ACT-IAC Blockchain Playbook

Assessment Section

**Section Leads:** Aleks Zelenovic (Sapient), Star Vanamali (Sapient) & Sandy Barsky (GSA)

**Date:** Jan 25, 2017

**Suggested Length:** 4-5 pages; Current Length: 25 pages (with graphics & appendix)

**Audience:** Business Owners and Government Execs

**Overall Purpose and Goals:** As blockchain is an emerging technology, both Gov and Industry are still discovering what are best practices, approaches and how to evaluate offerings, technologies and approaches. This section provides guidance on assessing Blockchain offerings, technologies, … and when to apply them.

Table of Contents

[Introduction (Suggested: .5 pages) 2](#_Toc504671121)

[Setting the Stage 2](#_Toc504671122)

[Method 2](#_Toc504671123)

[What does success look like? 2](#_Toc504671124)

[Assessment Overview (Suggested: 1-2 pages) 2](#_Toc504671125)

[Explaining Basic Principle of Assessment at a high-level 2](#_Toc504671126)

[Enabling reference to the broader knowledge base 3](#_Toc504671127)

[“Do I need a blockchain?” (Supporting Graphic) 3](#_Toc504671128)

[Blockchain Types (Permissionless / Public Consortium / Private Consortium) 4](#_Toc504671129)

[Which type of Blockchain is best fit for me? 7](#_Toc504671130)

[Practical Advice & Best Practices (Suggested: 2 pages) 7](#_Toc504671131)

[Set of practical advice around blockchain assessment 7](#_Toc504671132)

[Focus on 5-10 key practices 9](#_Toc504671133)

[Outcomes (Suggested: 0.5 page) 11](#_Toc504671134)

[Clearly define few deliverables/outcomes of the assessment 11](#_Toc504671135)

[How outcomes from assessment link to next phase - readiness 11](#_Toc504671136)

[Team reference content to support discussion and/or for appendix 12](#_Toc504671137)

# Introduction (Suggested: .5 pages)

## Setting the Stage

(1-2 sentences providing the purpose of the section and referencing the rest of the content)

* Assessing Blockchain in the effort to better meet mission while realizing gains in cost savings, efficiency, and reducing risk. The reason to apply a (new/emerging) technology is to realize gains in cost saving, efficiency, and reduced risk in the use of IT to meet mission. There are many use cases that will benefit from a distributed ledger, not all require a Blockchain. [*CONTRIBUTOR: Sandy*]
* Blockchain is a nascent technology.  Both the government and industry are still discovering  best practices, approaches and how to evaluate offerings, technologies, approaches and when to apply them.  This section will help decision makers assess whether a blockchain solution is the right technology to apply against the use case and requirements they are addressing.  It will also guide decision makers towards the type of blockchain solution that best fits their requirements. [*CONTRIBUTOR: Tennenbaum*]

## Method

(How? – guided, practical, blockchain specific?) [*CONTRIBUTOR: Sean H.*]

* Fully outline operational and strategic context surrounding identified business problem(s) and/or unmet stakeholder need(s) to ensure comprehensive understanding of environment
  + Include both current-state and desired future-state
* Identify and document pain points and/or gaps within the current business processes that are hindering transition to future state
* Document functional requirements for resolving pain points and/or filling gaps via technical solution (i.e. agnostic of blockchain)
* Conduct analysis of alternatives (AoA) including blockchain as alternative along with other available technical solutions

## What does success look like?

* CONTRIBUTORS/CONTENT NEEDED

# Assessment Overview (Suggested: 1-2 pages)

## Explaining Basic Principle of Assessment at a high-level

[*CONTRIBUTOR: Bajinder*]

* The ever increasing demand on federal CIOs to deliver more for less while better enabling the agency mission with measures for improving operational efficiencies, enhancing customer experience, reducing cost of IT solutions and safeguarding sensitive agency/public information. Increasing demand for reporting due to oversight of the CIO’s by both the executive and the legislative branches designed to ensure IT strategies are delivering results that optimize service and operational delivery (increase gains in efficiency, saving, and reduced risk). CIOs now are accountable to demonstrate compliance with the Federal Information Technology Acquisition and Reform Act (FITARA), OMB’s Data Center Consolidation Initiatives (DCOI) and indeed cyber security risk mitigations, and have the opportunity to bank and reinvest those gains in savings, efficiency and reduced risk as per the Modernize Government Technology Act. The Federal government spends approximately $80B on its IT needs on an annual basis, significant percentage of which is allocated to maintain legacy O&M and Data Center operations. The burden of maintaining legacy operations environment impacts the CIOs to drive much needed modernization leveraging innovation.
* The implementation of Blockchain based solutions must demonstrate that both the architecture and solutions enable not only compliance to oversight regimes such as FITARA, GAO and OMB oversights but also drive efficiencies, Resiliency, transparency, accountability and enhance security of digital assets (increase gains in efficiency, saving, and reduced risk). The use of Blockchain must also demonstrate alignment to the priorities of the federal policies. Currently, these include enhancing customer experience, improving cyber security of federal systems and data and promoting shared services. Defined Blockchain criteria shall be used to assess Blockchain implementations for alignment to address above mentioned mandates and drivers. If a Blockchain thread can be weaved into a legacy or other IT solution then the benefit of the Modernize Government Technology Act can be realized by the department/agency.

## Enabling reference to the broader knowledge base

* Providing links to libraries, self-guided learning tools, concepts etc. [*CONTRIBUTOR: Jim and others?*]
  + Links: Create a library landing page that is updated regularly with the latest guidance (Jim has volunteered to update; need to work out details with ACT-IAC on opportunity; possibly coordinate with Justin at GSA if needed)

