Trusted Data

Understanding Distributed Ledger Technology

**TODO: add missing citations**

**TODO: streamline content to the original vision of a 20 page doc**

did cra, nrc, cbsa, jeremy, malcolm edits

November 7, 2017

**Contents**

[PURPOSE OF THIS DOCUMENT 6](#_30j0zll)

[EXECUTIVE SUMMARY 7](#_1fob9te)

[SECTION 1. DISTRIBUTED LEDGER TECHNOLOGY FUNDAMENTALS 9](#_3znysh7)

[What is Distributed Ledger Technology? 9](#_2et92p0)

[Potential Benefits 10](#_tyjcwt)

[Contrasting the types of Distributed Ledger Technology 10](#_3dy6vkm)

[Relationships 11](#_1t3h5sf)

[SECTION 2. BLOCKCHAIN CONCEPTS 12](#_4d34og8)

[SECTION 3. UNDERSTANDING THE IMPACT 17](#_2s8eyo1)

[Business, Legal and Technical Perspectives 17](#_17dp8vu)

[What does Distributed Ledger Technology enable? 17](#_3rdcrjn)

[Reducing Market Friction 17](#_26in1rg)

[Interaction Friction 18](#_lnxbz9)

[Information Friction 18](#_35nkun2)

[Innovation Friction 18](#_1ksv4uv)

[Strengths, Weaknesses, Opportunities and Threats for Distributed Ledger Technology 18](#_44sinio)

[Where is Distributed Ledger Technology being used? 19](#_2jxsxqh)

[Impacts to Business Capabilities 20](#_z337ya)

[Finance and Accounting Management 20](#_3j2qqm3)

[Marketing Management 21](#_1y810tw)

[Legal Management 21](#_4i7ojhp)

[Human Resources Management 21](#_2xcytpi)

[Procurement Management 21](#_1ci93xb)

[Contract Management 21](#_3whwml4)

[Asset Management 21](#_2bn6wsx)

[Risk Management 21](#_qsh70q)

[Information Technology Management 22](#_3as4poj)

[SECTION 4. WHEN TO CONSIDER DISTRIBUTED LEDGER TECHNOLOGY 23](#_1pxezwc)

[Difference between DLT and centralized transactional databases 23](#_49x2ik5)

[Difference between DLT and traditional server architecture 24](#_2p2csry)

[DLT Decision Matrix 24](#_147n2zr)

[SECTION 5. PUBLIC SECTOR EXPERIMENTATION 27](#_3o7alnk)

[Canadian Governments 28](#_23ckvvd)

[Strategic 28](#_ihv636)

[Experimentation 29](#_32hioqz)

[Execution 32](#_1hmsyys)

[SECTION 6. PATH TO ADOPTION 32](#_41mghml)

[Experimentation 32](#_2grqrue)

[Experimentation Framework for Disruptive Technology 33](#_vx1227)

[General View of Architecture Elements 33](#_3fwokq0)

[Barriers to Adoption 35](#_1v1yuxt)

[Lack of mature tools 35](#_4f1mdlm)

[Understanding the choice 35](#_2u6wntf)

[Open Source 35](#_19c6y18)

[Market Correction 36](#_3tbugp1)

[Lack of Standards 36](#_28h4qwu)

[SECTION 7. CONSIDERATIONS FOR THE GC 37](#_nmf14n)

[POLICY Considerations 37](#_37m2jsg)

[Recourse 37](#_1mrcu09)

[Smart Contracts 37](#_46r0co2)

[51% Attack Problem 37](#_2lwamvv)

[Know Your Customer 37](#_111kx3o)

[BUSINESS Considerations 37](#_3l18frh)

[Legacy Business Processes 37](#_206ipza)

[Legal Code Vs Technical Code 37](#_4k668n3)

[Business Relevance 37](#_2zbgiuw)

[Innovation 38](#_1egqt2p)

[Environmental 38](#_3ygebqi)

[ARCHITECTURE Considerations 38](#_2dlolyb)

[Foundational Architecture Elements 38](#_sqyw64)

[Application Programmable Interfaces 38](#_3cqmetx)

[Reduce Lock-In 38](#_1rvwp1q)

[Architectural Patterns 38](#_4bvk7pj)

[Scalability 39](#_2r0uhxc)

[Performance 39](#_1664s55)

[Emerging Technologies 39](#_3q5sasy)

[INFORMATION Considerations 39](#_25b2l0r)

[Knowing Your Data 39](#_kgcv8k)

[Understanding Of Immutability 39](#_34g0dwd)

[Big Data 39](#_1jlao46)

[Open Data 40](#_43ky6rz)

[Data for New Services 40](#_2iq8gzs)

[Costs for Data 40](#_xvir7l)

[APPLICATION Considerations 40](#_3hv69ve)

[Understand the Business Context 40](#_1x0gk37)

[Design 40](#_4h042r0)

[Legacy 40](#_2w5ecyt)

[Data Centre Storage 40](#_1baon6m)

[Reconciliation 40](#_3vac5uf)

[TECHNOLOGY Considerations 40](#_2afmg28)

[Assessing DLT Platforms 40](#_pkwqa1)

[OSI Model 41](#_39kk8xu)

[Open Source 41](#_1opuj5n)

[SECURITY Considerations 41](#_48pi1tg)

[Vectors of Attack 41](#_2nusc19)

[Response to Threats 42](#_1302m92)

[Anonymity 42](#_3mzq4wv)

[PRIVACY Considerations 42](#_2250f4o)

[Policy Changes 42](#_haapch)

[Read Access 42](#_319y80a)

[Consent 42](#_1gf8i83)

[SECTION 8. RECOMMENDATIONS 43](#_40ew0vw)

[DISTRIBUTED LEDGER TECHNOLOGY CONCEPTS AND TERMS 44](#_2fk6b3p)

[General Concepts 44](#_upglbi)

[Key Capabilities of Distributed Ledgers 45](#_3ep43zb)

[System organization 46](#_1tuee74)

[Types of DLT System 46](#_4du1wux)

[Consensus 47](#_2szc72q)

[Roles 47](#_184mhaj)

[Applications & Services 48](#_3s49zyc)

[Acknowledgements 50](#_279ka65)

[References 51](#_meukdy)

# PURPOSE OF THIS DOCUMENT

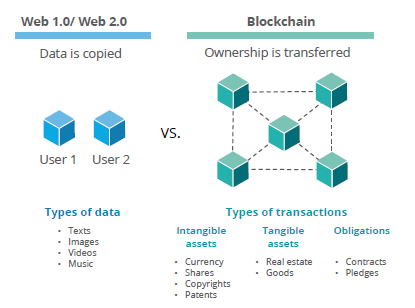
The development of whitepapers is one of the Pre-Strategy collaboration activities identified within the Government of Canada (GC) IT Operating Model for Disruptive Technology. This whitepaper provides the foundational understanding of Distributed Ledger Technology (DLT), the impact and potential of DLT toward GC services, a status update on GC activities pertaining to DLT and recommended next steps for the GC.

The objectives of the whitepaper are to avoid duplication of effort within the GC, maximize the use of GC resources, and increase awareness and knowledge of DLT.

The GC community is encouraged to perform the following if they are considering a DLT experiment, proof-of-concept (PoC) or DLT adoption:

1. Review this document to ensure a common understanding of the fundamental concepts and terms for DLT.
2. Identify if your DLT effort is aligned to the recommendations identified in this document.
3. Consult the GC Experimentation Framework for Disruptive Technology if you are proceeding with a DLT experiment.
4. Engage the GC Blockchain Working Group for awareness and knowledge transfer.

# EXECUTIVE SUMMARY

Over the past 20 years the Internet has become the backbone for furthering communication and the open sharing of information for people across the globe. It broke down physical geographic boundaries and created a new connected community. Distributed Ledger Technology (DLT) represents a shift in authority and rule enforcement from central institutions to the broader edge of networks. DLT is not just a new way of further leveraging the benefits of the Internet but it makes us revisit the fundamental norms associated to the transfer of assets and value that have been followed for hundreds of years. It challenges how the rules and control of value are defined and followed. DLT shifts the perceived power of trust from singular institutions with varying levels of transparency; such as banks, corporations, and governments to a more transparent and broadly distributed network and a community that is not bound by geography. Decisions require a combination of trust and rules. Trust is enabled by cryptographic proofs and is maintained and have rules enforced by a network of trusted computers that ensure its security unrestricted by borders.

In essence, the adoption of DTL technologies represent a further step in codifying transparency, trust and integrity into the daily activities of the Government of Canada (GC). It provides new and efficient ways to show evidence of the relationships, goals and target outcomes that the GC has committed to action and provides evidence of progress. The GC has made progress with its Open Government initiatives; however DLT provides an opportunity to further the goals of increased transparency and collaboration.

The general public has come to use Internet terms within their everyday language including terms like websites, browsers, HTTP and HTML. Segments of the public have been introduced first to terms like Bitcoin and then blockchain. The common language will soon be expand further to include terms like distributed ledgers, smart contracts, consensus algorithms and digital wallets. We have become accustomed to using the internet and web browsers to search for products and services and we could soon be accustomed to searching for verification of digital ownership of assets and value.

Digital trust is enabled by trustworthy data. In order to deliver certain higher value digital services we need to strengthen how we verify the digital identity of a person or if the verified person is related to a digitally identifiable organization. True decentralization would allow people to own their identity and related information, and to control access to, and sharing of, this information. DLT instills trust by ensuring that digital events are witnessed by all users in the network, by having data approved by consensus, and by storing the events in a database that cannot be altered by a single malicious actor. Secure, distributed, and non-alterable records provide a shared truth.

DLT offers the GC new choices in how it could interact with Canadian citizens and its partners. Listing what problems DLT could solve for the GC is not the lone question. The GC will approach DLT by understanding the risks, considering what problems can be solved, exploring opportunities for the GC and its partners and enabling DLT capabilities by experimenting with various deployment models and platforms.

The GC cannot get the full return benefits of DLT by itself, and it must be willing and able to collaborate with citizens, suppliers, and partners in new ways. GC can embrace DLT for its socially beneficial opportunities and invest in planning and experimentation to better understand and manage any risks. It is hard to predict or create disruptive innovation; however failure to assess DLT can place Canada behind its economic partners as they act to leverage DLT and its strengths of an open, inclusive and accountable economy. The GC must understand the differences between current and future technologies in order to ensure it is positioned to deliver maximum business value.

# SECTION 1. DISTRIBUTED LEDGER TECHNOLOGY FUNDAMENTALS

## What is Distributed Ledger Technology?

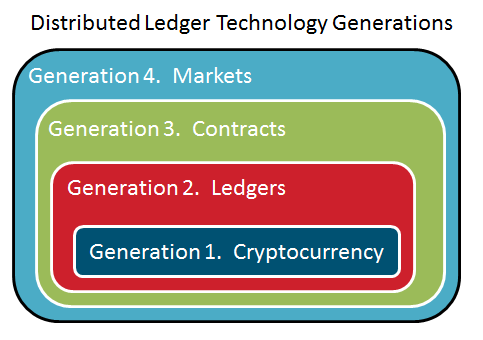
A DLT in common terms provides the ability for members of a network to store and access information, or records, as a list of transactions that are replicated across a number of computers, rather than being in a central database. A DLT has the following themes:

* Contains transactions of value exchange
* Replicated across a number of systems in almost real-time
* Usually exists over a peer-to-peer network
* Uses cryptography as a means of storing assets and validating transactions
* Use digital signatures to prove identity, authenticity and access
* Can be written by certain participants
* Can be read by certain participants
* Designed to make it hard to change historical records
* Capable of operating without a central validator

Distributed Ledger Technology (DLT) has the potential to be an engine for trust-based services where just as you search the Web for information you may be able to check and verify the authenticity of transactions, data, processes, events or many things that you could do in a Web Search. DLT services are likely to replace or augment many established intermediary services and become new sources of authoritative data.

It is important to first discuss DLT in the context of business fundamentals before diving into the technical details. We must start with the understanding that distributed ledgers are structures that enable parties who don’t fully trust each other to form and maintain consensus about the existence, status and evolution of a set of shared facts. DLT has the potential to replace established decision makers, or intermediaries, as a single central authority decision maker and replace it with a new approach for reaching consensus. DLT builds upon the centuries old business concept that networks connect people and organizations together, all participants in a network have identities, transactions describe the exchange of assets in the network, contracts are the rules that structure transactions and a ledger is the record of all transactions made within the network. What is new with DLT is reliance on cryptographic mathematics and computer algorithms to arbitrate and choose between competing possible versions of a ledger, and as a result all participants end up with one leger they can all agree as having been created according to the rules.

