**Blockchain Playbook**

**Assessment Section**

Section Leads: Aleks Zelenovic (Sapient) & Sandy Barsky (GSA)

Date: Jan 11, 2017

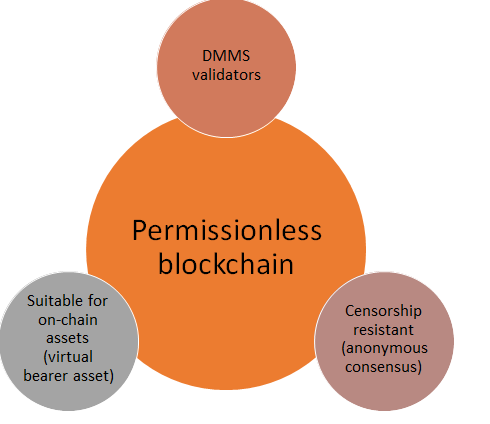
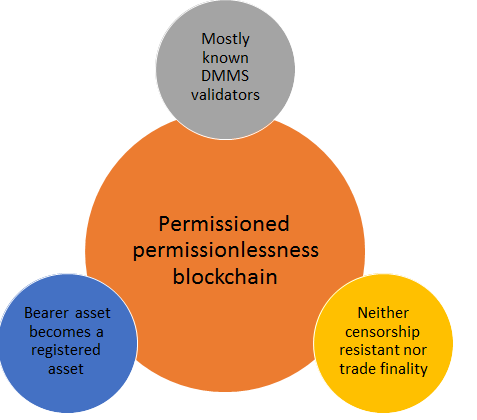
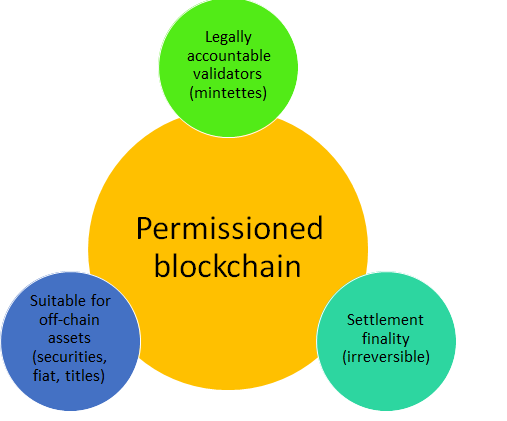
Suggested Length: 4 pages; Current Length: 19 pages (with graphics)

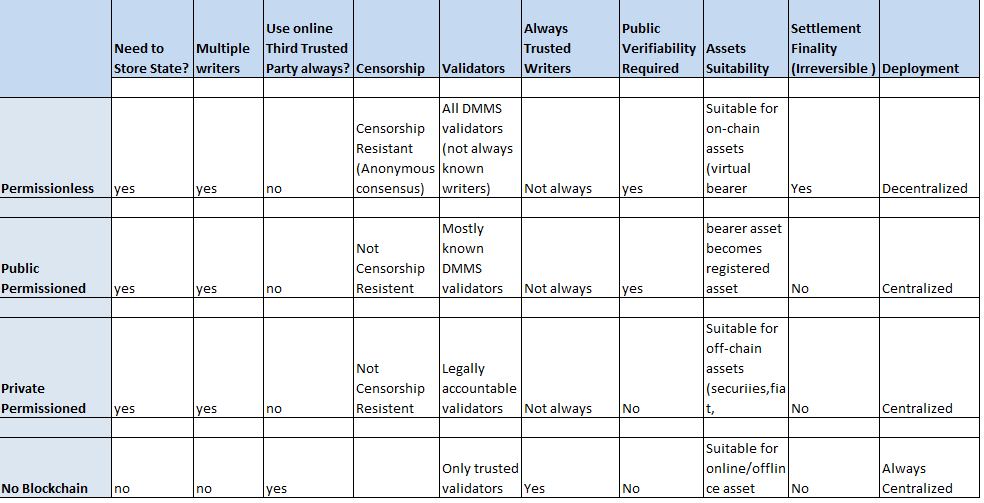
Audience: Business Owner and Government Exec

**Introduction (Suggested: 1 page) – [NEED MORE CONTRIBUTORS HERE]**

* Overall purpose and Goals [*Contributor: Jeff T*]: Blockchain is a nascent 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.
* 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 obtainment of 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?