## 

# “Do I need a blockchain?” (Supporting Graphic)

[*CONTRIBUTOR: Jim and team*]

|  |  |
| --- | --- |
| Consideration/Question | Points |
| 1. Does the use case involve a high number of contributing users? | 3 |
| 1. Does the use case involve transacting with outside organizations (organizations other than my own)? | 2 |
| 1. Are the writers of transactions trusted (Or do we need a separate level of authentication)? Note: This can be a device – like an IoT device; not just a person. | 5 |
| 1. Is it required to restrict participation to blockchain to a limited community (consortium / permissioned blockchain) or is it open to the public? (Permissioned vs. Public) | 1 |
| 1. Is identity of the transaction participants required? | 1 |
| 1. Does anonymity of the transaction need to be preserved. (Anonymous contributor) | 1 |
| 1. Does privacy of the transaction need to be preserved (in some form).  E.g., Party A transacts with Party B – Party C should not be able to see Parties A/B. | 1 |
| 1. Are there going to be relatively few number of transactions per second? (<1K/sec)  Note: high performance requirements are typically not met by blockchain solutions.\* Note2: Near Real Time performance typically is not met by blockchain. | 1 |
| 1. Is provenance of an asset – tracking the lifetime history of an asset (moving from factory to distribution center to final destination across the life cycle) – of value? | 1 |
| 1. Do you need strict immutability at the record level (no cancel, amend, even by admin)? | 1 |
| 1. Will the system be standalone, not needing access to legacy data/systems?   (OK to use legacy systems and still draw data from them) Example: Electronic Health Records data could hold subset of data in blockchain. | 1 |
| 1. Do you not have a trusted system validation for all parties? (Could rephrase to positive and assign a point value of –1 if they answer yes). | 3 |
| 1. Are your data sets/stores relatively small that you intend to store on the blockchain? (Large amounts of data are not typically conducive to blockchain solutions, though you can segregate and redirect to other data stores). Would be OK to store hash value in the block chain that validates a large data store (design) off chain. | 3 |
| 1. Are you trying to resolve inefficiencies or complexities that span multiple organizational/agency groups? | 3 |
| 1. Can you not solve this problem using current other (non-blockchain) technologies? (discuss centralized versus decentralized etc. - maybe separate). | 3 |
| 1. \*\* See Sanjeev's pro/con arguments to complete this list. | 1 |

A point total of 15 or more indicates you may get a substantial ROI from a blockchain approach.

# Blockchain Types (Permissionless / Public Consortium / Private Consortium)

[*CONTRIBUTOR: Sanjeev + subgroup]*

|  |  |
| --- | --- |
| **Permissionless Blockchain**  Any participant is able to become a validator for a block’s integrity | |
| **Features** | Trustless public blockchain supporting multiple readers and writers with open read/write. |
| High public verifiability |
| Consistent state of blockchain across all users |
| Potential to disrupt current business models through disintermediation with no middle man is required as the same shared ledger of transactions and shared set of programs to update transactions are made available at every node in blockchain. |
| Membership with anonymity based access to data with anyone can join network , access the transactions and participate in consensus. |
| Slower with all the nodes are involved in validating transaction blocks. |
| **Context** | Open source and permissionless with anyone can download the protocol and validate the transactions (validating integrity of blocks by participating in consensus) |
| Anyone in the world can send transactions through the network and expect to see them included in the blockchain if they are valid |
| Anyone can read transaction on the public block explorer. Transactions are transparent, but anonymous/pseudonumous. |
| Public blockchains, hold the potential to replace most functions of traditional financial institutions with software, fundamentally reshaping the way the financial system works |

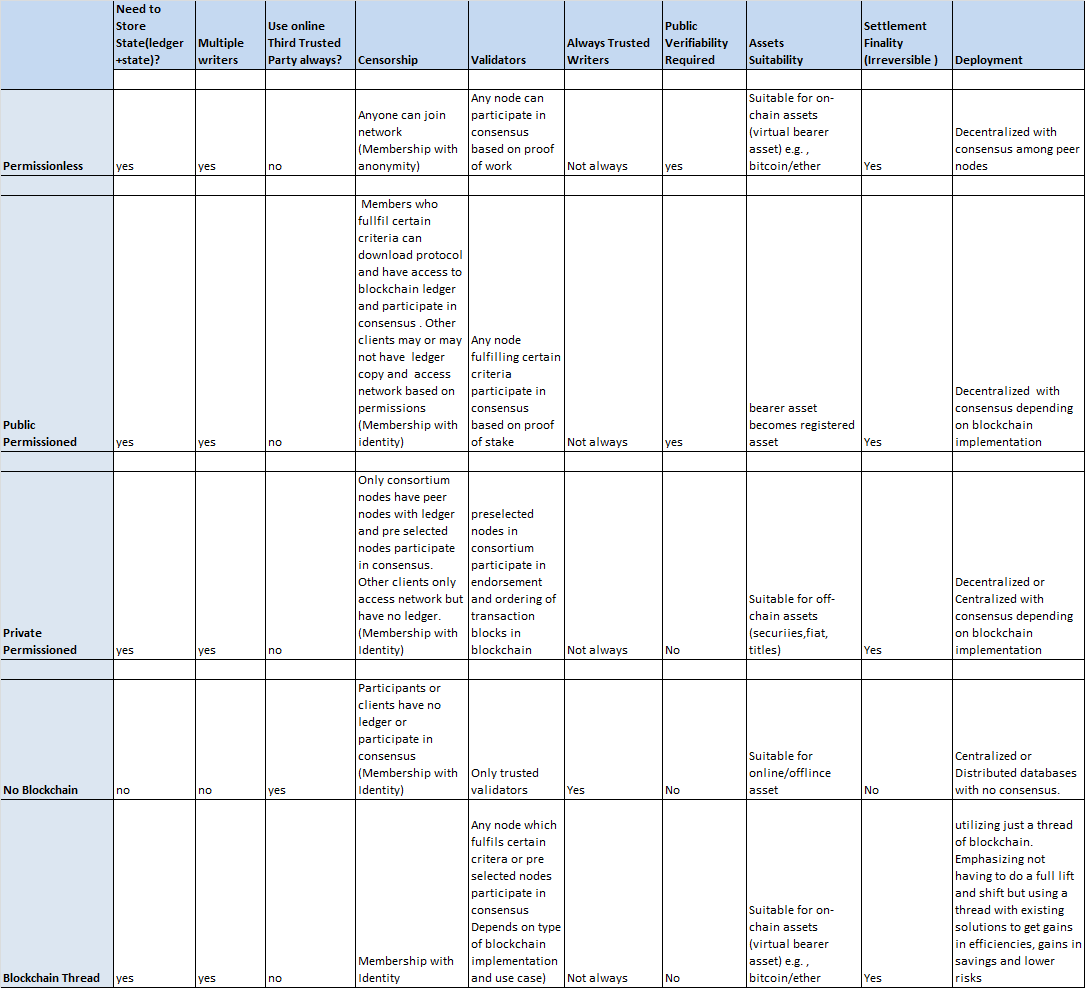
|  |  |
| --- | --- |
| **Public Consortium Blockchain**  Requires only pre-selected parties to validate transactions. | |
| **Features** | High throughput and scalability as relative number of validators is low compared to public blockchain. |
| Federated or consortium blockchain operate under the leadership of a group (gov agencies or financial institutions) which decide the criteria for others to participate in blockchain network. |
| High transaction privacy as any client access to blockchain in is controlled based on permissions configured by consortium peer nodes. |
| The consensus process is controlled by a set of nodes meeting a certain pre defined criteria and consensus is based on proof of stake. for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. |
| Custom defined consensus algorithms with flexible chain trust model. |
| Membership with Identity based access controls(Read/Write) on data through hybrid modular cryptographic approach |
| Faster and Permissioned read/writes. |
|  | Anyone who meets certain pre defined criteria can download the protocol and validate the transactions. |
| **Context** | Consortium of government and financial institutions with all would have one or more peers and each peer would have a copy of the ledger and participate in validating the transactions. Other institutions or the public could be granted access based on permissions, to the network as clients which may or may not have a copy of the ledger. |
| Useful to implement both financial and non financial use cases in government or multi organization controlled blockchain networks and allowing access based controlled access on network to client organizations and public. |