The first generation of DLT were focused on cryptocurrencies such as Bitcoin. The second generation is presently happening and it leveraged the decentralized applications to programmatically control the exchange of value across parties. Future generations are expected to see greater prevalence of smart contracts, architectures and consensus models that are optimized to different (non-currency) use-cases and entirely new forms of organization that could have DLT at their core.



**Figure 2: Evolution of Distributed Ledger Technologies**

### Potential Benefits

1. Cost savings – DLTs are more expensive than central databases, but may realize savings indirectly by disintermediating central parties and eliminating data indirection

2. Speed – DLTs follow automated rules that can clear and settle cash and other assets without human intervention. This increases speed but removes discretion

3. Transparency – providing the right information to the right people within the network

4. Access – more equitable access to information

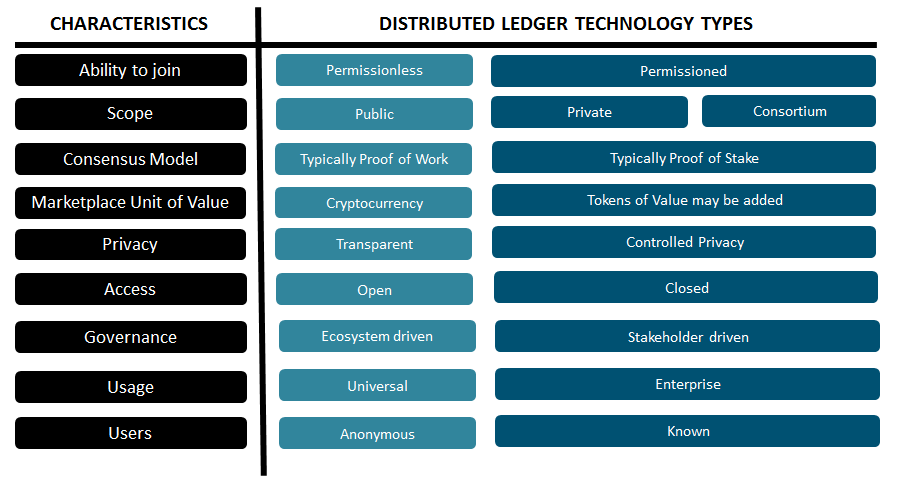
5. Productivity – more work output

6. Efficiency – faster processing or reporting of transactions

7. Quality – Automation of rule enforcement with fewer errors and greater access to the same data

8. Outcomes – enhanced trust in governance, business growth and innovation

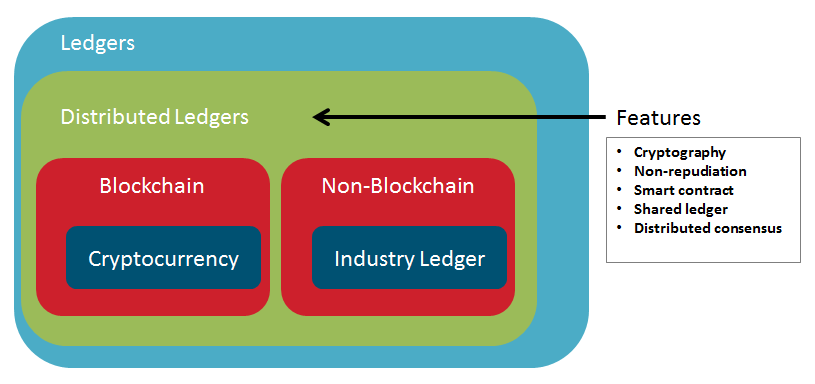
### Contrasting the types of Distributed Ledger Technology

The type of DLT that an organization selects will be an evaluation of multiple criteria. The table shows that Permissionless DLTs provide a much higher level of distribution and sharing which results in more nodes in the rule enforcement process, whereas Permissioned DLTs inherently have a higher degree of trust since the nodes are known and may be pre-determined, in addition to controlling what data is actually shared to identified parties.

**Figure 3: Distributed Ledger Technology Comparison**

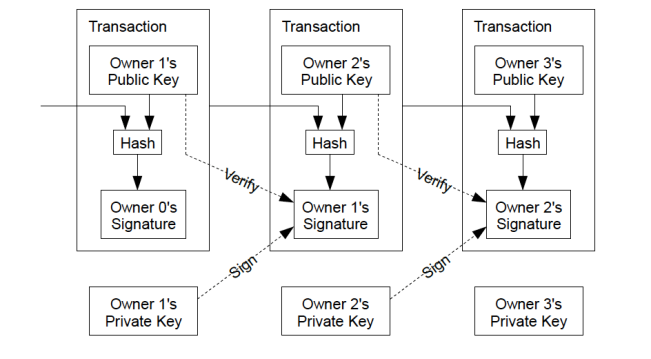
DLT is identified as having two costs which could influence the rate and direction of innovation – the costs of verification and the cost of networking. (<http://ide.mit.edu/publications/some-simple-economics-blockchain>). DLT is seen as an enabler to a new marketplace that has increased competition, lower market friction, and avoiding central authority being in the hands of single operator. The type of DLT that is selected could influence the types of benefits that will be realized. There isn’t a one size recommendation for selecting a DLT and the selection should be based upon the desired business outcomes and requirements.

### Relationships

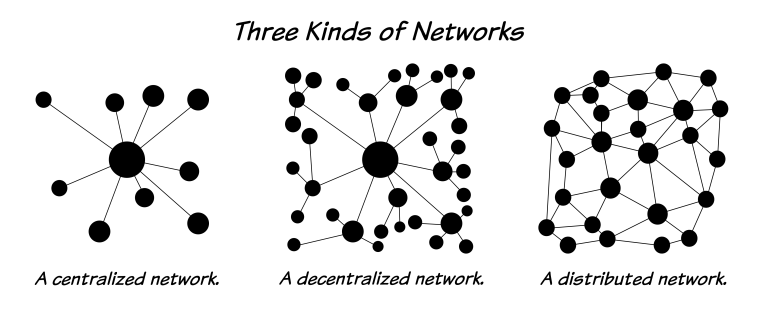
In order to fully understand the DLT ecosystem it is an imperative to understand the hierarchical relationship of ledgers. For instance, not all DLT’s are blockchains and nor do they all have the exact same characteristics as blockchain based solutions. The Distributed Technology Ledger Comparison table in the previous section shows some of these distinctions. Bitcoin would be an example of a cryptocurrency that is a blockchain type of distributed ledger. The R3 Corda project would be an example of a non-blockchain type of distributed ledger. One of the distinguishing traits is between a blockchain solution and a non-blockchain is that parties stay in sync at the transaction level versus at a block of transactions. (https://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwjpooy3ya3XAhXj7IMKHXblDK4QtwIIMjAD&url=https%3A%2F%2Fvimeo.com%2F230670985&usg=AOvVaw0ecPWHqKKk\_qDU7X51V\_Lr)

**Figure 4: Relationship of ledgers**

# SECTION 2. BLOCKCHAIN CONCEPTS

***Blockchain*** is a type of distributed ledger technology in which confirmed and validated sets of transactions are held in ***blocks***, and the blocks are chained together in a way that makes tampering difficult and allows a participant only to append additional blocks in a sequential way. Thus, each chain starts with an original, or ***genesis block***, followed by a time ordered sequence of blocks, wherein each block contains a **hash** of the prior block in the chain as well as the information in the current block. This forms a long continuous chain of hashes, hence the name blockchain (see Fig. 1). The length of the blockchain is referred to as its ***block height*** (i.e., the distance between the genesis block and the last block in the chain). In some blockchains, when the chain becomes quite long, it is shortened into a ***Merkle Tree***, where the root of the tree is the hash of all previous transactions. This allows storage space to be saved without breaking the integrity of the chain. When the continuous chain splits into two (e.g., when there is a change in the blockchain protocol or software) the blockchain is said to have ***forked.***

Each block consists of a set of ***records*** of ***transactions*** that form a ***ledger***. In this sense, blockchains are ***records systems***, which can be used to keep track of financial or other types of transactions. Records of transactions within the blocks represent a series of recorded actions often involving a unit of value (e.g., a unit of ***cryptocurrency***, referred to generically as a ***coin***) or an asset (a representation of land or other asset, sometimes known as a ***token***) that result in changes in the state of that unit of value or asset (e.g., a payment or a transfer of ownership). Records of transactions are created by taking input information about the unit of value or asset and ***digitally signing*** it to produce a hash which is recorded on the blockchain. 

Records of transactions are broadcast out through a ***distributed*** ***peer to peer mesh network*** of nodes (see Fig. 2). This is why blockchain technology is often described as a ***distributed ledger***. The nodes that operate as part of this distributed network, in theory, are unlimited in number and can operate from any location. Each node usually retains a complete copy of the ledger, though some nodes retain only a partial copy of it, such as ***light nodes***. Light nodes are nodes that trust a full node with a complete copy to keep it updated. The copies of the ledger kept on each node should all match exactly. 

**Figure 6: Three kinds of networks (TechGuru, 2017)**

Nodes in the network collect records of transactions into blocks, which are then put into a Merkle tree. The hash of a block is actually the hash of the block header, a piece of data that also contains a ***timestamp***. The timestamp establishes the sequential order in which each block enters the blockchain, but is not sufficient to link the recording of the block with the calendar date associated with its creation. To establish such link, some blockchains also publish block hashes to public newspapers so that is it possible to later validate the calendar date on which a block was recorded.

When a block is finalized, it is chained together with previous blocks. Blocks are chained together by cryptographically combining all of the transactions within a block, the header of the block, and the signature of the previous block, into a cryptographic signature of this block. This block and its signature are then broadcast to the network, which verifies the transactions and the signatures. Sometimes, different parts of the network could add different blocks at about the same time, or transactions in different orders. When this happens, nodes in the network must choose which blocks(or transactions)to keep. This choice is determined by the blockchain’s consensus mechanism.

The consensus mechanism is an algorithm designed to ensure that updates to the blockchain are agreed and communicated across the entire network in a transparent manner, that the order in which records of transactions entered the blockchain is undisputed and that any changes to what has been written to the ledger will be detectable. Once written to the blockchain, records of transactions are meant to be immutable. There are many different types of consensus mechanisms used by blockchain and distributed ledger systems. A simplification of consensus mechanisms is to think of nodes voting on what data should be replicated across the network. To stop a malicious node from dominating the vote, nodes either vote by demonstrating a scare or valuable resource (computational work, holdings of the currency, etc) or the list of nodes is controlled by a manager and a traditional fault tolerant algorithm is used.

Each of these consensus mechanisms incentivizes the nodes on the network to behave slightly differently depending on its ***reward or incentive mechanism***. A reward or incentive mechanism is a consideration (such as a payment) given to a party for undertaking some activity within the blockchain system. An example of such activity is the work involved in running the consensus mechanism, as in the Proof of Work consensus mechanism. In the case of the Bitcoin network, nodes – called ***miners*** - involved in this work – called ***mining*** – receive a payment in Bitcoin for performing the Proof of Work. This reward incentivizes the miners to validate and secure transactions on the Bitcoin network. Once validated by means of the ***consensus mechanism***, each node receives an update to its copy of the ledger.

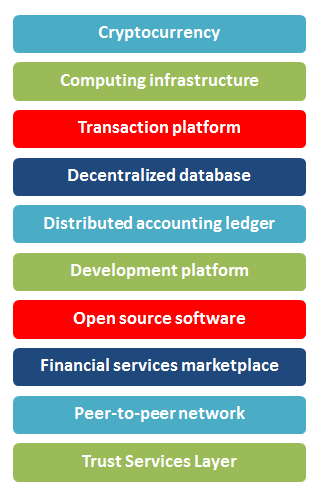
In blockchains that record financial transactions, for example, this might reflect that a certain amount of value, or coin, has been deducted from the value attributed to one ***wallet*** and added to the value attributed to another wallet. Wallets are actually just addresses on the network. These addresses are denoted by the hash of a ***public key*** - a hash that functions somewhat like an IP address indicating the destination of a particular transfer of value. For each public key there is a matched ***private key***, which unlocks the wallet. The person who holds the private key controls the wallet and the assets in it. When individuals want to transfer value to someone else’s wallet, they must use their private key to digitally sign the transaction in order to give effect to the transaction. Since there is nothing inherent in the operation of the blockchain that links a person’s real world identity to their public or private key pairs, blockchains are said to operate ***pseudonymously***. Just like the early days of the Internet, this ability to appear to be anonymous has made blockchains (e.g., Bitcoin) popular with those involved in criminal activity who desire to make and receive payments without detection. The association with criminal activity has led many to eschew the use of blockchain technology. Now, however, law enforcement agencies can use special techniques to link public keys to individuals’ real world identities in order to combat criminal use of blockchains. In addition, not all blockchain implementations are used to make payments nor do they all not rely on the use of cryptocurrency to record transactions. These types of blockchains are said to be ***tokenless.***



**Figure 3. Transaction processing using public-private key pairs on the blockchain**

In addition to being distributed systems with many dispersed components, some blockchains (i.e., public blockchains) operate as ***decentralized*** systems; that is, nodes do not operate under the control of a centralized server, but in an independent albeit coordinated manner. These blockchains may also be characterized by decentralized governance; that is, they may not operate under the formal authority of a single person or organization (even though groups of individuals or organizations may wield informal control over their operation). Examples of these types of blockchains include Bitcoin and Ethereum. Other blockchains and distributed ledgers operate under the control of a single authority (e.g., Ripple, Guardtime) or the authority of a consortium (e.g., R3).