**Assessment Overview (Suggested: 1 page)**

* Explaining Basic Principle of Assessment at a high-level [*CONTRIBUTOR: Bajinder*]
  + Federal Drivers: Overview of key federal drivers the assessment framework will need to address. Examples could be the FITARA framework that focuses on IT enterprise, OMB drivers, etc. Allowing CIOs to have an assessment framework that directly identifies issues that blockchain can solve.
* Providing links to libraries, elf-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)
* Enable people to have reference to the broader knowledge base [*CONTRIBUTOR: Sanjeev]*
  + 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.
  + 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.



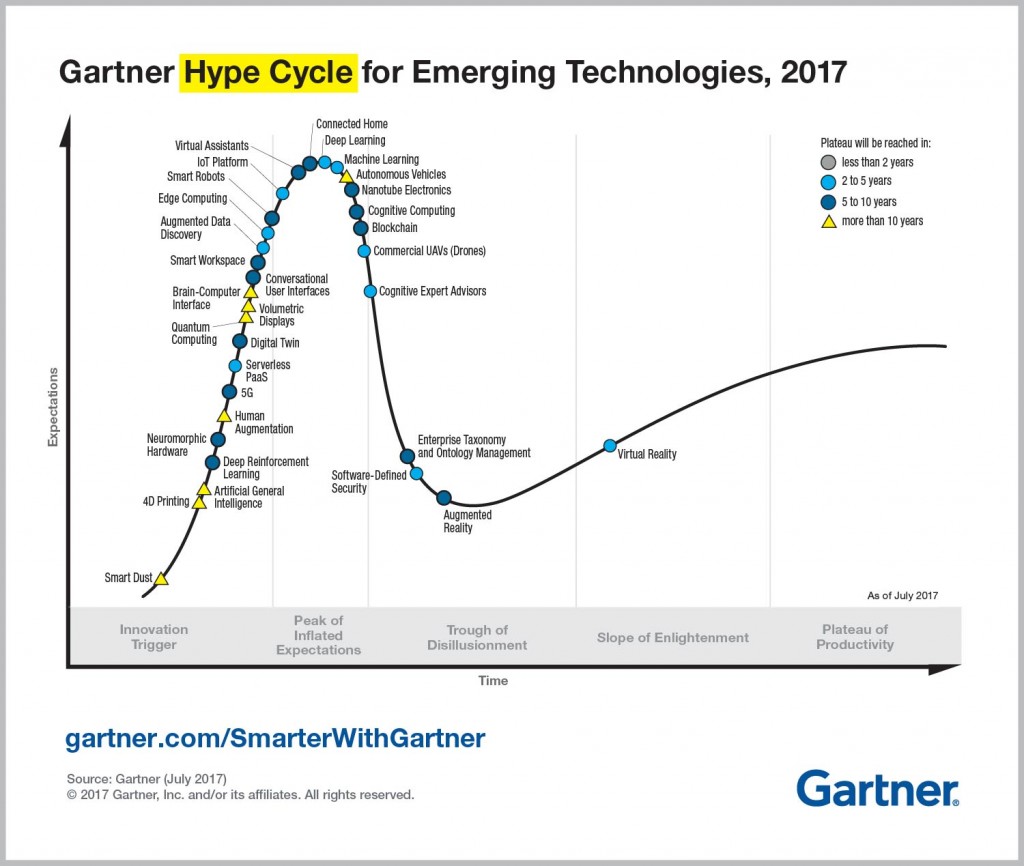
**Best Practices (Suggested: 2 pages)**

* 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*]
    - 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 MGT Act
  + Create List of Questions to Consider (needs research by all). Suggestions below: [*CONTRIBUTORS: Mark and Jeff, others?]*
    - What makes a great use case for blockchain for the business network? That it provides value to the business network (not just for one business network member) through one or more of the following:
      * Consensus; all parties agree to network verified transactions.   
        Provenance; enable any asset to be secured to a Blockchain ledger, physical or virtual.   
        Immutability; once data has been written no one, not even a system administrator, can change it.
      * Finality; once an operation is completed, that operation is completed for good.  
        Privacy & permissioned; ensure appropriate visibility; transactions are secure, authenticated & verifiable.
      * Controlled access & transformation; smart agreements on how to use the data embedded in transaction database & executed with transactions.
    - Resulting in:
      * Removing Friction
      * Getting rid of the “middle man”
      * Leveraging an Existing Business Network but not a Closed Network
      * Valuing Transparency and History of a Shared Ledger to all participants
      * Adding the Citizen/Customer to the value chain
* 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) – [NEED CONTRIBUTORS HERE]**

* Clearly define few deliverables/outcomes of the assessment
* How outcomes from assessment link to next phase - readiness

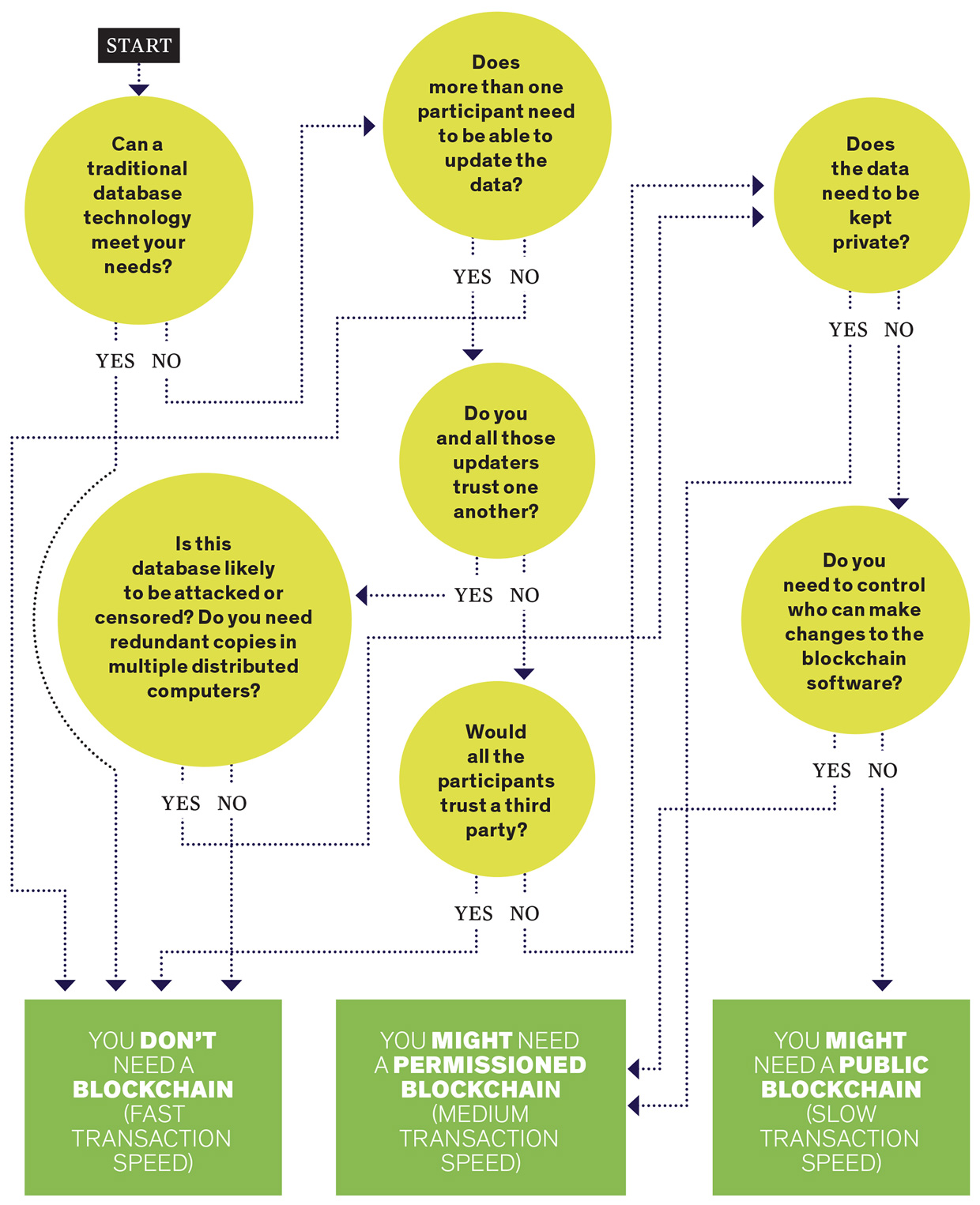
Graphics [*Contributor: Jim*]:



Do I need a blockchain?

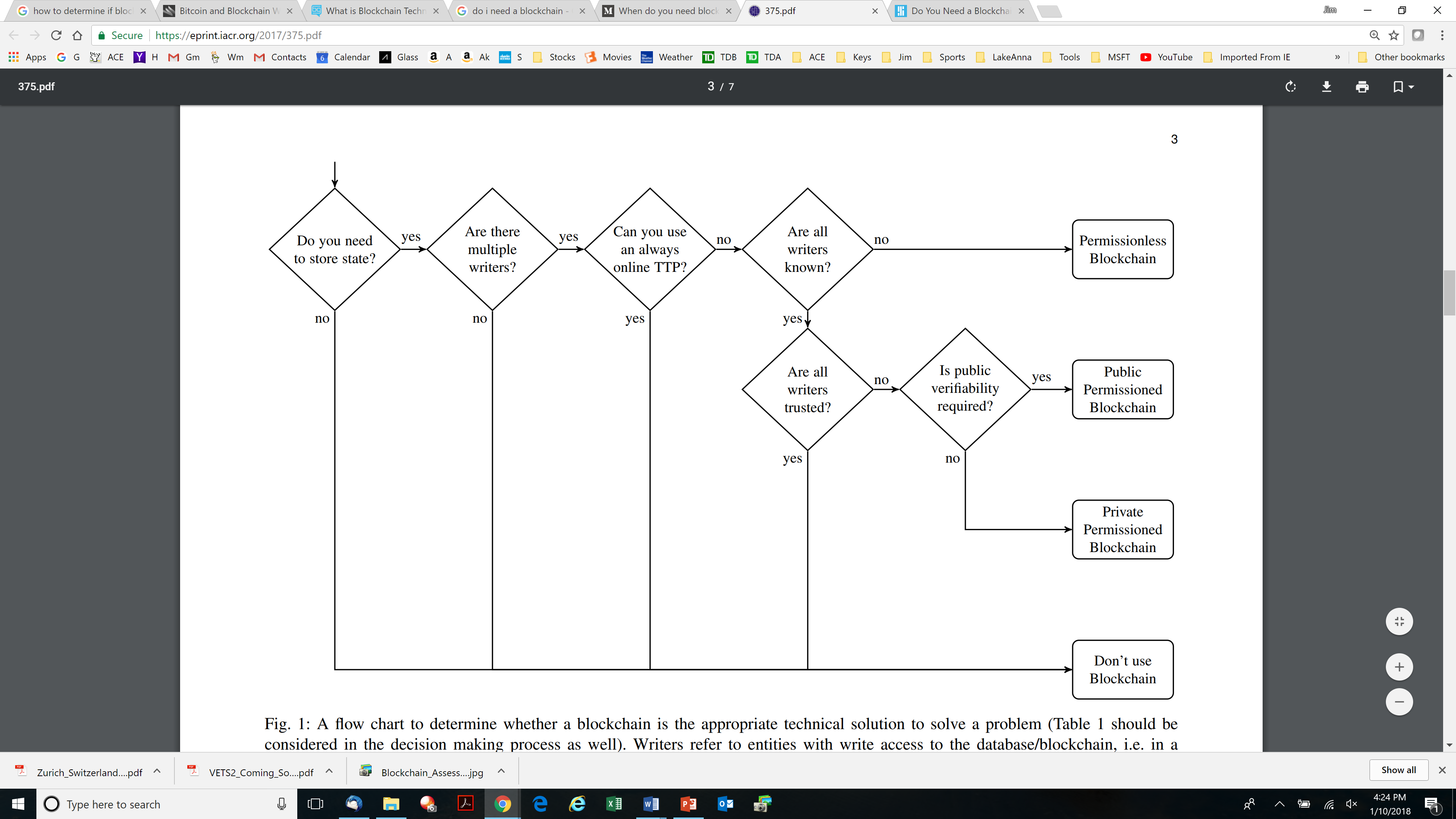
IEEE Spectrum September 2017 has a good graphic to consider:

<https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain>



From Zurich Switzerland:

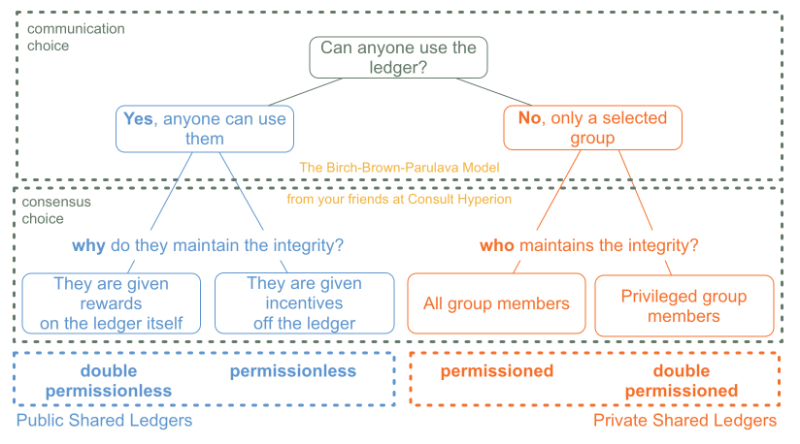
<https://eprint.iacr.org/2017/375.pdf>



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

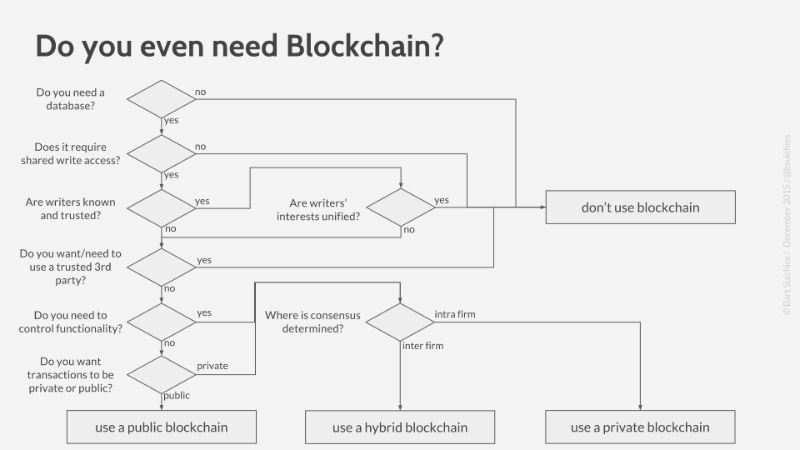
<https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1>