|  |  |
| --- | --- |
| **Private Consortium Blockchain**  Permission to write data onto the blockchain is controlled by a single or group of organization | |
| **Featuress** | High throughput as the relative number of validators is low compared to permissionless blockchain |
| Federated or consortium blockchain operate under the leadership of a group (gov agencies or financial institutions) which decide the criteria for other clients to participate in blockchain network. |
| High transaction privacy as any client access to blockchain in is controlled based on permissions configured by consortium peer nodes. |
| The consensus process is controlled by a pre selected set of nodes defined by configuration who will participate in endorsement and ordering of the transaction blocks . Custom defined consensus algorithms with flexible chain trust model. Client nodes cannot participate in consensus. |
| Different access controls(Read/Write) on data through hybrid modular cryptographic approach |
| Consortium peer nodes have the blockchain ledger and state database with client only access to blockchain network based on access permissions. Clients will not have access to ledger. |
| Faster and Permissioned read/writes with only pre selected nodes determined by administrator nodes in consortium participate in consensus. |
| **Context** | Consortium of government and financial institutions with all would have one or more peers and each peer would have a copy of the ledger and participate in validating the transactions. Other institutions or the public could be granted access based on permissions, to the network as clients which will not have a copy of the ledger. |
| Useful to implement both financial and non financial use cases in government or multi organization controlled blockchain networks and allowing access based controlled access on network to client organizations and public. |

# Which type of Blockchain is best fit for me?

[*CONTIBUTOR: Sanjeev + subgroup]*

* Graphic Suggestions: Visually demonstrate an evaluation methodology with a set of pro/con criteria/features for each option. Could be a table with columns and rows that as an option meets a criterion/feature, the individual uses a check-mark.



# Practical Advice & Best Practices (Suggested: 2 pages)

## Set of practical advice around blockchain assessment

[*CONTRIBUTOR: Sandy, Mark, Jeff, Sudha, and others?*]

* Include regulatory considerations/mandates [*CONTRIBUTOR: Sudha*]
  + View the advances in banking frameworks to see how the financial frameworks can support extension of rule based regulations for other implementations.
  + Use elements of “Smart contracts, industry standards, technical standards, regulations, acts, common law” to address regulatory needs. For example BitLicense requires personal and professional recommendations. Or create BitLicense scenarios for encryption, whereby users of public encryption must be licensed.
  + Review recommendations from Swiss based “ICO Code of Conduct’ to help with integration of future regulatory hurdles.
* Provide guidance on approval for implementation of a prototype [*CONTRIBUTOR: Sudha*]
  + Provide guidance on a phased vs mass adoption at the agency level to avoid obstacles due to regulartory or security requirements.
  + Define what loss of control from an agency perspective may be and address regulation for the use of the blockchain implementation.
  + Lay out the adavantages in the auditing and security touchpoints to gain buy-in and get definitions of agency level or component level regulatory framework.
  + Take into account the the Congressional resolutions proposed July 14, 2016 in the U.S., “blockchain technology with the appropriate protections”.
  + Include Factors such as identity proofing, authentication, authorization mecanisms to take into account to address trust and identity needs at an agency level depending on the Risk level of the project.
  + Integrate security considerations to establish in online transactions in applicable sectors including financial services, payments, health care, energy, property management, and intellectual property management prior to prototype architecture and technology integration.
* Emphasize ROI to common costs and benefits to the network as a whole, the individuals members, etc (design thinking based on personas and a prioritization matrix around value vs. complexity should be included) and specific to government, not just about dollars but efficiencies and meeting the mission [*CONTRIBUTOR: Sandy*]
  + ROI
    - Gains in efficiency and cost savings - in bits and bites, keeping to a true agile methodology this is not a lift and replace, but a shifting to strategically assured positive ROI
    - **Cloud first and shared services -** the blockchain relies on distributed computing, grid computing, the cloud. The blockchain can be useful as a distributed ledger to enabling vendor provided shared services to demonstrate adherence to the current regulations and policies, and to have previous actions audit-able to previous instances.
    - Reducing risk - avoid the repeating the -<https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do> and  [OPM security breach](https://www.opm.gov/cybersecurity/cybersecurity-incidents/).  The ROI on being up and running, avoid a DoS, to meet mission without surrender PII or other critical data, priceless. Just as the FDA can leverage blockchain to make the food supply chain traceable so can the IT software and hardware do so to audit for a secure supply chain.
  + Proof of Concept vs. Proof of Technology [*CONTRIBUTOR: Sandy*]
    - The assessment is whether the use case is appropriate for the application of Blockchain. It is crucial that any Blockchain use case is a proof of concept, meaning that it is proving the viability (measured by gains in savings and efficiency, and reduction of risk) of the use case and not proving that the capabilities of the technology.
  + Trust among CIOs (networks between agencies that exchange data/asset and/or information)
  + Hype Cycle for Emerging Technologies (graphic below) – how to employ correctly to avoid the dip and not overpromise [*CONTRIBUTOR: Jim*]
  + Impact of Modernize Government Technology (MGT) Act
    - The MGT Act encourages agencies to take an enhanced strategic, incremental approach to IT with goals to drive gains of efficiency, cost savings, and lowered risk. Blockchain technology may be used to enhance an existing IT solution invest without a need to replace existing systems, instead it can enrich existing solutions with new capabilities and functionality that can be better provided by Blockchain technology.  Government cannot modernize using existing technology it is through the adoption of new technology, such as Bockchain, that modernization may be achieved. Strategically, if an agency has targeted an IT process to modernize, but does not have the budget to do so, it could choose a smaller project or projects that will realize savings in year one, and apply those savings (which can be banked for three years) to the larger more critical project in year two. This is a different way of modernizing around multiagency business networks and processes.  A strategic Blockchain solution is extensible, able to grow over time, adding new members and processes to the business network.  It also facilitates data sharing, the reduction of existing frictions and inefficiencies.  This approach is consistent with the MGT Act narrative; therefore, the assessment that an agency must make through a standard analysis of functions and gaps is to determine if the use of a blockchain will enhance an existing solution through gains of efficiency, cost savings, and lowered risk. [*CONTRIBUTORS: Barsky/Tennenbaum*]