There are multiple dimensions by which blockchains can be described. Some of the optional characteristics by which they can be described are the following. Blockchains (and distributed ledgers) may be ***public*** or ***private***, ***permissioned*** or ***permissionless***. Public blockchains are those that any ***participants*** may use and access. Public blockchains are often permissionless; that is, participants do not require special authorization or ***authentication*** to access, read, write and be participants in transactions and in the consensus process. ***Permissioned*** blockchains, on the other hand, are ones in which nodes must have a member identity and participants must have authority and authentication to access. These are often private blockchains, meant for the use of only members of a ***shared ledger***, a single ledger that multiple participants may access and use. Permissioned blockchains have ***membership services*** that manage the identity, privacy, confidentiality and auditability within the blockchain system.

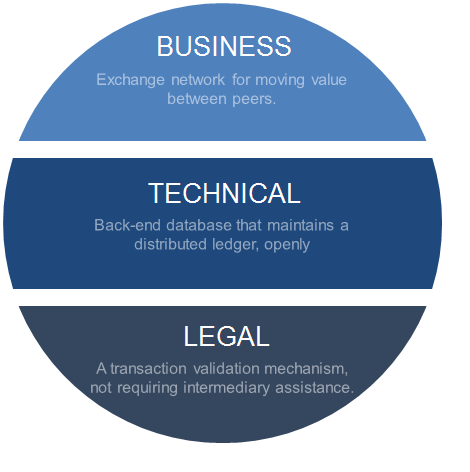
Blockchains are said to provide ***transparency*** and ***traceability*** (e.g., the ***provenance*** of an asset such as an artwork) because it is possible for participants to read the information (e.g., hashes) recorded on chain. Even though public blockchains are said to be transparent, they may also support privacy through the use of cryptography to keep information secret unless the person(s) who control(s) that information agrees to release it. 

As use of blockchain technology has expanded, new applications and services have emerged. ***Blockchain applications***, for instance, run over blockchain networks and permit participants to easily interact with these networks. ***Smart contracts*** (also termed ***chaincode***, ***programmable asset*** or ***programmable contract***) are blockchain applications that express logic associated with a transaction and execute on a blockchain platform. Smart contract code determines what transactions are recorded into the blockchain and the information they will contain. Through the use of smart contracts, their proponents claim that many kinds of contractual clauses may be made partially or fully self-executing or self-enforcing, or both. In this sense, smart contracts represent a digital means to administer and enforce digital property rights. Note, however, that the outcome of a smart contract may or may not be legally binding. ***Inter-blockchain services*** enable smart contracts to operate across ***blockchain platforms***. ***Oracles***provide a trusted service designed to supply external data to a smart contract or blockchain system. ***Asset registries*** link digital currencies to other assets or records on top of a distributed ledger. Asset registry applications are often termed a “ledger within a ledger”, meaning that a (distributed) ledger is embedded within the ledger dealing with the assets and parsed independently. ***Off-chain access services*** provide secure means to access capabilities outside a blockchain system, such as trusted data sources or functions. ***Sidechains*** are separate blockchains associated with a main blockchain and can participate in transactions with it, typically in both directions. In contrast, ***subchains*** are logically separate chains that form part of a blockchain (Also known as a ***channel*** in the Hyperledger blockchain). Each subchain may be owned by a different entity and may be accessible to a different set of users. Nodes may be set up so that some nodes participate in certain subchains and not in others. The result of this configuration is that the ledger on some nodes contains transactions for that subchain while the ledgers on other nodes do not.

The design and method of operation of blockchains is intended to solve an important problem: the problem of trust. Trust is necessary in any form of interaction. Through cryptographically securing records and distributing copies that can be compared, it is possible to protect and validate the integrity of records as one of the key elements necessary to be able to trust them. Trusted records are an important foundation for other types of trust, such as the trust between citizen and state, business counterparts, or communicating system components. This ability to provide a foundation for trust is what sets blockchain technology apart from other information processing technologies and makes it a unique innovation as well as an especially important one.

# SECTION 3. UNDERSTANDING THE IMPACT

## Business, Legal and Technical Perspectives

In William Mougayar’s book The Business Blockchain he identifies that the capabilities that blockchain represents can be viewed through three lenses: *technical, business and legal*. He also identifies that we need to stop thinking of the blockchain as just a product in itself and to think of it as a core element within a greater whole of products and services that exchange assets and value. If you only look at DLT as a technology then you may lose sight of it as a business change enabler, and if you ignore the legal aspect then you may feel empowered by its governance characteristics.



## What does Distributed Ledger Technology enable?

In Gartner’s research paper The Disruptive Potential of Blockchain Technology May 2017, they include the concepts of DLT enabling items such as:

* Dynamic, self-organizing markets on demand
* Peer-to-peer approaches
* Transaction entities bundled with rules or programs
* New forms of value exchange through smart objects with self-enforcing contracts
* Emergence of new markets in bottom-up fashion

## Reducing Market Friction

The transparency of information that DLT represents has the potential to eliminate the frictions that traditionally challenge the GC and its partners in the exchange of assets. Some examples of frictions can represent the need to comply with regulations, duties and taxes that must be applied to good and services, or the inability to access information in a timely manner.



**Figure 10: derived from IBM Institute for Business Value**

### Interaction Friction

Interaction Friction is when the cost of a transaction is too high or the degree of separation between parties is too great.

### Information Friction

Information Friction is when information is not equally shared, not accessible, or technology risks occur related to the management of information.

### Innovation Friction

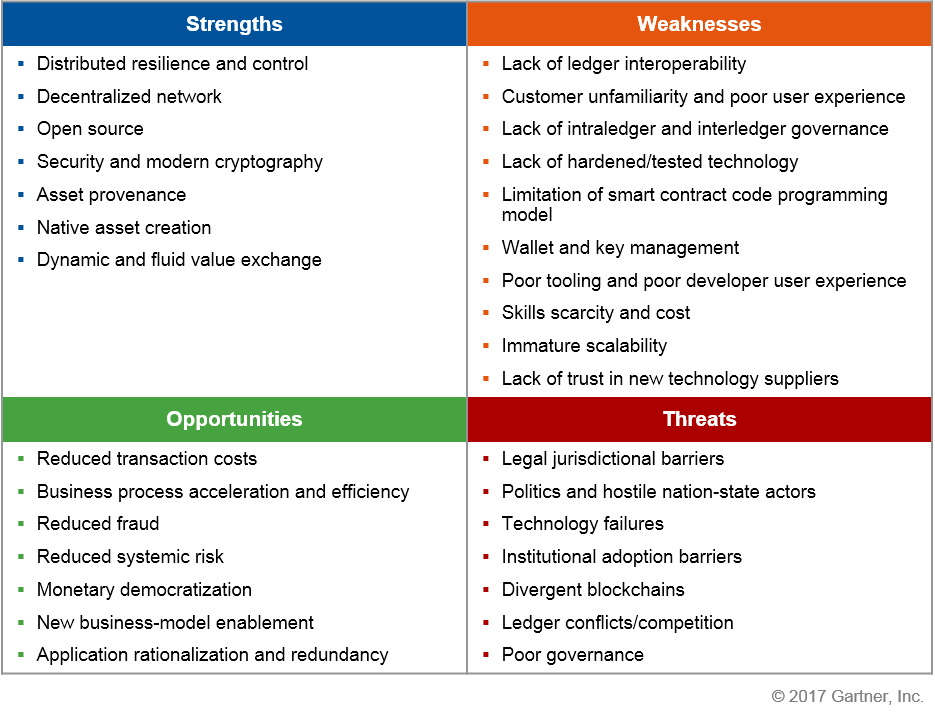
Innovation Friction is any condition that compromises an organization's ability to respond to market changes.

## Strengths, Weaknesses, Opportunities and Threats for Distributed Ledger Technology

Canada has developed robust institutional systems where banks, governments and a strong legal framework serve as trustworthy intermediaries for many of the critical purposes and use cases that DLT could represent. Many of these capabilities are interdependent and mutually supportive. Therefore, there are costs and benefits of displacing these capabilities that are difficult to analyze on a stand-alone basis.

A measured approach must be taken to understand and balance the current reality of DLT maturity, the potential for divergent solutions that are not interoperable, and capturing opportunities for innovation.

The Gartner SWOT Analysis on Blockchain can be used as a starting point for further assessing DLT. For example, in a broader analysis of DLT having resilience as a Strength for public ledgers should be revisited, the lack of standards should be placed as a Weakness, and concerns regarding the pace of policy keeping up with the technology should be listed as a Threat.



**Figure 11: Gartner SWOT Analysis of Blockchain**

## Where is Distributed Ledger Technology being used?

The book The Business Blockchain outlines a simple method to identify the various areas that DLT can impact. The book identifies the acronym ATOMIC which refers to the various programmable concepts that DLT can influence.

* **Assets** – digital assets can be created, managed, and transferred using DLT
* **Trust** – rules can be inserted into transactions to represent trust and validation by the network instead of a central authority
* **Ownership** –timestamping of documents that are cryptographically secure represents irrefutable proof of ownership
* **Money** – provide a means to make payment in exchange for the value for good and services
* **Identity** – move beyond document based evidence for identity
* **Contracts** – insert business logic to manage the conditional flow of enforcing agreements

The concepts contained within the ATOMIC acronym are a helpful reminder when considering DLT relevance. Bitcoin and blockchain are the most common usages of DLT and they have become known as opportunities for cryptocurrencies and the financial sector, however DLT can address a broader range of requirements as shown in the following diagram (Figure 9).



**Figure 12: Use cases for distributed ledger technology**

# Impacts to Business Capabilities

DLT disrupts and redefines the commonly accepted beliefs on trust. It provides a transparent trust layer that can lead to the earlier identification of warning signs of potential issues thereby providing a means to distribute and reduce risk. DLTs do not eliminate trust and are seen as shifting where trust resides. Centralized trust intermediaries may actually be more divisive versus a distributed approach that requires the community to come together. DLT isn’t just about replacing intermediaries - it is also about creating new ones. DLT could influence the transformation of business models and how the GC approaches its own business capabilities.

## Finance and Accounting Management

* + The financial information representing the value of an enterprise can be discovered in near real-time if it is placed on a public blockchain, thereby increasing the level of transparency and potential for stakeholders or reviewers to identify concerns.
  + An enterprise will be able to invest less in validating a user’s identity and they will have a guarantee to receive funds, thereby reducing efforts to manage delinquent accounts.

## Marketing Management

* + If people place their identities and profiles on a blockchain with open consent for enterprises to discover their profiles then this can result in new approaches for targeted marketing and understanding user behaviours and their online journey.

## Legal Management

* + Parties can enter into binding agreements where the contractual terms can be initiated and enforced through software, thereby automating agreements and enforcing commitments that have been made.
  + The transparency of enterprise activities on the blockchain can eliminate the need for individual attestations to verify statements.
  + Legal authorities will be required to determine which party has the responsibility to address malicious activity that occurs within a DLT network that Canada has joined but has malicious activity occurring external to Canada.

## Human Resources Management

* + If individuals have the ability to manage their own identities on a blockchain then they can provide consent for it to be queried during staffing processes. For example, the educational credentials of a candidate can be verified as a digital query to a blockchain instead of requiring paper based evidence to be presented and then copied.

## Procurement Management

* GC procurements related to DLT will have a lack of standards to reference within the procurement statements, which may result in the GC either being too prescriptive or too vague in its requirement definitions.
* The open source DLT projects which could become core elements of GC services have varying levels of documentation available. This will directly impact the ability to effectively assess procurement bids.

## Contract Management

* + The ability to meet contractual requirements for deadlines or task completion can be more visible with blockchain and the performance history is recorded on a blockchain for others to validate reputation and trust. This transparency can be an incentive to ensure positive performance management by the service provider.

