# Ethereum Vs. HyperLedger Vs. R3 Corda Vs. Microsoft COCO

# Platform Description

# Governance

# Mode of Operation

# Consensus

# Smart Contract

# Currency

# Chain Data requirements

# Operational Requirements (Service Level requirements)  
# ATO Process, FedRAMP?

Prior to selection process, the business problem and requirement must be clearly identified to ensure the appropriate blockchain platform is chosen for the business problem at hand. Blockchain is a cross-cutting and transformative technology but it is not the solution to every problem.

* **Platform Description:** Review and understand the description of the platform and ensure it matches the business need. Watch for jargons and pitfalls. For example, ‘Hyperledger Fabric can be used as a permissioned blockchain infrastructure, originally contributed by [IBM](https://en.wikipedia.org/wiki/IBM)[[19]](https://en.wikipedia.org/wiki/Hyperledger#cite_note-ibm201701-19) and Digital Asset, providing a modular architecture with a delineation of roles between the nodes in the infrastructure, execution of [Smart Contracts](https://en.wikipedia.org/wiki/Smart_contract) (called "chaincode" in Fabric) and configurable consensus and membership services.’ Note the terms ‘infrastructure’, ‘permissioned’ etc.
* **Governance:** Determine the nature of who controls and governs the software platform. For example, the Ethereum platform is completely open source and is governed by a series of developers while Hyperledger Fabric is also open-source, but governed by The Linux Foundation. The governance model of the platform determines the support structure. Traditionally the Government has opted for software that has a defined support model while some agencies have ventured into open-source in the recent past.
* **Mode of Operation**: This checklist item provides insight into what different modes can each blockchain infrastructure operates in. For example, an Ethereum platform can operate in both Permissionless and Permissioned mode, while Hyperledger Fabric can operate only in the permissioned mode. Typical use cases in the Government require the underlying infrastructure to operate in the ‘Permissioned’ mode as a ‘network peer’ has to be ‘permissioned’ to be a validating peer on the network and must have a ‘need to know’ for security reasons. There could be use cases needing a hybrid model that operates in-between the Government’s permissioned chain and the public permissionless chains.
* **Consensus**: Does the blockchain infrastructure support the type of consensus needed by the use case? In most Government situations, a Smart Contract based Proof of Work (PoW) or Proof of Delegation (PoD) consensus or Proof of Stake (PoS) are the most common needs. The consensus is almost always at the Transaction level. Of note, Department of Defense use cases with Proof of Stake consensus associated with Hyperledger is showing great promise.
* **Smart Contract**: What type of Smart Contract is needed? Do we have the resources to code the Smart Contract in the specific language supported by the platform? Do we need a Legal Framework around the Smart Contract? These are the main questions the selection process need to answer in choosing the right type of Smart Contract. This particular area is constantly evolving and evolving very fast. The Government selection should not only consider the current landscape, but should also consider the stated product Roadmap of each platform. For example, Hyperledger offers its composer tool that allows organizations to develop Smart Contracts without writing much code. R3 Corda offers a form of Smart Contract that allows for Legal jargon to be included in the Smart Contract.

The need for a legal review and acceptance shouldn’t be overlooked, especially as we delve into use cases such as Government Contracts.

* **Currency**: The initial implementations of blockchain infrastructure was limited to Digital Currency (also known as crypto-currency) and was expected to serve as digital currency and was based on the Doctor’s Thesis paper written by Satoshi Nokamoto. But, later solutions have incorporated the use of Any Asset of value. For example the Hyperledger and the latest versions of Ethereum implementations can be done around any Asset, physical or digital. Although initial use cases in the government will be around non-currency digital assets such as contracts or land deeds, as the adoption of crypto-currencies become mainstream, the Government may be forced to consider use cases around them, including having to accept crypto-currencies for Government Services.
* **Chain Data Requirements**: The Government should pay attention to **What** data will be stored within the blockchain and **How** will it be stored. For example, do we want to store the entire set of contract documents or a hash value of the location of the documents inside a Content Management System? Should we use hashes or plain text? Should the hash be SHA-256 compliant? What other meta data should be stored in each block of the chain? Experience has shown that we should limit the ‘size’ of data stored in each block of the chain due to performance concerns.
* **Operational Requirements**: Operational considerations should be taken into account when choosing the right platform. Will the system operate in a SaaS model or within the agency’s private cloud? Where are all the ‘participating nodes’ going to reside? What interface requirements have to be met? What is the response time requirements for the blockchain? Other considerations include MTBF, MTTR, uptime in addition to the standard operational requirements for any software solution.
* **Cyber Security Requirements**: A key factor in choosing any blockchain solution is to ensure its ability to obtain an Authority to Operate (ATO) with relative ease. An ATO for a blockchain environment should consider the unique nature of the potential of the peer nodes residing outside the standard system boundary. A blockchain platform operating in an already FedRamp’ed environment might be attractive as it makes getting an ATO much simpler.