## Focus on 5-10 key practices

[*CONTRIBUTORS: Sapient Consulting, others?]*

* Key Best Practices
  + Scope a Pilot Implementation: As an emerging technology that will provide the foundational data layer for your organization’s business applications and services, a blockchain implementation will include not only the introduction of a new technology to your ecosystem, but will also encompass modernization and integration of your legacy systems. This is a major transformation that entails major change management components. With that, a key focus of the assessment phase should be to define scope of a pilot blockchain implementation. Start small and strategically scale with the transformation of one priority area at a time.
  + Build Blockchain Architectural Blueprint During Assessment Phase: During the assessment phase, the organization should determine which desired technologies and subsequent capabilities can be enabled by blockchain implementation. That is, with blockchain in place, which additional technologies would the organization desire to take on? Options are abundant, though a close look at applications of machine learning, artificial intelligence, and robotic process automation may be a good starting point. To properly scope the broader, post-pilot future-state implementation, begin by identifying all systems for integration and understanding precisely how they interact. Building a blueprint of the technical architecture will provide a powerful tool for understanding and describing how the solution is likely to grow, to address pain points, to align stakeholders, and ultimately, to accomplish the transformational objectives of the blockchain solution.
  + Determine Throughput and Latency Requirements of Business Processes: Understanding your organization’s required amount of data and the speed by which data transactions must occur within the blockchain ecosystem are key inputs in determining your optimal architecture, accelerators, etc. Large blockchain ecosystems with many systems and players such public permission-less chains would be best served by minimizing data-load, whereas small private/consortium chains that don’t require many transactions per second can theoretically handle the exchange of larger “blocks” without interruption to business processes.
  + Assess Current State of Customer Experience: As with most transformative efforts, the blockchain initiative should also be used as an opportunity to enhance user experience. Robust usability testing will be key to successful user adoption as the blockchain solution is scaled outward. Users have little tolerance for solutions/systems that lack usability in the form of user-friendliness, intuitiveness, and/or accessibility. As a nascent technology, ensuring usability of the blockchain solution is doubly important in order for scaling of the solution to build and maintain momentum of adoption.
* Map each best practice with links or references to:
  + Use Case from GSA github library
  + Recommended Appropriate Taxonomy
  + Each best practice should have similar format
    - Header with high-level tagline/naming of the practice
    - Three key elements: description, analysis, takeaway/outcome

# Outcomes (Suggested: 0.5 page)

**[CONTRIBUTORS NEEDED]**

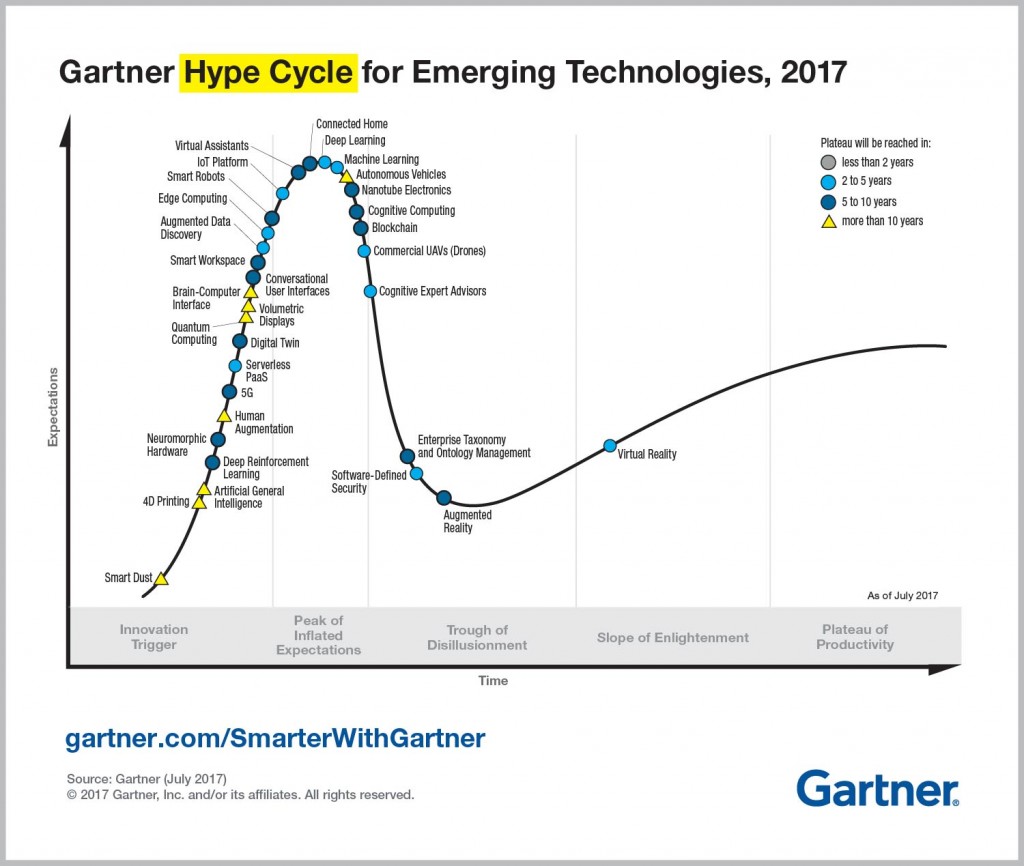
## Clearly define few deliverables/outcomes of the assessment