## Asset Management

* + Visibility into the trusted recording of what is being transacted or transferred can introduce greater awareness of the inventory of assets thereby emphasising attention to reduce duplication and unwarranted investments.

## Risk Management

* + DLT requires the need to redefine the relationships between the GC and existing partners which may introduce change to current processes.

## Information Technology Management

* + If identities are managed within a blockchain then this reduces the enterprise costs of storing user profiles and it reduces privacy risk in storing the data.
  + Transactions on a blockchain have audit capabilities inherently embedded within the blockchain, therefore changing the way how business applications need to be designed.

# SECTION 4. WHEN TO CONSIDER DISTRIBUTED LEDGER TECHNOLOGY

## The value of DLT

While there is much hype about the “distributed” part of DLT, the real innovation lies in the “Ledger” and the protocol value that a distributed ledger allows. Prior to DLT, we had created digital goods –such as documents, music, videos, etc... One useful thing about digital goods is that they can be copied as many times as we want, and distributed at almost no cost.It is technically impossible to identify “the”authentic original of an electronic document unless it is directly and completely coupled to the original source of production. If I take an “original” document and sell it to you, nothing stops me from keeping a copy for myself, or selling exactly the same “original” to some third party–the so-called “double spend” problem. As a result, until the invention of DLT,it has not been possible to create and distribute unique digital assets, and it has been almost impossible to sell them for any value without incurring significant cost to protect against piracy. Many digital goods are just given away for free because it would cost too much to secure them against piracy. Without DLT, the best we have been able to do is to distribute and control access or decryption credentials, using Public Key Encryption or central registries.However, this has limited use because it is difficult for me to transfer my asset to you, without the permission of the original issuer: either I have to give you my private keys(which I can then give to multiple parties), or I have to allow the issuer to revoke my access in favour of yours.

With DLT, the rights are recorded in the ledger, and there is no central party whose permission I must seek to transfer some or all of my rights to you, under conditions of my choosing. This has created the possibility to have unfettered transfer and control of authentic digital goods, under control of individual owners of these rights, rather than a third party acting as a fiduciary. The “double spend” problem is eliminated, and we now have the capability of creating, distributing and creating economic value from digital assets. Furthermore, many physical assets can be represented in digital form, and now that we have a solution for transferring rights of digital assets,we can apply these same solutions to representations of physical assets, so called “tokens”. The implications for commerce and information handling are enormous.

Without DLT, although cash is a digital asset, in order to transfer it reliably between individuals without the possibility that it could be fraudulently multiplied or transferred along the way, directed to terrorists or routed to avoid taxes, it must go through a trusted third party. Banks exist for this purpose. Although health records are a digital asset, in order to ensure that privacy is maintained and not leaked indiscriminately, access is tightly controlled through hospital administrators. Although land records are digitally maintained, in order to ensure that land can be transferred to one and only one person at a time, these records are maintained by land registry offices. These so-called “central” parties suffer from several serious issues: first, they represent an identifiable vector from which data can be compromised or altered; second they rest on third-party processes that interfere with or limit the capability for information and rights to be exchanged between two parties; third, they incur costs involved in administration of these third-party processes, which ultimately boil down to highly-trusted people, and controls on the behavior of these people; and finally, because they rest on people, no matter how trusted, they are exposed to being compromised, either by accident or intent.

DLT were explicitly designed to serve these same purposes, although without the need for trusted people anywhere in the process. Instead, the ledgers, and the verifiable mathematics on which they rest provide the trusted platform. The distributed nature means that this trusted capacity to transact between two parties can be ubiquitously and reliably available to all parties at all times. Ultimately, because math is cheaper than meetings, DLT technologies represent opportunities to replace many of the social processes that have stood in place for hundreds of years.However, there are limits to this technology. A key limit is theso-called“Oracle” problem. While the ledger can cryptographically prove that a transaction authorizing the transfer of my car to my neighbor, it does not cryptographically prove the existence of the car, that it is in fact blue, or that the engine hasn’t just seized. It also does not guarantee that I am not in fact masquerading as my neighbor. In other words, the fact of a transaction can be verified, but if it has to do with anything that is not on the network, its truth cannot be verified except from outside the network.Therefore, the only transactions that do not rely on a trusted third party are transactions that occur totally within the network. This limits the “trustless” nature to exchange of digital assets, and explains why the primary economic use-cases of blockchains have been limited to payment in cryptocurrency, settlement of debts, and various transactions which update data on the chain as a consequence.Another key limit is that transactions only move in one direction, under the cryptographic control of the originator. These transactions cannot be reversed, except through another transaction, and then only with the counterparty’s participation. This leads to asymmetrical risks to the advantage of the counterparty. This limits widespread utility to transactions that can be completed atomically, or where the transaction value can afford a substantial deduction for risk, or where the risk asymmetry cannot be exploited to the advantage of the counterparty. A third risk is the loss or compromise of a private key. If a private key is compromised, it is not possible to repudiate any of the transactions authorized by that key. If a private key is lost, it is not possible to recover or transfer any of the associated information.

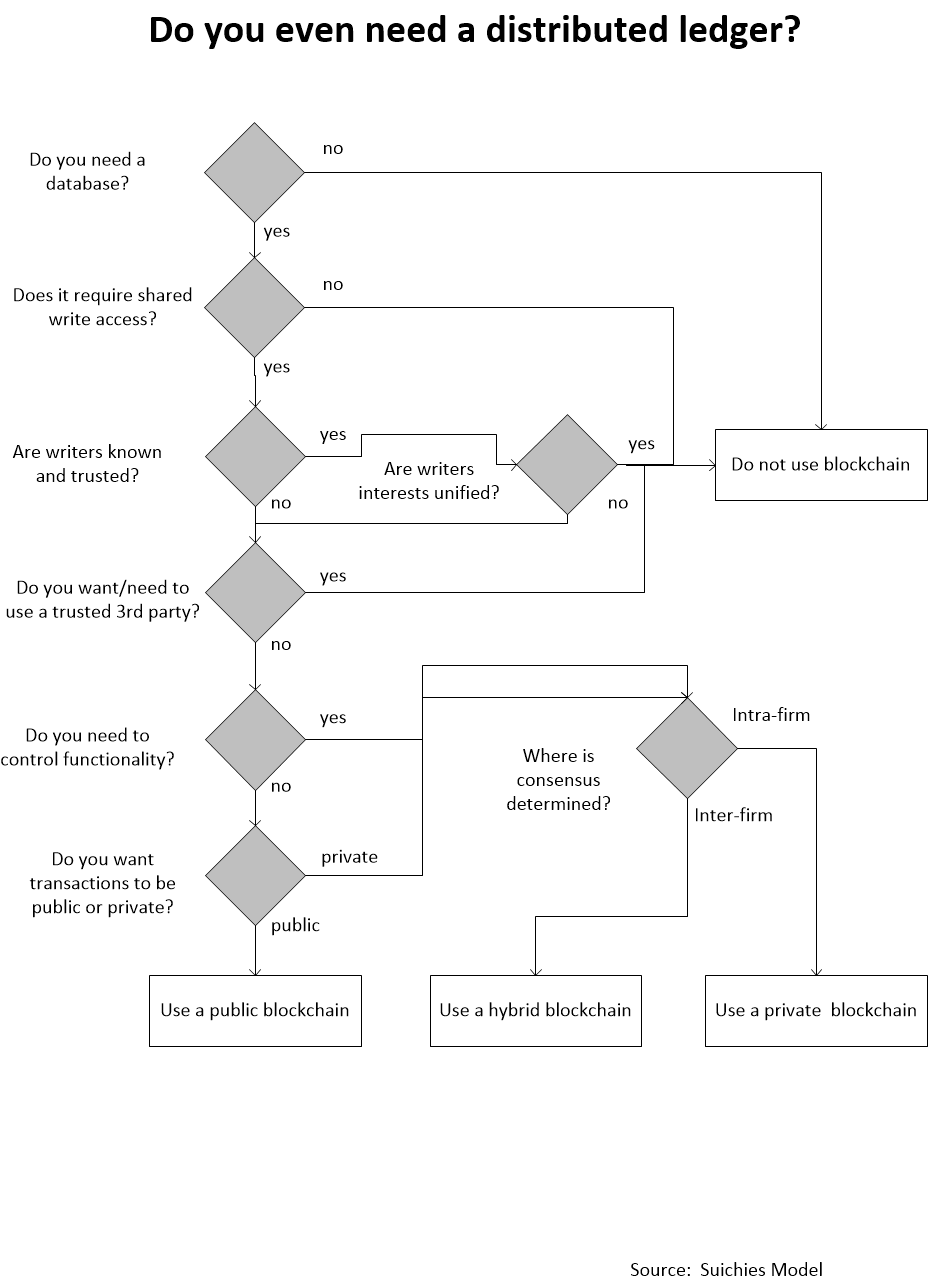
Last and not least, there is an issue in some DLT with two issues that emerge from digital consensus: lack of “finality”, and exposure to “censorship”. The consensus mechanism of the distributed ledger chooses which information is recorded in the ledger. In a distributed ledger, it takes some time for a block solved by one node to be distributed to all of the nodes. In this time, it is possible that a competing node could solve a different block, and its solution could also be propagating through the network. Some of the nodes in between could even build new blocks on top of the competing blocks. The consensus mechanism ultimately forces all of the nodes to agree on a common chain, but if we just look at one node we cannot tell for sure that the nodes near the end are being built on the version of the chain that will be ultimately accepted. Generally, we need to wait for at least six blocks to have been built on a given block before we have a reasonable probability that this block is going to be present in the “final” version of the chain, and even then, there is still a remote possibility that it will not. So while we can look far back into the chain and view the ledger with certainty, the same can’t be said for the most recent transaction. If blocks are produced every ten minutes or so, this means that we can’t really trust any transactions that are less than an hour old. Censorship is another problem: if we are trusting the contents of a ledger to be “true”, then anyone with the power to prevent a transaction from being recorded can influence the truth. Generally speaking these two issues mean that submitting a transaction to the network is not a guarantee that it will be recorded, and that even once a transaction is recorded that it might not be finally recorded. These aspects make DLT particularly unsuitable for transactions that must be verifiably complete within a short, finite period of time.

### DLT Selection Matrix

While DLT might have had a catalytic effect to spur action to delve deeper into current business problems, it is still vital that you evaluate the suitability of different technologies and their business cases.

From a GC perspective, DLT is probably not ideal technology selection for the following situations:

* Systems requiring high performance (millisecond) transactions
* Systems that record or make secondary decisions (e.g. smart contract input) including or based on Protected or non-public data
* Small or single organizations (no business network)
* Looking for a database replacement
* Looking for a messaging solution
* Looking for a transaction processing replacement



**Figure 14: DLT Decision Matrix**

# SECTION 5. PUBLIC SECTOR EXPERIMENTATION

There are numerous examples of expressed interest in DLT technology and its support for continued research and development outside of Canada:

* The United States Internal Revenue Service (IRS) is creating a virtual currency strategy to address the risk that undetected noncompliance of virtual currency taxable transactions will result in an increase to their tax gap.[[1]](#footnote-0)
* The United States Government. is exploring blockchain solutions for IT procurement.[[2]](#footnote-1)
* A number of countries are discussing the creation of national digital currencies. [[3]](#footnote-2)
  + The Bank of England’s top economist, Andrew Haldane, has proposed a national digital currency for the United Kingdom.
  + The Deputy Chief of the Bank of Russia, Olga Skorobogatova, said that it was “time to develop national cryptocurrencies”.
  + The People’s Republic of China has been experimenting with Ethereum to develop a digital yuan.
* Estonia has deployed blockchain solutions for digital identity[[4]](#footnote-3) and voting[[5]](#footnote-4) and is expanding to include health care.[[6]](#footnote-5),[[7]](#footnote-6)
* Other countries, such as India[[8]](#footnote-7) and Australia[[9]](#footnote-8), are exploring blockchain to secure citizen’s digital data.
* Deloitte reports that, “The United Arab Emirates government is exploring a wide range of use cases, including business registration,[[10]](#footnote-9) trade,[[11]](#footnote-10) and central bank operations.[[12]](#footnote-11)”[[13]](#footnote-12) This March, Dubai began workshops to identify potential blockchain use cases and plans to build a shared platform—Blockchain as a Service—for Dubai government entities to use for implementing their projects.
* Sweden[[14]](#footnote-13), Republic of Georgia[[15]](#footnote-14), India[[16]](#footnote-15), and perhaps Honduras[[17]](#footnote-16), are all exploring blockchain for land registry solutions.
* The United Kingdom (UK) began a social welfare payment DLT pilot project in May 2016 and is currently considering whether to expand it and how to advance to a production-ready solution.[[18]](#footnote-17)
* The European Union is funding a three-year, €5 million project to develop forensic tools that will aid law enforcement agencies in the detection of criminal transactions involving virtual currency. 15 organizations in seven European countries are participating
* The IRS is using tools to identify participants in virtual currency networks to detect tax non-compliance.[[19]](#footnote-18)
* Mexico plans to create a digital peso using bitcoin technology. This cryptocurrency would be controlled by the central bank of Mexico.
* Honduras has announced that it will apply blockchain for land registry and property title tracking.
* China’s National Council for Social Security initiated a blockchain initiative that intends to reduce the transaction costs associated with the investment and the management of social security funds.
* Philippines’ two largest telecommunications companies, Globe Telecom and Smart Communications have invested in the blockchain startup Coins to support economic inclusion in Southeast Asia.
* The UK has implemented a FinTech hub with government-backed efforts such as the FCA Sandbox and the Whitechapel Think Tank in order to support blockchain development.
* In Switzerland, pro-cryptocurrency and pro-blockchain regulations have fostered the creation of numerous blockchain start-ups, most of which are located in Zug.
* Singapore has established a Financial Technology and Innovation Group, and launched a sandbox mechanism for blockchain and other related technologies.
* The State of Delaware is currently providing open access to archival records based on blockchain technology

## Canadian Governments

The UK government report Distributed Ledger Technology: Beyond Blockchain states that DLT could provide a new type of trust mechanism for various forms of services. The GC has been active in assessing DLT for its impact to GC services.

