministries, newspapers and broadcasters. While Guardtime aggressively markets its technology as blockchain, this is a large stretch since of the five components that establish a blockchain, Guardtime only utilizes two; Merkle Tree and Secure Hash which are combined to create a secure ledger of external data.

Guardtime monitors files and databases resident on external computers and creates a linked hash associated with every modification. The linked hash concept creates an immutable ledger that is stored externally which can be used to assure data has not been tampered with. Because a SHA hash is relatively simple to calculate Guardtime can monitor very large sets of data that are modified frequently. Because the hash is not based on PKI and is impossible to reverse engineer to expose the data the hash was created from, Guardtime is very secure.

Guardtime is used widely by commercial entities and by several government agencies, including US intelligence, to monitor critical software systems. The company sells the solution as licensed software but also sells a hardened hardware solution that greatly reduces external threats.

Guardtime is not a distributed solution and uses only technology that has been deployed for years. As such the product is available today to protect a wide range of off-the-shelf systems, including the Oracle database. Guardtime as a clever utilization of technology but is not a blockchain implementation.
Guardtime: Sectional Comments

Overview
Guardtime has implemented an immutable ledger on a single node to monitor and detect inappropriate changes to external files and databases. Utilizing only basic hash functions and Merkle Tree structures on a local node, the solution is not a blockchain, but establishes an immutable ledger for external systems that can detect when a computer has been hacked. Guardtime is not a blockchain, which is why it scores so well on transactions, data access privileges, and regulatory issues. Guardtime provides a valuable function that is used by several US Government agencies today.

- Adherence to Blockchain Conceptual Framework 14%
  - Very Poor Fit
- Transactional Data Elements Utilized 100%
  - Poor Fit
- Data Access Privileges / Data Availability Utilized 88%
  - Moderate Fit. Many issues depend on implementation.
- Regulatory, Data Ownership and Residency Requirements 95%
  - Moderate Fit. Many issues depend on implementation.
- Settlement Requirements
  - Not Applicable to Identity
Guardtime Observations By Section

Adherence to Blockchain Conceptual Framework 25%
• Guardtime does not require distributed nodes or a trust algorithm and is not considered a blockchain solution by Mercator. It does support an immutable ledger that gives it 25%.

Transactional Data Elements Utilized 100%
• The Guardtime solution is designed to collect and store hashes of data from multiple systems so it can provide a trace of all changes made to any system. As a result, it has a very simple ledger structure consisting primarily of a unique name for the resource and a hash. This made it easy to address all the data element tests.

Data Access Privileges / Data Availability Utilized 86%
• Because the stored data is only offered to the originator of the data (or others they designate), the need for permissions is extremely simple.

Regulatory, Data Ownership and Residency Requirements 83%
• As the stored data does not fall under any banking regulatory constructs it was also able to pass this aspect of the evaluation with flying colors.

Settlement Requirements NA
• Guardtime has no settlement functions or requirements.
Ripple Use Case Evaluation
Ripple:
Application Evaluation Status

- Research Solution
- Fill In Excel Matrix, Identify Areas of Uncertainty
- Establish Open Questions
- Interview Company
- Create Interview Notes
- Update Excel Matrix
- Update PowerPoint
Ripple Solution Overview

Ripple’s distributed network, based on blockchain technology, enables banks around the world to directly transact with each other without the need for a central counterparty or correspondent banking relationship.

Unlike Evernym that is developing a complex business structure and architecture to address its use case, Ripple has already pivoted from its original use case to one that is designed specifically to address the needs of banks.

Initially Ripple was designed to incorporate end users, banks, and exchanges in a tightly coupled environment that made all transactions visible to all parties. This solution, based on a blockchain construct utilizing the Ripple Consensus Protocol, implements collectively-trusted subnetworks. The Ripple technology has been deployed for some time and has remained stable. Ripple is now modifying its technology and organizational structure to specifically address the needs of banks and bank regulators.

Ripple will announce a new structure and legal construct soon and with several banks already on board, may be able to win over more banks and regulators within 6 – 12 months.
Ripple: Sectional Comments

Overview

Ripple was initially designed to enable banks to perform international remittances using XRP (Ripple's digital currency) and was intended to directly support consumers, banks and exchanges through its blockchain solution. It is now focused primarily on bank to bank transactions and is adapting the technology and legal structure to address the regulatory construct required.

Mercator Advisory Group estimates it will take 6-12 months to better align solution with the banking regulatory framework.

- Adherence to Blockchain Conceptual Framework 57% (71% if Maybe = Yes) – Poor Fit
- Transactional Data Elements Utilized 57% (86% if Maybe = Yes) – Poor Fit
- Data Access Privileges / Data Availability Utilized 65% (94% if Maybe = Yes) – Moderate Fit. Many issues depend on implementation.
- Regulatory, Data Ownership and Residency Requirements 16% (63% if Maybe = Yes) – Moderate Fit. Many issues depend on implementation.
- Settlement Requirements 40% (80% if Maybe = Yes)
  • Not Applicable to Identity
Ripple Observations By Section

**Adherence to Blockchain Conceptual Framework** 57%

- Ripple solution is a good utilization of blockchain, but ILP protocol used to align with banks is closer to a P2P protocol, only using the blockchain to record transactions. Management today is unaligned, but that should soon change.

**Transactional Data Elements Utilized** 57% (86% if Maybe = Yes)

- If the modifications Ripple plans come to fruition it will excel in this section.

**Data Access Privileges / Data Availability Utilized** 65% (94% if Maybe = Yes)

- If the modifications Ripple plans come to fruition it will excel in this section.

**Regulatory, Data Ownership and Residency Requirements** 16% (63% if Maybe = Yes)

- Will have a passing grade of able to bring its plans to fruition, but distributed transactions across geographies may remain a challenge for some regulatory bodies.

**Settlement Requirements** 40% (80% if Maybe = Yes)

- Connecting banks core systems utilizing ILP would enable bank to bank settlement if appropriate organizational structure is implemented as planned.
A Strategic Framework Checklist
For Evaluating Blockchain Solutions