* Content needed

## How outcomes from assessment link to next phase - readiness

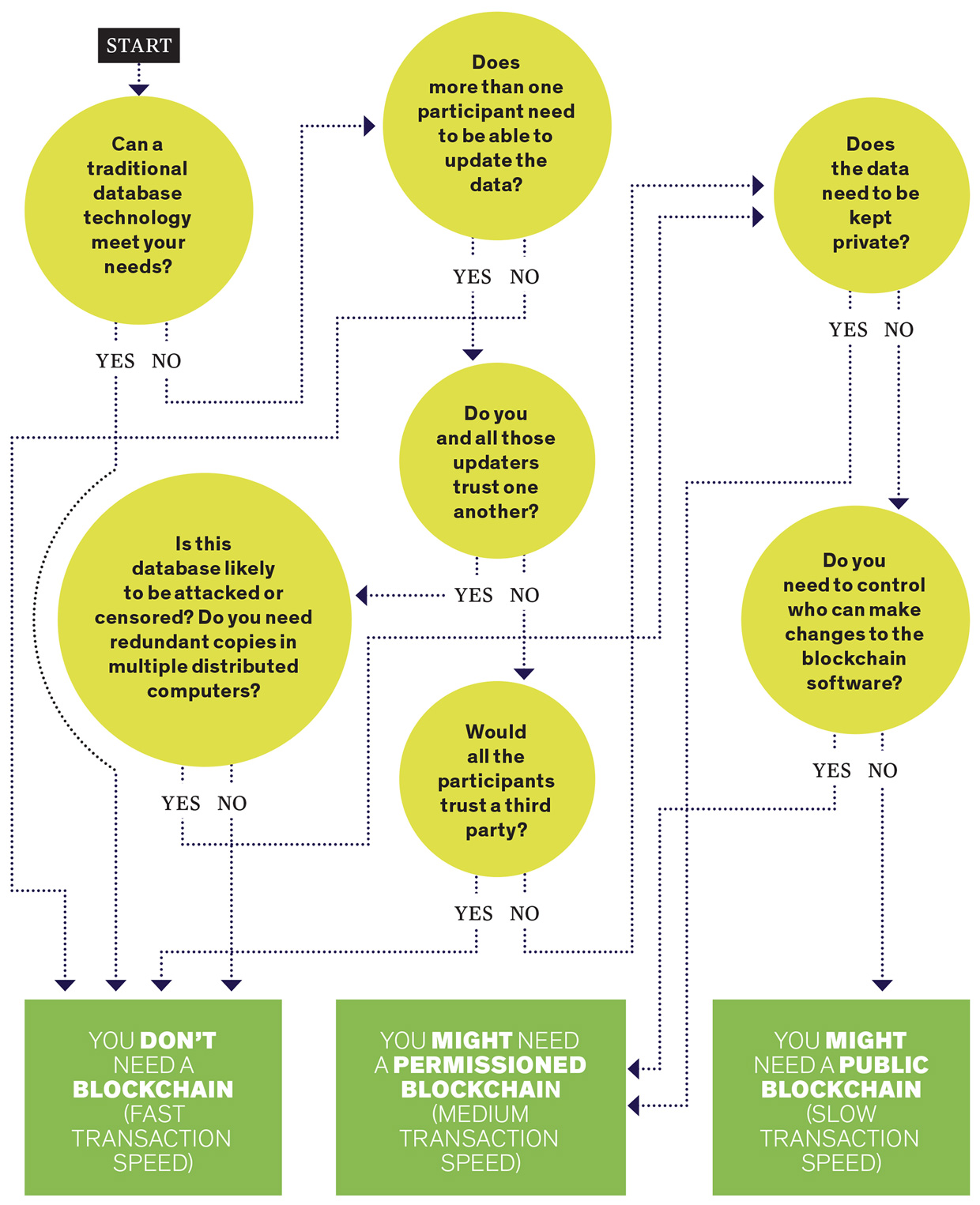
* Content needed

# Team reference content to support discussion and/or for appendix

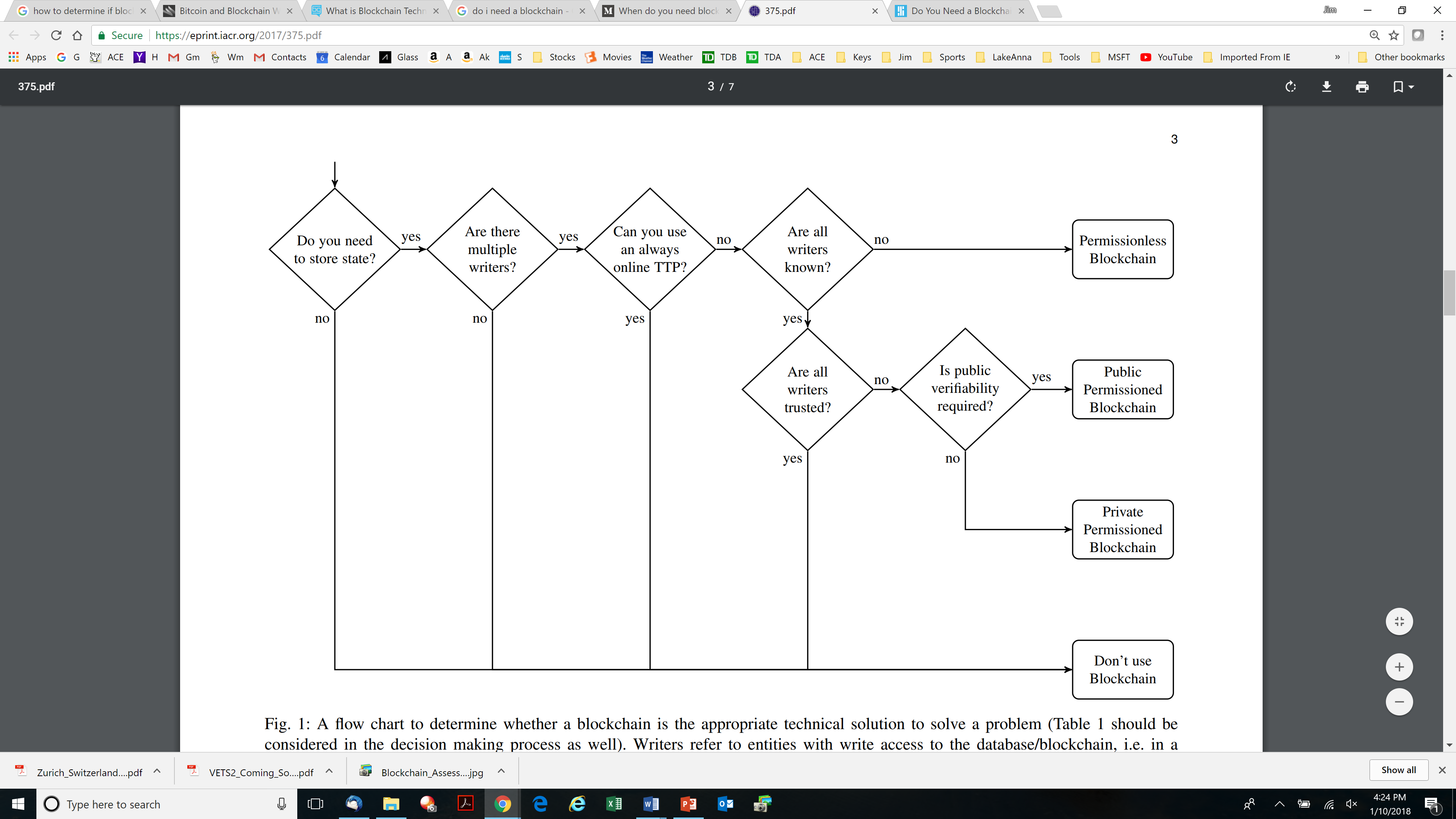


“Do I need a blockchain?” Graphic options for discussion

IEEE Spectrum September 2017 has a good graphic to consider: (<https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain>)