### Strategic

* **General**
  + In June 2015, the Senate Standing Committee on Banking, Trade and Commerce[[20]](#footnote-19) recommended that the GC:
    - explore how to leverage blockchain technology to deliver government services and to enhance security,
    - foster innovation with this technology, and
    - amend legislation to address illegal activities related to digital currencies.
  + In December 2016, senior GC officials met to explore the feasibility of Canada becoming a global hub for blockchain technology.[[21]](#footnote-20)
  + Budget 2017 emphasized the strategic importance of innovation for Canadian economic growth and stated that supporting innovation is a key responsibility achieved by enabling widespread adoption and better use of digital tools. [[22]](#footnote-21)
  + In June 2014, Canadian legislation[[23]](#footnote-22) to treat virtual currency businesses as “money service businesses” for the purposes of its anti-money laundering law received royal assent. Once policies and regulations are established, the new law will take effect. The Province of Québec has also enacted policies related to money service businesses.[[24]](#footnote-23)
* **National Research Councilo**
  + Since 2014, the Industrial Research Assistance Program of the National Research Council has been assisting Canadian Small and Medium enterprise with advisory services and financial contributions totaling over 0.5 M$ to research, develop and commercialize blockchain technologies.
  + NRC and IRAP is actively engaged to expand and encourage private-sector capabilities to design, deliver and commercialize distributed ledger technologies in SME of all sectors and in all regions.
* **Financial Transactions and Reports Analysis Centre of Canada**
  + Since 2016, the FINTRAC, the Canadian financial intelligence unit (FIU), has been monitoring and assessing the potential impacts widespread uptake of blockchain technologies across the financial sector may have on Canada’s ability to detect, prevent and deter money laundering and terrorist activity financing. This ongoing analysis includes both assessment of the blockchain technologies that display the greatest vulnerabilities to abuse for illicit purposes, as well as those that have the potential to enhance the Canadian anti-money laundering and anti-terrorist financing (AML/ATF) regime through their ability to enhance the compliance programs of businesses required to comply with Canadian AML/ATF legislation and regulations.
* **Canada Revenue Agency**
  + The CRA identified the need to develop policy for the tax treatment of digital currency at the Senate Standing Committee for digital currency in 2014. Policy development would include areas such as privacy, banking and cybersecurity.
  + The CRA also identified the need to further analyze the overall risk blockchain may pose the Canadian tax base.
* **Bank of Canada**
  + Carolyn Wilkins, Senior Deputy- Governor of the Bank of Canada, believes central banks everywhere should seriously study the implications of moving entire national currency systems to digital money.[[25]](#footnote-24)

### Experimentation

* **General**
  + IBM Canada, the Province of British Columbia, and DIACC collaborated to develop a PoC to explore the viability of blockchain technology as a tool to enable more secure, effective, and efficient corporate registrations – both within a single province and across multiple jurisdictions.
  + The GC, Province of Ontario and City of Toronto have all contributed funding towards the creation of the Blockchain Research Institute in Toronto[[26]](#footnote-25), a joint private-academic-government venture.
* **Innovation Science and Economic Development Canada (ISED)**
  + ISED is working with the Blockchain Research Institute (BRI) to understand how the government can use blockchain to improve its operations and service delivery. The research project will consist of four use cases examining different sectors of the government. Each use case will produce an assessment of how blockchain could be implemented as well as any expected challenges. The project began in August 2017 and will finish by May 2018.
  + As part of the project, the Canadian Intellectual Property Office (CIPO) will have a case study developed which seeks to understand how the registration of copyright could leverage blockchain technology under the constraints of current legislation and CIPO’s mandate. Blockchain could add clarity to a creation’s chain of ownership including any licenses, sub-licenses and assignments. Also, it could potentially provide immutable proof of ownership by providing a unique identifier created from the digital signature of the work, and the exact time of registration to help in dispute resolution.
  + The Government of Canada, Province of Ontario, and City of Toronto undertook a PoC which explored the use of blockchain technology to expedite the time it takes business owners to open a restaurant in Toronto. Currently, the process of setting up a new restaurant in Toronto is laborious, involving compliance to over 25 provincial statutes by obtaining various permits, with much duplication of information. Rather than submit their information to each agency separately, the PoC demonstrated that applicants could submit their information only once as it was securely shared between all agencies through a private blockchain platform. The PoC also demonstrated that third parties such as banks might hold read-access to certain information that would allow mortgages be issued to business owners without the need to re-submit certain information.
* **Bank of Canada**
  + The Bank of Canada recently completed a one-year DLT pilot project named Jasper and concluded that DLT is not yet mature enough to run a national interbank payment settlement system. The project compared two different distributed ledger platforms. Results indicate that while one provided more resilience, it had issues such as cost efficiency and privacy while the other satisfied those issues at the expense of resiliency.
  + The Bank of Canada has committed to researching the new technology and partaking in a PoC alongside Payments Canada, Canadian commercial banks and the R3 consortium. During the Summer of 2017 they released their analysis of distributed wholesale payments in a document titled Project Jasper.
  + The Bank of Canada, Payments Canada and the TMX Group recently announced Phase 3 of the Jasper project and will develop a proof of concept for the clearing and settlement of securities.
* **National Research Council**
  + The Industrial Research Assistance Program (IRAP) of National Research Council (NRC) determined that the entering into and recording of contribution agreements is an area in which blockchain technology could be useful. The process of entering into a contract involves execution of a document that is legally binding and potentially subject to later dispute. Contract is a document that both parties desire to be subject to authentication and nonrepudiation. Robust and practical secure key management, particularly by non-Government participants (who may lose, forget or compromise keys), presents several significant operational challenges that remain to be resolved.
  + All Canadian granting and contracting departments and agencies make proactive disclosure of key government contracts. NRC IRAP has also determined that the ledgering capacity of public blockchain technology, coupled with the public capability to design and implement various blockchain explorer technologies may be useful on a stand-alone basis to provide enhanced proactive disclosure of grants and contributions. This is extensible to the government’s open-data initiative. NRC-IRAP is undertaking an active experiment to make public disclosure of contributions on one or more public blockchains in near real-time.
  + IRAP is presently using the BCIP process and procuring services of Canadian SME in anin an experiment to use blockchain as part of the solution for their proactive disclosure process.
* **Canada Revenue Agency**
  + The CRA has created an Innovation and Emerging Technologies section to perform technology research. An early project will be a blockchain PoC.
  + The CRA has undertaken research to learn more about cryptocurrencies and the risks they pose to the Canadian tax base. This research will inform future risk assessment and audit approaches.
  + The CRA is exploring tools to identify participants in virtual currency networks to detect tax non-compliance.
  + SecureKey has partnered with CRA and Telco on the Verified.me project to build a new blockchain-based digital identity service. The new service will expand on SecureKey’s Concierge service which is used by individuals to authenticate themselves to the GC through the banking sector.
* **Elections Canada**
  + Interest in blockchain remains at the research level, monitoring initiatives that address practical applications that might support Voter List Management, Secure Identity Management, and management of electoral geography.
* **Natural Resources Canada**
  + The department is currently exploring the feasibility of using blockchain to serve as a public registry for the disclosure of payments by companies under the Extractive Sectors Transparency Measures Act (ESTMA).
* **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**
  + The agency is currently exploring blockchain and mobile payments technologies to better understand their implications for anti-money laundering/counter-terrorism financing.
* **Public Safety Canada**
  + The department is monitoring advances in blockchain from a cyber-security perspective. Public Safety Canada’s focus is primarily on the various uses and misuses of virtual currencies (extortion or blackmail).
* **Public Service Procurement Canada**
  + Defining a pilot that will use DLT to verify business organizations in order to further enable self-service capabilities for partners on the BuyAndSell platform.
* **Receiver General of Canada**
  + Exploring opportunities to recieve, maintain and manage recordscurrently recorded inthe Common Departmental Financial System and/ortheCentral Financial Management Reporting System

### Execution

* **Canada Revenue Agency**
  + The CRA has identified and executed a process to seize digital currency holdings to satisfy debts to the Crown.
* **Canadian Securities Administrators** 
  + The Canadian Securities Administrators are taking steps to ensure protection for consumers who invest in cryptocurrency offerings by tech companies that are seeking to raise capital through initial coin offerings (**ICO**), initial token offerings (**ITO**) and sales of securities of cryptocurrency investment funds. Concerns include the use of unethical practices or illegal schemes and poor consumer understanding of the risks involved.[[27]](#footnote-26)

# SECTION 6. PATH TO ADOPTION

## Experimentation

The path to adoption of any new technology, including DLT, typically follows several stages of

Development and begin with a “proof of concept.” These proof of concepts are, experimental uses of the technology on a small scale in a non-production environments, and are used to help understand the potential and limits of a technology for a specific purpose and to understand the risk. At this stage, some important aspects of the technology and operations that are critical in a production environment, such as scalability or security, may not be fully understood or addressed.

The GC must encourage experimentation of DLT to occur outside of a defined project. It must look outside of its existing business models in order to avoid replicating existing behaviours in a new technology. In order for the GC to prepare for experimentation it must prepare to answer:

1. What DLT platforms are suitable? What are the platform selection criteria?
2. What information is suitable for putting on DLT and what should be stored off-chain?
3. What are the performance requirements that need to be assessed?
4. Which deployment model should be used for a particular use case (Public, private, consortium)?
5. Should only existing business processes be revisited or should the GC only focus on new opportunities?
6. How will GC DLTs operate in a global environment?

The GC must establish a means to ensure awareness and collective learning of best practices and standards so that each experiment incrementally further matures the GC’s knowledge toward DLT. The GC should be further encouraged to do ideation of DLT opportunities and develop the required skills to aid other GC members with their experiments. Communication and awareness can occur within communities of practice; however they traditionally are comprised of members with varying levels of availability, experience and motivation. A more focused task force of practitioners should be established to help link experiments to GC lines of business.

### Experimentation Framework for Disruptive Technology

The GC Experimentation Framework for Disruptive Technology aims to increase the level of awareness of GC experiments to avoid duplication, ensure that subsequent experiments are incrementally maturing the GC’s knowledge and skills, and provide opportunity for collaboration. It will capture information related to the following questions.