**Birch-Brown-Parulava model**



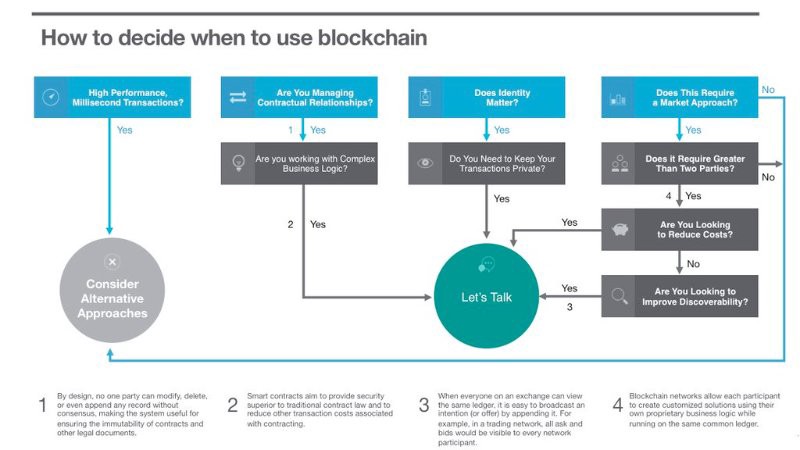
This is a good model that does not focus on the technology but on the distributed ledger concept, helpful to sort permissionless Vs permissioned ledgers out. Minor comment: it is not fully MECE because we could have a public network (“anyone can use”) maintained by a privileged group of validators (~Ripple),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

### B. Suichies Model



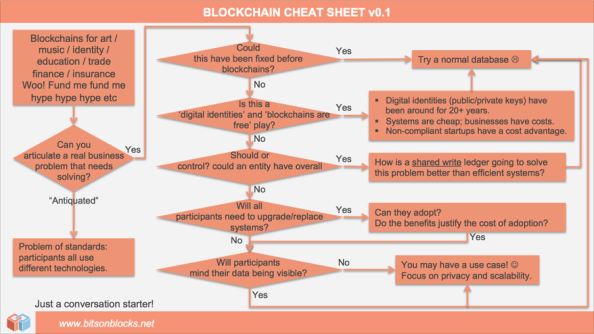
This model introduces the differences between public and private. Corda is typically an inter-firm effort building an hybrid DL platform. Personally I think an intra-firm blockchain doesn’t make sense — if in the past you couldn’t solve the reconciliation of the data shared across your group, it means 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.

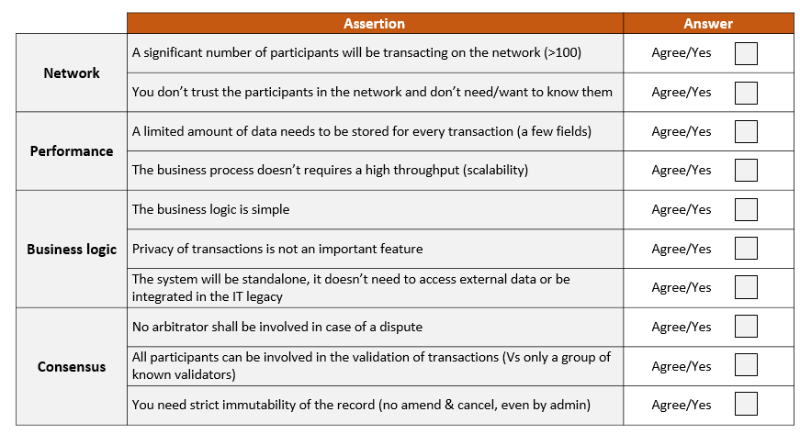
### A. Lewis model



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.