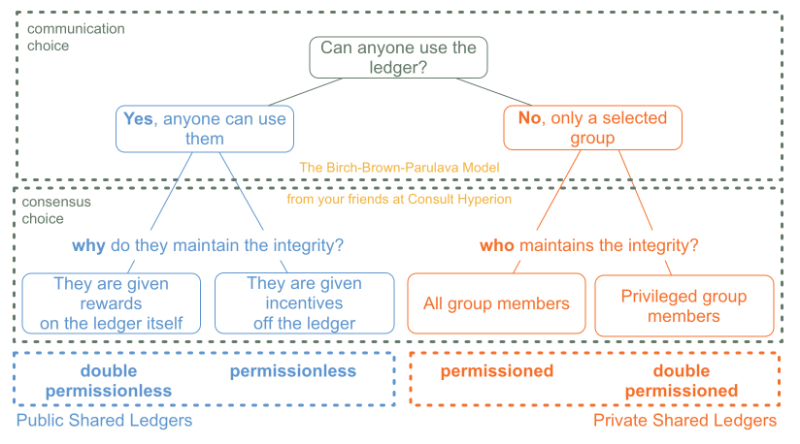
From Zurich Switzerland: (<https://eprint.iacr.org/2017/375.pdf>)



From here to the end are all from the link below and all have benefits/drawbacks:

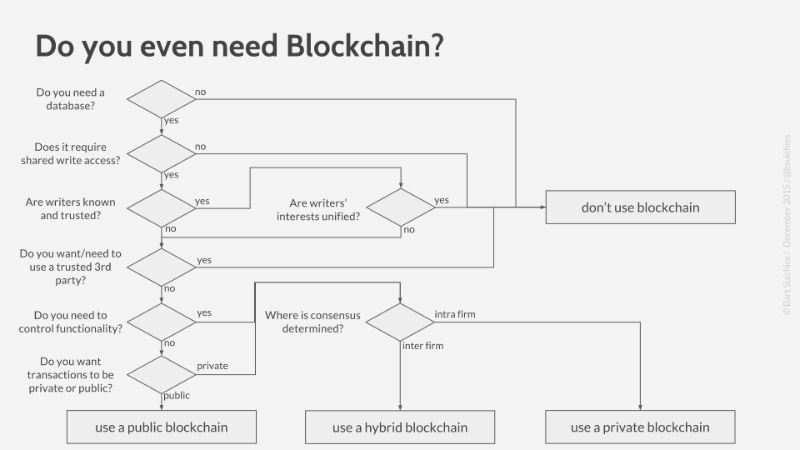
<https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1>

**Birch-Brown-Parulava model**



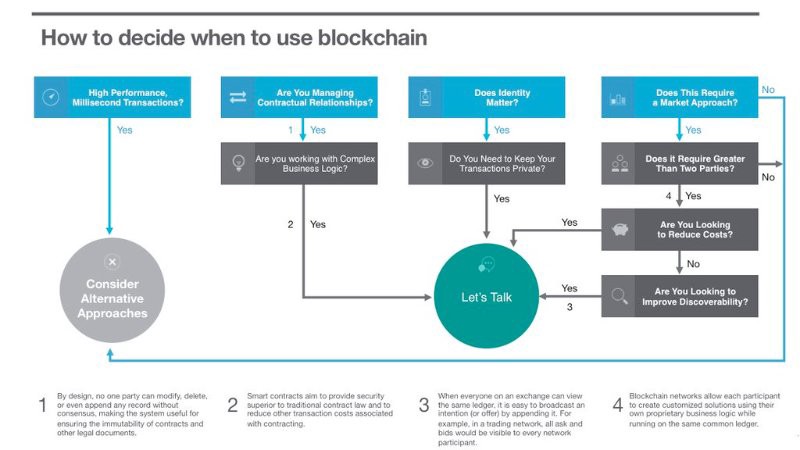
This is a good model that does not focus on the technology but on the distributed ledger concept, helpful to sort permissionless Vs permissioned ledgers out. Minor comment: it is not fully MECE because we could have a public network (“anyone can use”) maintained by a privileged group of validators (~Ripple), and private validators could be incentivized as well.

**B. Suichies Model**



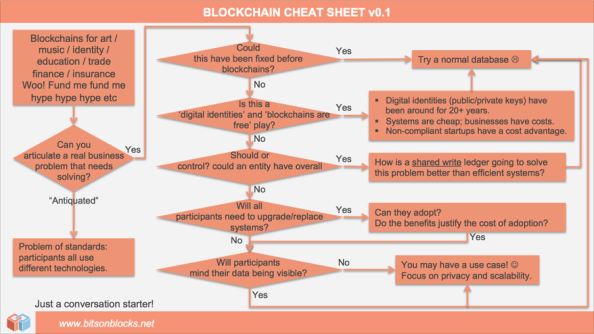
This model introduces the differences between public and private. Corda is typically an inter-firm effort building an hybrid DL platform. Personally I think an intra-firm blockchain doesn’t make sense — if in the past you couldn’t solve the reconciliation of the data shared across your group, it means you have larger issues (IT architecture budget systematically cut, regulatory constraints, etc.)… probably a blockchain won’t help.

**IBM model**



This model acknowledges that you need a “market” approach. But the step 2 should lead to “alternative approaches” as smart contracts can only manage simple business logic (lesson from The DAO). A strong need for privacy should also be dissuasive: do you want to share data or keep it private? Pick one.