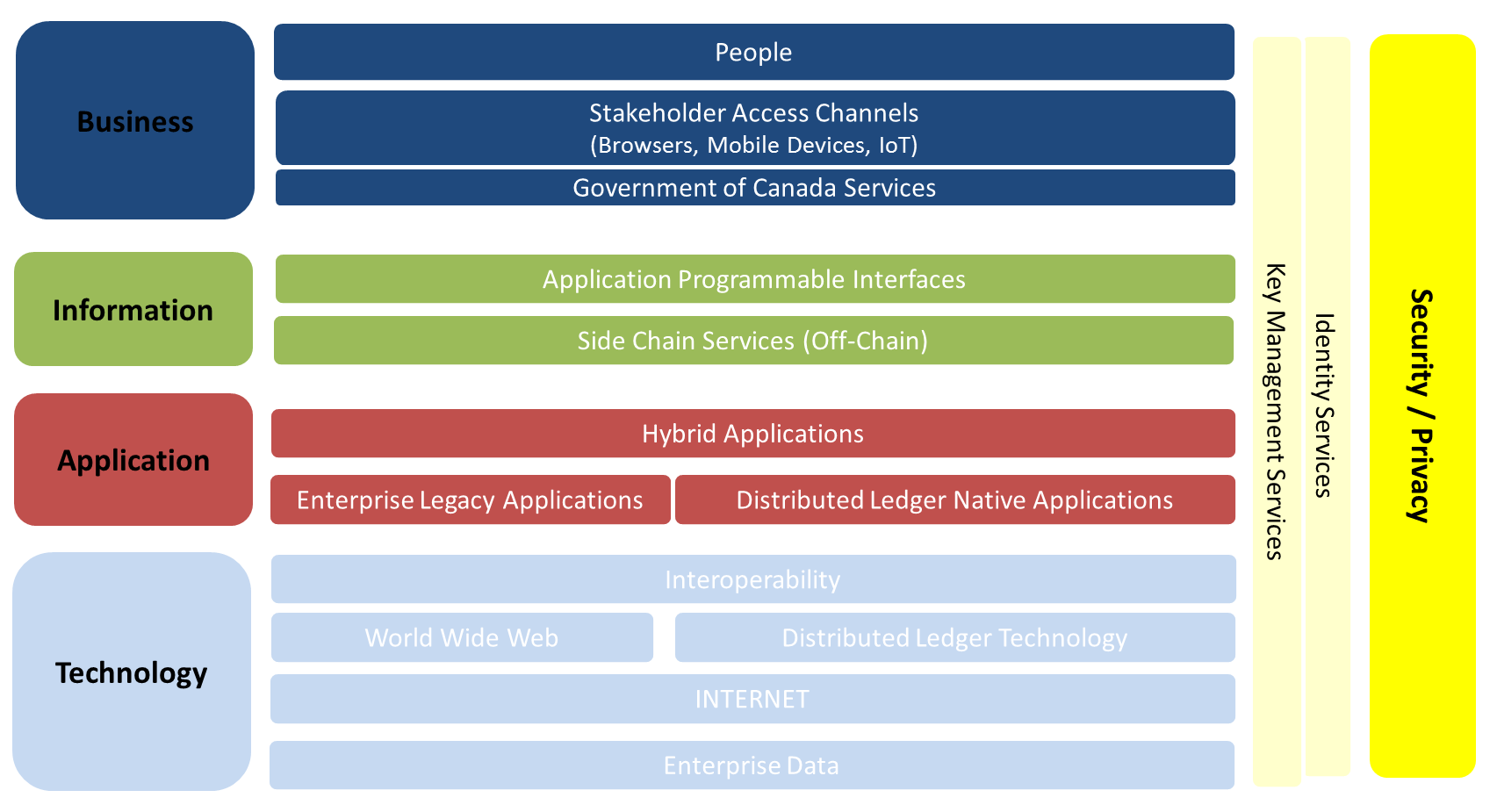
1. What are the strategic target outcomes that we want to focus upon and what are the predicted outcomes as determined by our present level of understanding?
2. What lessons are we learning and making in order to apply best practices for the future?
3. What critical success factors and performance indicators are we measuring?
4. How do we align the GC internally in order to effectively collaborate with our partners and industry?
5. How do we grow our knowledge without having to associate all of the learning activities to a project with a much broader business scope?
6. How do we ensure that the GC has diversity in the technology and service options that exist related to DLT?
7. How will the GC balance the selection and management of PoC or proof-of-technologies to ensure that they deliver value?
8. What special circumstances evident in this particular department made a substantial contribution to its success or failure?
9. Are there factors that other departments must have that are prerequisite to obtaining predictably similar results?

## General View of Architecture Elements

A DLT platform both introduces new and leverages existing GC architectural elements. The various DLT platforms have common architecture building blocks such as:

* Infrastructure and Protocols
* Middleware and Services
* End-User Applications

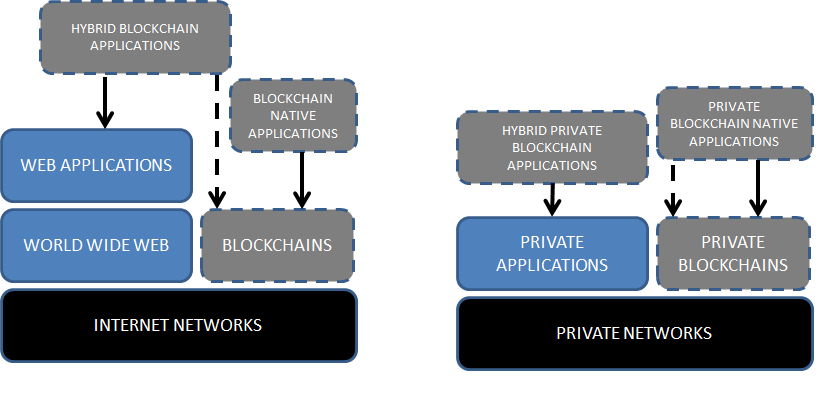
Each of the elements will be detailed as the GC proceeds with developing a reference architecture to help guide DLT experiments.



**Figure 15: Government of Canada Architecture Reference Model Level 0**

The diagram noted above serves to reinforce that infrastructure capabilities are required to support the middleware software and services that could be built or delivered on top of the infrastructure elements. Middleware extends the functionality of the infrastructure elements and makes it easier to make applications in addition to integrating with legacy applications. The development of DLT applications can occur in parallel to the deployment of infrastructure and middleware.

The following Blockchain Reference Model diagram serves to reinforce that not all DLT based solutions will follow the same architectural deployment pattern as the requirements identify the need for level of integration to legacy data and whether an open or closed network will be selected.



**Figure 16: Four Types of Blockchain Applications**

## Barriers to Adoption

### Lack of mature tools

DLT represents a rapidly evolving space for both business and technology. The technology concepts have individually been proven and around for several years however the ecosystem and list of available DLT service offerings and tools are changing. This can create reduced confidence in robust testing of the code. For example, it was only in the summer of 2017 when R3 Corda introduced its open source code for its platform and Hyperledger has had projects added in early 2017.

### Understanding the choice

The growing list of DLT service provider options, the changes to the open source code and the various architectural patterns that they represent result in a wide variety of solution decision points to address known GC requirements, however the GC must also invest in identifying new business opportunities. This may result in a hesitation to commit beyond experimentation until the DLT ecosystem and the GC need is better understood.

### Open Source

The fact that DLT platforms are widely open source is both an enabler and a deterrent. The GC is presently defining its strategy and policy position on open source so until this activity is finalized there will be uncertainty toward the adoption of DLT based upon the same concerns that other open source technologies receive – i*.e. versioning and forking of source code, support, understanding true cost model of open source, further removed from the GC focusing on the consumption of Software-as-a-Service versus the need for development, warranty and liability indemnity*.

### Market Correction

As the DLT ecosystem evolves there could be start-ups and mature enterprise efforts that are either cannibalized or the code they represent is abandoned. If the GC wishes to reduce its technical debt and focus on the consumption of services over the development of services then it could be reluctant to invest in a marketplace where the service provider longevity is a risk in itself. This may also create a competitive environment where the race to release new code trumps the quality and stability of code.

### Lack of Standards

The lack of market adoption to derive informal widely accepted approaches and the lack of formal standards introduces the challenge to defining DLT project implementations based upon a history of best practices.

# SECTION 7. CONSIDERATIONS FOR THE GC

## POLICY Considerations

### Recourse

The decentralized nature of DLT raises cross-jurisdiction and multinational questions that must be understood before the GC fully invests in DLT. For example, if Canada participates in a public ledger and the cause of an issue within the public ledger is external to Canada then what recourse can Canada pursue?

### Smart Contracts

The GC must not enter into Smart Contracts without having a clearer understanding of the legal enforceability, liability and accountability of Smart Contracts.

### 51% Attack Problem

Proof-of-Work systems are vulnerable if 51% of the computing power colludes since there is the risk that this majority may produce a longer blockchain than the other 49%. This allows the colluding majority to write the transactions and exclude transactions that go onto the block, thereby controlling the network.

### Know Your Customer

The GC must ensure that DLT implementations are capable of meeting any regulation requirements that do not permit anonymous transactions.

## BUSINESS Considerations

### Legacy Business Processes

The GC must determine the degree to which DLT could be integrated into existing regulatory frameworks, GC business applications and processes. Don’t limit the potential usage of DLT as a substitute to solve existing business problems and ensure that analysis is being done to identify new opportunities to apply DLT. Identify the plausible scenarios for decentralization and candidate responses to pursue.

It must identified if DLT will be setup as a greenfield platform only to seek out new opportunities.

### Legal Code Vs Technical Code

Smart contracts are not an equivalent to legal contracts. Understanding the present distinction and how they could fit in the law in the future is a key item to monitor.

### Business Relevance

ATOMIC – use as the ability to generalize all DLT related uses cases (assets, trust, ownership, money, identity, contacts)

Those that design and implement DLT can have an economic advantage. The GC can establish a DLT backbone for Canada.

Decentralization also implies that the GC could seek out new partners – how could the GC engage industry and its partners? Identify the value chain for GC services and analyze which parts are candidates for change to support reduced friction in markets and future sustainability

Further assess the ability to aid Canadian businesses entering into new business relationships with the support of GC enabled DLT services, such as individual and organization identity verification.

### Innovation

Innovation – GC public school usage for open learning badges, education credentials or GC hiring process accepting credentials vs current paper based approach that is required for each staffing process even for existing GC employees

### Environmental

Asses the environmental impact for Proof-of-Work design implementations which could lead to additional weighted criteria in order for the GC to determine when to favour a permissioned or permissionless DLT model.

## ARCHITECTURE Considerations

### Foundational Architecture Elements

DLTs are comprised of a database, a software application, a number of nodes connected to each other in a peer-to-peer network, clients to access it, a software environment to develop on it, and tools for monitoring. The foundational services require a network topology to setup, the ability to manage identity interfaces to a DLT implementation, and the ability to store the required security keys.

### Application Programmable Interfaces

How do blockchains relate to the ability to get and share information via APIs? Is the implementation of a blockchain easier than the setup of APIs to access data?

### Reduce Lock-In

DLT capabilities themselves and options are rapidly evolving, how could the GC get acclimated to DLT but not fully committed to a single direction?

### Architectural Patterns

Explore the suitability of Sidechains as a means to extend scalability, interoperability and flexibility of blockchain solutions.

Be aware of DLT anti-patterns where the need there is no issue of trust between the participating parties and the immutability of data is not a priority.

Assess architectural patterns for public, consortium and private distributed ledgers and their ability to meet mission critical requirements or enterprise grade requirements.

Assess the transaction costs to participate in DLT and in various deployment models.

Assess the role of mobile devices as nodes in the network that will routinely connect and disconnect.

### Scalability

The nodes within a DLT must be able to access the network at all times which results in the architectural need for a low latency network, which may be influenced by geographic proximity of nodes and the physical constraints of the network.

### Performance

The transaction volumes to support existing GC business services, and consideration for future opportunities, should be measured against the processing performance of proposed DLT implementations. The throughput and latency of DLT solutions is not presently at the same scale as the throughput of industry leading financial services. This may become a determination in selecting between public and private DLT implementations.

### Emerging Technologies

Assess the relevance of Internet of Things (IoT) and Artificial Intelligence spawning new business requirements that require an understanding of the user journey for *things* – *ie. sensors, monitor, devices*.

## INFORMATION Considerations

### Knowing Your Data

The GC must know what information assets are being placed into public blockchains. This means that the information architectures must identify what are the data elements that are pointers to GC solutions residing in transactional databases. The data placed on the blockchain must obviously account for the security and privacy considerations in addition to the impacts to data retention periods and audits of the GC solutions.

### Understanding Of Immutability

Data within a DLT is often communicated as being unable to be altered. The understanding of this statement needs to be re-assessed since the data can be appended and more importantly the data can be edited if compromised, however the DLT security design is to easily identify when the data is edited and blockchain abandons that record of data by creating a new blockchain branch that gets used by all future transactions.

### Big Data

IoT requires new information architectures to be created that include DLT. For example, an autonomous business that is sending data for each step of its supply chain process to the systems or nodes connected to a DLT network generates an increased volume of data (i.e. Big Data) and the consumers of the data must plan for how they can effectively use this increased source of insight. The continual compliance to Canadian regulations has the potential to be done in real-time with DLT.

### Open Data

The relevance of IoT and Big Data to DLT also have the impact to provide updates to Open Data in near real-time.