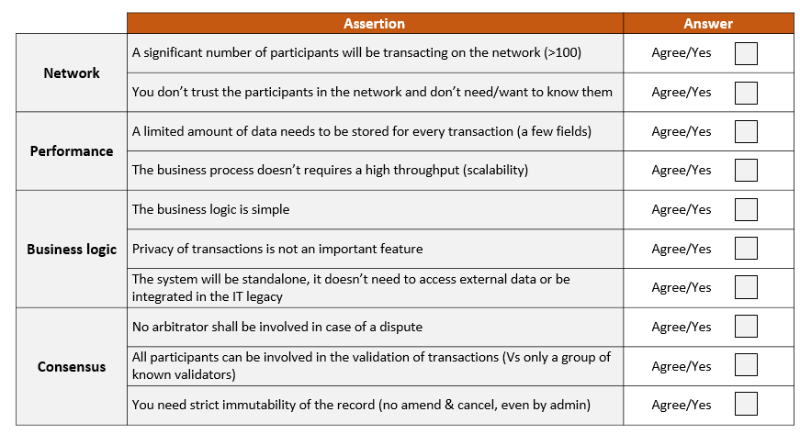
**A. Lewis model**



Antony has an excellent [blog](https://bitsonblocks.net/)on Bitcoin, Blockchain and Distributed Ledgers. I like the second question very much: “Could this have been fixed before blockchain?”. Blockchain is composed of existing pieces of technology (a bit of cryptography, a P2P consensus protocol and basic storage capabilities), so it is key to ask yourself why you couldn’t use these pieces of technology before.  
Also, notice that at the end of the tree you might still try a normal database :-)

**My model (as of Aug. 2016)**

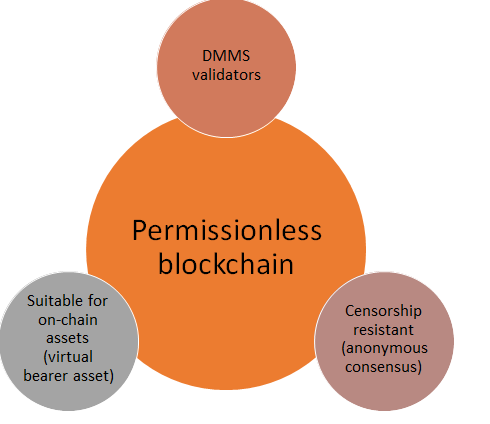
Well I thought about creating a smart tree to decide whether one needs a blockchain or not, but I ended up with a questionnaire :-)



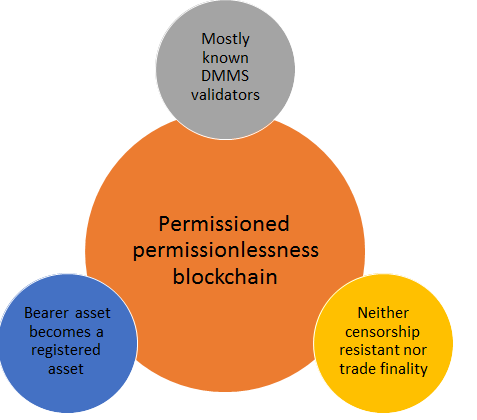
If you have 10/10, congratulations you might be building the next Bitcoin or Ethereum system!

Now the less ‘ticks’ you have, the more trade-offs and customization you need and the less blockchain technology is relevant for your business issue. Probably below 7/10 blockchain technology doesn’t make sense — you might still try to build a shared ledger but don’t call it a blockchain.

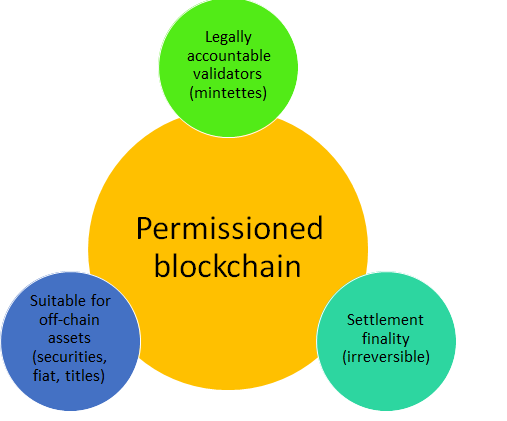
* Permissionless Blockchain
  + Permissionless Blockchain means that any participant is able to become a validator for a blockchain.
  + Bitcoin and Ethereum are the most prominent examples of Permissionless blockchains, which are public and decentralized.
  + Participants can leave and join the blockchain’s network at any time.
  + No central authority or trusted third party manages who is allowed to join the network, or bans illegitimate users from connecting to the network.
  + Anyone can read the chain, make legitimate changes or write a new block into the chain. Thus the number of vreaders, writers and untrusted writers are very high.
  + In a Permissionless setup, the number of nodes is expected to be large, and these nodes are anonymous and untrusted since any node is allowed to join the network.
  + Most of the DMMS (dynamic membership multi-party signature) validators join Permissionless blockchain as a DMMS digital signature to sign blockheads is formed by group of signers of no fixed size. Bitcoin’s blockheaders are DMMSes because their proof of work has a property that anyone can contribute without enrolment required and their contribution is weighted by computational power rather than one threshold signature contribution per party , which allows anonymous membership without risk of sybil attack (where party joins many times and has disproportional input into the signature).
  + Completely decentralized as the permissions to read and write data onto the Blockchain are shared equally by all the connected users, who come to a consensus before any data is stored on the database.
  + Censorship resistant with anonymous consensus based on a completely trust-less system where no user is given special privileges on any decision
  + Consensus mechanism to prove the transactional verifiability is mainly based on proof of work (PoW). Nodes have to prove that they have expended significant amount of energy as Proof-of-Work (PoW) towards solving a hard cryptographic puzzle
  + Proof of work consensus assumes that amount of validators (miners) is unknown and validators are anonymous and have no reputation. In order to vote, proof of work needs to be presented, which requires hard computations . A consensus is reached if parties that control majority (usually 51% of computational power) agree.
  + Highly Immutable blocks as any tempering requires >51% participant node consensus in a very large public blockchain which is almost impossible.
  + Some Permission less blockchains also support PoS (proof of stake) based consensus . For Example Ethereum (in future), NXT , Peercoin.
  + PoS (proof of stake) consensus assumes that the validator of the next block is chosen in a deterministic way. The chance that a validator is chosen depends on its stake and a validator loses its stake if it commits an attack. The consensus is reached if the parties that control majority of wealth agrees.
  + High public verifiability with each state change validated by verifiers, e.g. miners on bitcoin’s or ethereum’s  blockchains. Any observer, or reader, on the other hand, can verify that the blockchain’s state has changed as per the protocol and eventually, all readers will have the same version of the blockchain.