### Data for New Services

DLT isn’t just about replacing existing legacy processes with a new one. It provides the potential for new opportunities for the GC. For example, a Proof-of-Location service that proves that you were in a given location at a specified time could be the authoritative piece of information for resolving out of country claim disputes for CRA or ESDC.

### Costs for Data

DLTs can also be viewed as shared infrastructure that is like a utility. The utility typically requires a payment based upon usage and this model may quickly apply to blockchains where your transactions receive an added transaction fee in order to cover the expenses associated to operating the utility.

## APPLICATION Considerations

### Understand the Business Context

Developers should become familiar with the business context for considering DLT in order to ensure that their development efforts are anchored in the current and future business requirements

### Design

DLT applications require the internet, however they do not all require the World Wide Web.

### Legacy

Developers should understand the ability to integrate DLT into existing back-office applications to ensure that the end-to-end business processes are understood.

### Data Centre Storage

Ensure familiarity with GC business requirements for distributed storage that could be met through cloud computing and how DLT can alter current investments in existing or planned data storage capabilities.

### Reconciliation

If the typical application design is to reconcile data during non-peak periods as batch jobs then developers will need to assess how applications could be designed for near real time data access.

## TECHNOLOGY Considerations

### Assessing DLT Platforms

All systems can be described by a set of quality attributes that are the non-functional requirements used to evaluate a system. They can represent the architecturally significant requirements that developers must assess related to their needs. Therefore, DLT platforms also have quality attributes characteristics and developers should be questioning the following for each platform that they assess.

1. Programmability – what languages are available and supported by the platform?
2. Scalability – how many nodes can the DLT platform add and what are the upper limits?
3. Upgradability – what is the history of developers for delivering enhancements and upgrades to the platform?
4. Transaction manageability – is there real-time transparency for all transactions?
5. Visibility – do you have a full view on the transaction activity?
6. Affordability – what is the cost of deploying the technology?
7. Security – what is the documented confidence level in the security design for the platform?
8. Performance – what are the upper limits for speed in transaction validation?
9. Availability – what is the historical record and defined target for availability?
10. Extensibility – can you extend the basic functionality of the platform?
11. Interoperability – does it inter-operate well with other solutions or technologies?
12. Transparency– What is the level of collaboration and contributions from the developer community for the open source code?
13. Portability – does an investment in the selected DLT platform introduce the constraint of lock-in?
14. Learnability – how complex is the platform to learn in order to be added to the GC technology stack?

### OSI Model

DLT is made up of several technologies and has influence upon other technologies. It is an overlay of computers and networks on top of the Internet using the IP protocol. DLT is within the Application Layer of the Open Systems Interconnection (OSI) model.

### Open Source

A key trait of DLT is that it is open source. GC resources should be familiar with open source technologies in order to further explore DLT. For example, Hyperledger is an open source blockchain codebase that is hosted by the Linux Foundation. It is one example of how the DLT landscape is evolving to focus on enterprise requirements.

## SECURITY Considerations

### Vectors of Attack

A general concept of a DLT is that all users that are in the network have visibility to the data. If the DLT model is permissionless then in theory the numbers of security vectors are increased when compared to the number of security vectors within a permissioned network.

### Response to Threats

The number of attack vectors may influence the response time to resolve security threats, bugs in the network, malicious code in applications and compromised public and private keys resulting in different degrees of vulnerability for each DLT deployment model.

### Anonymity

DLT enables anonymity and this trait is what concerns current intermediaries that are responsible for monitoring and reporting of financial regulations.

### Key Management

Cryptographic functions and transactions require the use of public/private key pairs.Considerations include recovery from the loss of a private key and secure storag eof private keys.

## PRIVACY Considerations

### Policy Changes

The information architecture for GC applications using DLT must ensure that only the minimal amount of required data is designed to be included within the DLT. If the DLT provides a permanent record of information then this fundamentally impacts the current understanding of data retention needs where the approved Privacy policies today may or may not be the same in the future.

### Read Access

DLT solutions are described as not allowing unwarranted database write activities to a transaction, however the ability to manage read transactions needs to be further understood to ensure privacy of data. Obfuscating data may be explored as a safeguard against privacy concerns.

### Consent

GC and partner business applications that have a desire to leverage identities contained in a DLT deployment must further assess how identity owners grant or deny the usage of their identity within new architectural models for identity validation.

# SECTION 8. RECOMMENDATIONS

DLT is similar to Cloud Computing, Big Data and Internet of Things in that they are all not a single technology and are a combination of utilizing existing technologies in new and innovative ways. The emergence of Bitcoin in 2009 and the later arrival of Ethereum are references to the open source community paving the path forward for new models of trust. The more traditional path to innovation led by enterprise and industry can be seen by the Linux Foundation Hyperledger project.

The Government of Canada can play an important role in further maturing DLT and helping Canadians to benefit from DLT by participating in both modes. The Government of Canada has the current challenge to determine how, when and where the detailed impacts of DLT could reside. Therefore, the following six recommendations have been defined for the GC.

1. Contribute to international efforts toward the development of a Distributed Ledger Technology taxonomy, such as ISO/TC 307.
2. Map existing experiments and pilots that are in various project lifecycles to ensure knowledge sharing
3. Identify dedicated resources to monitor and communicate developments concerning DLT in the world
4. Develop expertise for DLT through experimentation and training
5. Encourage a DLT community be established within the GC with a communication channel between the GC, academia, industry and the public
6. Ensure that the DLT is assessed from Business, Information, Application, Technology, Security and Privacy perspectives

# DISTRIBUTED LEDGER TECHNOLOGY CONCEPTS AND TERMS

## General Concepts

* A ***ledger*** is an information store which keeps a final and definitive record of (business) transactions.
* A ***record*** is information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the *transaction* of business (ISO 15489:2016)
* A ***transaction*** is the smallest unit of a work process consisting of an exchange between two or more participants or systems (ISO 15489: 2016).
* A ***distributed ledger*** is a ledger held in a across a series of nodes in a network, rather than in a centralized location.
* A ***shared ledger*** is a ledger which is accessible to multiple participants. Note that accessibility is independent of the ledger storage architecture, ledger control architecture, ledger sub-setting or ledger permissions.
* ***Distributed ledger technology*** (DLT) is a technology that keeps a ledger of transactions held in a decentralized fashion, across a series of nodes in a network, rather than in a centralized location.
* ***Blockchain*** is a type of distributed ledger technology in which confirmed and validated sets of transactions are held in blocks, and the blocks are linked (chained) in a way that makes tampering difficult and allows only to append additional blocks in a sequential way. Thus, each chain starts with an original, or ‘genesis’ block, followed by a sequence of blocks each of which contains a hash which starts with a genesis block and where each block contains a hash of the prior block in the chain.
* Note that the term "Blockchain" is commonly used in two different ways. It may mean a particular kind of DLT, as described in the previous paragraph – this is the common meaning of "blockchain" used in this white paper. However, it may also be used for the particular ledger data structure consisting of chains of blocks.
* A ***block*** is a data structure for a ledger record containing a set of one or more timestamped transactions and a header which contains data including the hash of the previous block in the chain.
* ***Block Height* is** the distance between the genesis block and the last block in a blockchain.
* **Genesis block** is the first or initial block in a blockchain.
* ***Merkle tree*** a method of saving disk space involving shortening a blockchain by hashing together all the transactions
* ***Cryptography*** a transformation of a message that makes the message incomprehensible to anyone who is not in possession of secret information that is needed to restore the message to its normal plaintext or cleartext form.
* ***Cryptocurrency*** is form of digital currency based on mathematics, where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds.
* ***Coin*** is a unit of value in a cryptocurrency
* ***Token*** is a representation of an asset (using metadata) where encryption techniques are used to regulation the generation of the asset and to verify transfer of ownership or other state changes to the status of the asset.
* ***Digital signature*** is cryptographic transformation of data which, when associated with a data unit, provides the services of origin authentication and data integrity and may support signer non-repudiation.
* ***Hash*** is astring of bits which is the output of a hash-function. ·
* ***Public key,*** in public-key cryptography, is the key that is widely available and is used by the sender to encrypt and by the receiver to verify signatures.
* ***Private key*** in public-key cryptography is the key that is known only to the recipient and is used for decryption and signing.
* ***Address*** is *used* to receive and send transactions on the network. An address is a string of alphanumeric characters, but can also be represented as a scannable QR code.
* ***Wallet*** is a file that contains a collection of private keys.
* ***Double spending*** is when digital money is duplicated and spent more than once. It has been a longstanding issue in the development of digital money.
* ***Forking*** refers to the creation of an alternative version of the blockchain, by creating two blocks simultaneously on different parts of the network.
* ***Hard fork*** refers to a change to the blockchain protocol that makes previously invalid blocks/transactions valid, therefore requiring all users to upgrade their clients. Recent examples include the Ethereum hard fork, which occurred on July 21st, 2016 and the Bitcoin hardfork, which occurred on August 1, 2017.
* ***Soft fork*** refers to a change to the blockchain protocol where only previously valid blocks/transactions are made invalid. This kind of fork requires only the majority of miners upgrading to enforce the new rules, as opposed to a hard fork which requires all nodes to upgrade and agree on the new version.
* ***Bitcoin*** is the first and most well-known decentralized cryptocurrency.
* ***Ethereum*** is a distributed public blockchain network that allows users to create their own blockchain applications or smart contracts.
* ***Ripple*** is a real-time gross settlement system (RTGS), currency exchange and remittance network operated by Ripple Ltd.
* ***R3*** is a distributed database technology company that leads a consortium of the world’s largest financial institutions attempting to create an open-source distributed ledger platform for financial services.

## Key Capabilities of Distributed Ledgers

* **Immutability** Blockchains create an immutable transaction record (i.e., one that is intended to be tamper resistant, unalterable and unchanging through time). Once a transaction is completed, a record of the transaction is added to the ledger and is never be altered or removed.
* ***Provenance*** ***traceability*** is evidence of the origin of the record of transactions in the sequence of transactions.
* ***Records system*** is an information system which captures, manages and provides access to records over time.
* ***Pseudonymity*** Since public and private key pairs used in recording transactions on the blockchain are not explicitly linked to the identities of people (or devices), the blockchain is said to operate pseudonymously. Because public keys can be traced to the identities of people (or devices), it does not provide anonymity.
* ***Confidentiality (privacy)*** Blockchain systems can be used to protect the confidentiality of records through, for example, the use of smart contracts and private keys.

## System organization

* A ***distributed system*** is a programming model in which components located on networked computers communicate and coordinate their actions by passing messages. The components interact with each other in order to achieve a common goal.
* A ***distributed program***, or ***distributed application program*** is an application that runs on a distributed system.
* ***Peer-to-peer*** ("P2P") is distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equally capable participants in the application. They are said to form a peer-to-peer network of nodes.
* A ***node*** is a peer to peer networked system which runs software components that communicate to support the distributed ledger and which can store a replica of the ledger. Examples could be servers, desktops, laptops or mobile devices.
* A ***DLT platform*** is a set of software and storage entities which provide the capabilities of the DLT system on a node. A ***blockchain platform*** is a DLT platform where the implementation technology is blockchain.

## Types of DLT System

* A ***tokenless*** DLT system is one that does not rely upon an underlying cryptocurrency for its operation (see, for example, Hyperledger).
* A ***permissionless*** DLT system is one where nodes and users are essentially unknown to anyone other than themselves and users require no authorization or authentication.
* A ***permissioned*** DLT system is one where nodes must have a member identity and users must have authorization and authentication.
* A ***public blockchain*** is one that is usable (access, read, write and participate in transactions and in the consensus process) by any participants without requiring any authority (usually a public blockchain is permissionless).
* A ***private blockchain*** is one that is usable (access, read, write and participate in transactions and in the consensus process) only by participants that have been given authority (usually a private blockchain is permissioned). Note that the process for granting authority may be centralized or decentralized.
* A ***consortium blockchain*** is a blockchain where the consensus process is controlled by a pre-selected set of nodes.
* ***Centralized*** (ledger control) architecture is where a central server (or authority) controls the rule enforcement relating to the distributed ledger (i.e. the validation of the new blocks of records).
* ***Decentralized*** (ledger control) architecture is where a central server (or authority) delegates the rule enforcement relating to the distributed ledger to a limited number of architecture elements.
* ***Distributed*** (ledger control) architecture is where all architecture elements (particularly nodes in the DLT system) control the rule enforcement relating to the distributed ledger, based on a consensus mechanism.
* ***centralized*** (ledger storage) architecture has a central server (broker) which indexes, lists and browses the files stored locally on each node of the DLT system.
* ***decentralized*** (ledger storage) architecture has some specialized nodes ("super-nodes") which index, list and browse files stored locally on each node of the DLT system.
* ***Distributed*** (ledger storage) architecture is where each node browses the files stored on other nodes of the DLT system in a “hop by hop” way.