* + **Pros**
    - Decentralized trustless public blockchain supporting a high number of readers and writers.
    - High public verifiability with all readers having same blockchain state at all times.
    - High security and immutability as Blockchain is mathematically very hard to hack as the cost of hacking becomes too high for a system where every node connected is synced with the entire Blockchain database and more importantly, once a hack is discovered, the value of the hacked coins would diminish exponentially
    - Consistent state of blockchain across all users.
  + **Cons**
    - Since all transactions in public blockchain need to be verified by thousands of users so transaction verification process is time consuming causing low latency and low throughput.
    - Users have to pay a larger amount of transactional fee compared to private blockchain.
    - All Transactions are shared and publically accessible, though private data can be concealed by using cryptographic primitives.
    - Scalability and Data Privacy is a concern.
* Public Permissioned Blockchain (Public Permissioned Blockchain. Aka. Permissioned permissionless blockchain)
  + A permissioned Blockchain requires only pre-selected parties to validate transactions. Permissioned blockchains have been proposed to authorize only a confined group of users to participate in the blockchain network. A central authority (consortium) determines and gives right to the predefined peers to write, read , monitor or audit the transactions on blockchain with a public verifiability of content is desired.
  + Permissioned Blockchains are operated by known entities (known as consortium entities) such as stakeholders of a given industry with immutability and efficiency is preferred over anonymity and transparency.
  + The participants require some means of identifying each other while not necessarily fully trusting each other.
  + In the world of business, permissioned blockchain systems often come across critical requirements (from a practical and regulatory perspective) for transactional security and privacy of business logic that is put on a shared ledger. In addition, commonly enterprise-purposed permissioned ledgers need to meet certain performance and scalability standards and/or comply with different cryptographic standards and practices, ultimately calling for modularity of crypto components.
  + In a permissioned blockchain, organization determines who may act as transaction validator on their network, A blockchain developer may choose to make the system of record available for everyone to read, but they may not wish to allow anyone to be a node, serving the network’s security, transaction verification or mining.
  + With permissioned blockchains, this may or may not involve 'proof of work' or some other system requirement from the nodes.  There may not need PoW but broad understanding of consensus at transaction level among peer nodes that allows multiple approaches, Generally permissioned blockchain algorithms are based on BFT(Byzantine Fault Tolerance) consensus type.
  + BFT consensus type assumes that amount of validators are known upfront. Validators know each other and adding or removing a validator require approval of the rest.
  + Although some degree of decentralization is maintained in their structure, the participants have the power to grant read/write permissions to other participants, leading to the ‘Partially Decentralized’ design of Permissioned Blockchains
  + The transactions are quick to verify in a Permissioned Blockchain as there are a handful of verifiers, with the transaction fee miniscule thus increasing the overall efficiency of transactions.
  + The Permissioned Blockchains maintain the privacy of a user’s data, without consolidating power with a single organization.
  + Hyperledger offers open source pluggable architecture based implementation of permissioned blockchain with flexibility for users to configure the consensus module that meets their needs.



* + **Pros**
    - High transactional throughput and transactions are quicker as lesser number of transaction validators are required to validate the transactions stored in blockchain. Scalability is high.
    - High Immutability guaranteed with access controlled by central authority. Security and Data privacy is high.
    - Different user defined consensus algorithm based implementation approaches possible with flexible chain trust model execution.
    - Transactions are highly secure and user data privacy with permissioned access control for all users accessing blockchain
    - Public verifiability of content is possible.
    - Hybrid approach possible with read and write access to selected nodes as well as read access to public on selected data with modular cryptographic approach.
    - Maintain privacy of user data without consolidating power with a single organization.
    - Very small or no transactional fee required to carry out transactions.
  + **Cons**
    - Transparency and anonymity is not fully implemented but rather controlled by consortium organization entities.
    - Single point of failure and bringing various organizations to use a common model.
    - Number of writers and readers are low compared to public blockchain.
    - Centrally managed.
* Private Permissioned Blockchain
  + Permission to write data onto the blockchain is controlled by a single organization which is highly trusted by all other users. Useful when no public Readability of content is desired.
  + This organization may/may not allow users to have access to read the data, as public readability might not be necessary in most cases.
  + In some situations, the organization might want the public to audit the data. Limited/restricted read permissions also provide a greater level of privacy to the users, a feature not available in Public Blockchains.
  + The organization in control has the power to change the rules of a Private Blockchain and may also decline transactions based on their established rules and regulations.
  + In a Private Blockchain, the transactions are quicker as they can be verified be a small number of devices. Thus, the users pay lesser amounts of transaction fees since the number of people verifying the transaction is fewer than in a Public Blockchain.
  + The devices are very well connected and any faults can be fixed by human intervention, which can be easily approved by the users since the users trust the single organization in control of the Blockchain.
  + Like public permissioned blockchain, private blockchains have a access control layer built into protocol.
  + With permissioned blockchains, this may or may not involve 'proof of work' or some other system requirement from the nodes.  There may not need PoW but broad understanding of consensus at transaction level among peer nodes that allows multiple approaches, Generally permissioned blockchain algorithms are based on BFT(Byzantine Fault Tolerance) consensus type.
  + BFT consensus type assumes that amount of validators are known upfront. Validators know each other and adding or removing a validator require approval of the rest.
  + The transactions are quick to verify in a private Blockchain as there are a handful of verifiers, with the transaction fee miniscule thus increasing the overall efficiency of transactions.
  + The Private Blockchains maintain the privacy of a user’s data, without consolidating power with a single organization.
  + Hyperledger offers open source pluggable architecture based implementation of private permissioned blockchain with flexibility for users to configure the consensus module that meets their needs.



* + **Pros**
    - High transactional throughput and transactions are quicker as lesser number of transaction validators are required to validate the transactions stored in blockchain. Scalability is high.
    - High Immutability guaranteed with access controlled by central authority.
    - Different user defined consensus algorithm based implementation approaches possible with flexible chain trust model execution.
    - Transactions are highly secure and user data privacy with permissioned access control for all users accessing blockchain
    - Hybrid approach possible with read and write access to selected nodes as well as read access to public on selected data with modular cryptographic approach.
    - Maintain privacy of user data without consolidating power with a single organization.
    - Very small or no transactional fee required to carry out transactions.
  + **Cons**
    - Transparency and anonymity is not fully implemented but rather controlled by single central organization.
    - Single point of failure
    - Number of writers and readers are low compared to public blockchain.
    - Centrally managed.