## Consensus

* ***Consensus*** is a set of rules and procedures that allow the DLT system to maintain and update the distributed ledger and to ensure the trustworthiness of the records in the ledger - i.e. their reliability, authenticity and accuracy.
* ***Consensus mechanisms*** are implementations by which consensus is achieved in DLT systems. There are many alternative consensus mechanisms in use in different DLT systems. Examples of consensus mechanisms include Delegated Proof-of-Stake, Paxos algorithm, Practical Byzantine Fault Tolerance, Proof-of-Authority, Proof of Burn, Proof-of-Capacity, Proof of ownership, Proof-of-stake, Zero knowledge proof, Proof-of-work.
* ***Mining*** is a consensus mechanism which operates through a demonstration of proof of work.
* ***Miner*** is an entity owning a node which runs mining programs.
* ***Timing service*** is a service that coordinates the time source used for transactions within the DLT system.
* ***Reward system*** or ***incentive mechanism*** is a consideration (such as a payment) given to a party for undertaking some activity within the DLT system. An example of such activity is the work involved in running the consensus mechanism.

## Roles

* A ***participant*** in a DLT system is a natural or legal person or a group of such persons, whether incorporated or not. Participants in the DLT system are the stakeholders of the DLT system. Types of typical participants include: open source communities, industry alliances, key enterprises, start-up companies, investment institutions, financial institutions and regulatory institutions.
* A ***user*** is a participant who submits transactions to the DLT system.
* A ***developer*** is a participant who writes chaincode and client-side applications for a blockchain system.
* An ***administrator*** is a participant who manages permissions for users to access a permissioned blockchain system.
* An ***operator*** is a participant who controls a centralized blockchain system.

## Applications & Services

* ***Blockchain application*** (or ***ledger application***) is an application which runs separately from the DLT system that acts as a client to the DLT system, used by users and administrators.
* ***Smart contract*** is a distributed application running on and distributed with the distributed ledger. It represents the process of agreeing on a transaction outcome (i.e., state change) rather than (necessarily) having legal status as a contract under law. Its outcome may or may not be legally binding.
* ***Note - Smart contract*** (also termed ***chaincode***, ***programmable asset*** or ***programmable contract***) are instantiated as computer programs that execute in a secure environment within the DLT platform of any node in the DLT system, when a user sends a transaction of a particular type to the DLT system.
* ***Decentralized Autonomous Organization*** refers to long-term smart contracts that hold the assets and encode the bylaws of an entire organization. Operating similar to a digital corporation, DAOs can be used to administer or manage private and public services***.***
* ***Asset registry*** refers to applications that link digital currencies to other assets or records on top of the distributed ledger. Asset registry applications are often termed a “ledger within a ledger”, meaning that a special purpose ledger is embedded within a more general ledger providing consensus on how all embedded data structures are managed.
* ***Membership services*** are services that manage the identity, privacy, confidentiality and auditability within the DLT system. Membership services only apply to permissioned DLT systems.
* ***Off-chain access services*** provide secure means to access capabilities outside the DLT system such as trusted data sources or functions.
* ***Inter-DLT services*** are services which enable smart contracts on one DLT system to interact with another DLT system.
* An ***oracle*** is a trusted service designed to supply external data to a DLT system.
* A ***subchain*** is a logically separate chain that forms part of a blockchain. Also known as a ***channel*** (Hyperledger). Each subchain may be owned by a different entity and may be accessible to a different set of users. Nodes may be set up so that some nodes participate in certain subchains and not in other subchains. The result of this configuration is that the ledger on some nodes contains transactions for that subchain while the ledgers on other nodes do not.
* A ***side chain*** is a second separate blockchain that is associated with the main blockchain and can participate in transactions with it, typically in both directions.

# Acknowledgements

The Government of Canada Digital Target Architecture and Direction micro-mission, which occurred from June 2017-October 2017, received invaluable contributions from several GC members and Canadian universities and colleges in order to develop this whitepaper.

We would like to thank the following people for their dedicated focus during this three month architecture sprint as they contributed to the coordination of review meetings, information sharing, content editing and final reviewing of this whitepaper.

|  |  |
| --- | --- |
| **Name** | **Organization** |
| **Adam Black** | **Innovation Science and Economic Development** |
| **Angela Walch** | **Saint Mary’s University (Texas)** |
| **Anton Bazilev** | **Canada Border Services Agency** |
| **Eric Paquet** | **National Research Council** |
| **Eva Ducas** | **Financial Transactions and Reports Analysis Centre of Canada** |
| **Henry Kim** | **York University** |
| **Jeremy Clark** | **Concordia University** |
| **Joel Garrod** | **Carleton University** |
| **John Shannon** | **National Research Council** |
| **Lisa Lescard** | **Canada Revenue Agency** |
| **Malcom Campbell-Verduyn** | **University of Waterloo** |
| **Ning Nan** | **University of British Columbia** |
| **Tom Keenan** | **University of Calgary** |
| **Troy MacFarlane** | **Treasury Board of Canada Secretariat** |
| **Victoria Lemieux** | **University of British Columbia** |

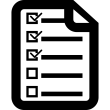
# Footnotes

1. <https://www.coindesk.com/irs-overhaul-bitcoin-tax-strategy/>
2. https://www.coindesk.com/gsa-official-blockchain-procurement-prototype-moving-forward/
3. World Economic Forum – Realizing the Potential of Blockchain, June 2017
4. http://fortune.com/2017/04/27/estonia-digital-life-tech-startups/
5. http://www.reuters.com/article/nasdaq-blockchain/nasdaq-successfully-completes-blockchain-test-in-estonia-idUSL1N1FA1XK
6. http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367
7. https://dupress.deloitte.com/dup-us-en/industry/public-sector/understanding-basics-of-blockchain-in-government.html
8. <https://www.coindesk.com/indian-state-partners-build-public-sector-blockchain-applications/>
9. https://www.coindesk.com/australian-delivery-service-exploring-blockchain-identity-services/
10. https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080
11. http://www.reuters.com/article/us-dubai-fintech/dubai-government-companies-team-up-with-ibm-on-blockchain-project-idUSKBN15M0RR
12. https://www.coindesk.com/emirates-nbd-enlists-uae-central-bank-blockchain-check-trial/
13. https://dupress.deloitte.com/dup-us-en/industry/public-sector/understanding-basics-of-blockchain-in-government.html#endnote-6
14. https://www.coindesk.com/sweden-taking-chance-blockchain-land-registry/

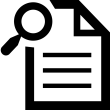
https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-

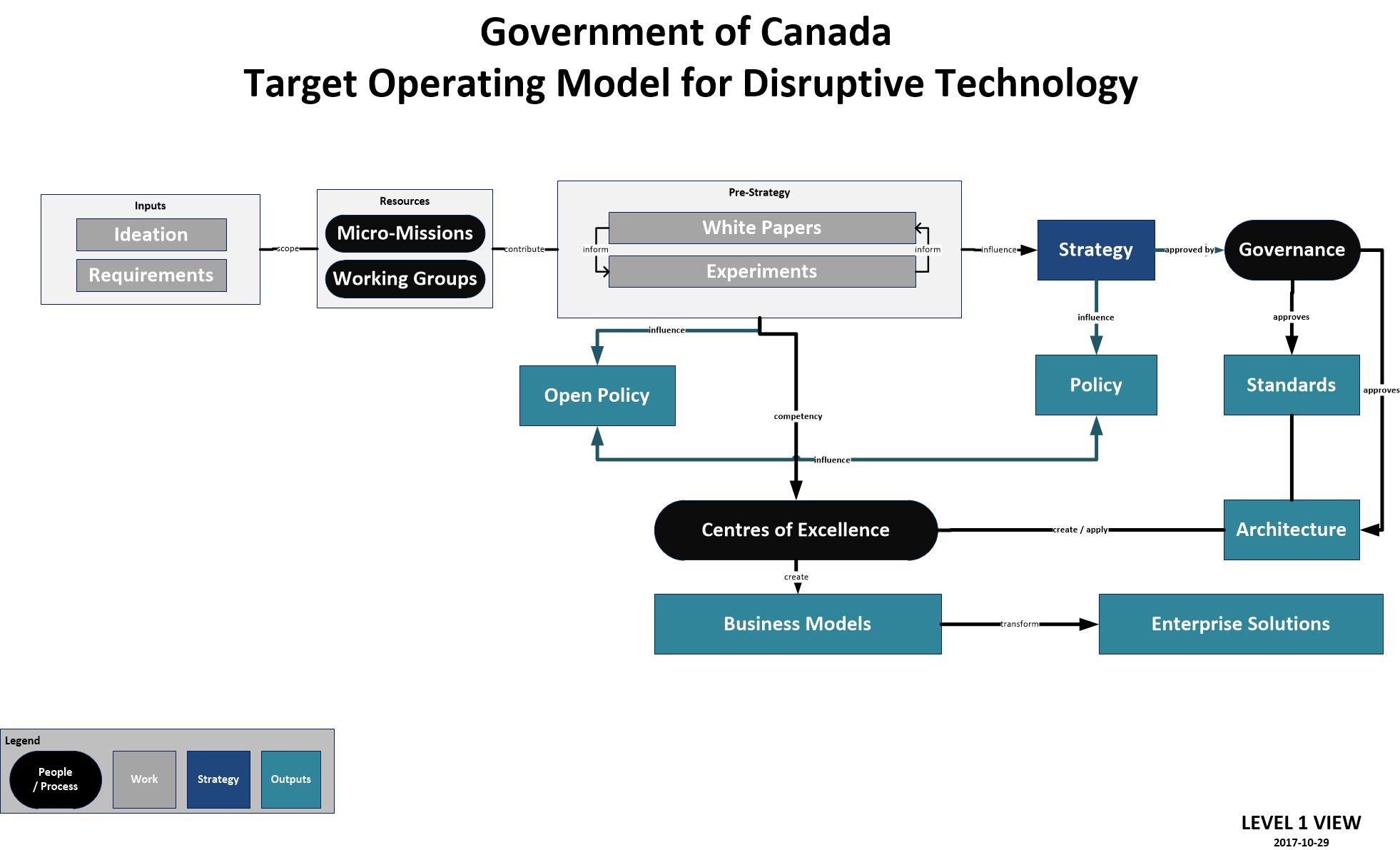
# References

1. Buterin, V. (2014) A next-generation smart contract and decentralized application platform. *white paper*. Https://www.weusecoins.com/assets/pdf/library/Ethereum\_white\_paper-a\_next\_generation\_smart\_contract\_and\_decentralized\_application\_platform-vitalik-buterin.pdf.
2. Cachin, C. and Vukolic, M. (2017) *Blockchain Consensus Protocols in the Wild*, https://arxiv.org/pdf/1707.01873.pdf.
3. Di, L. (2017) Why Do I Need a Public and Private Key on the Blockchain?, https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76.
4. International Standards Organization (2001). *ISO 15782-2:2001: Certificate management for financial services*, s. 3.20. ISO.
5. InterPARES Trust Terminology Project: Key Blockchain Terms and Definitions (2017) http://arstweb.clayton.edu/interlex/blockchain/
6. Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*.
7. Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.
8. Nick Szabo (1997) *The Idea of Smart Contracts*, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html
9. TechGuru (2017) Blockchain: Developer’s Guide & Use Cases, <http://www.techquark.com/2017/06/blockchain-developers-guide-use-cases.html>.
10. Blockchain for dummies, IBM Limited Edition (friction content)
11. Government of Canada Operating Model for Disruptive Technology
12. Government of Canada Experimentation Framework for Disruptive Technology
13. Mougayar, William The Business Blockchain
14. Tapscott, Don (2017) MITSloan Management Review – How Blockchain Will Change Organizations
15. <https://developer.ibm.com/academic/resources/blockchain-educator-guide/>
16. <http://ide.mit.edu/publications/some-simple-economics-blockchain>
17. China Blockchain Technology and Industrial Development Forum (2016), White Paper on China Blockchain Technology and Application
18. Government Office for Science (2016) Distributed Ledger Technology: beyond block chain
19. Treasury Board Secretariat (2017) TBS Blockchain Briefing to the Associate Secretary
20. Treasury Board Secretariat (2017) Blockchain Briefing for DFCIO Council
21. Gartner Blockchain SWOT Analysis
22. Richard Gendal Brown et al (2016) Corda: An Introduction https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf

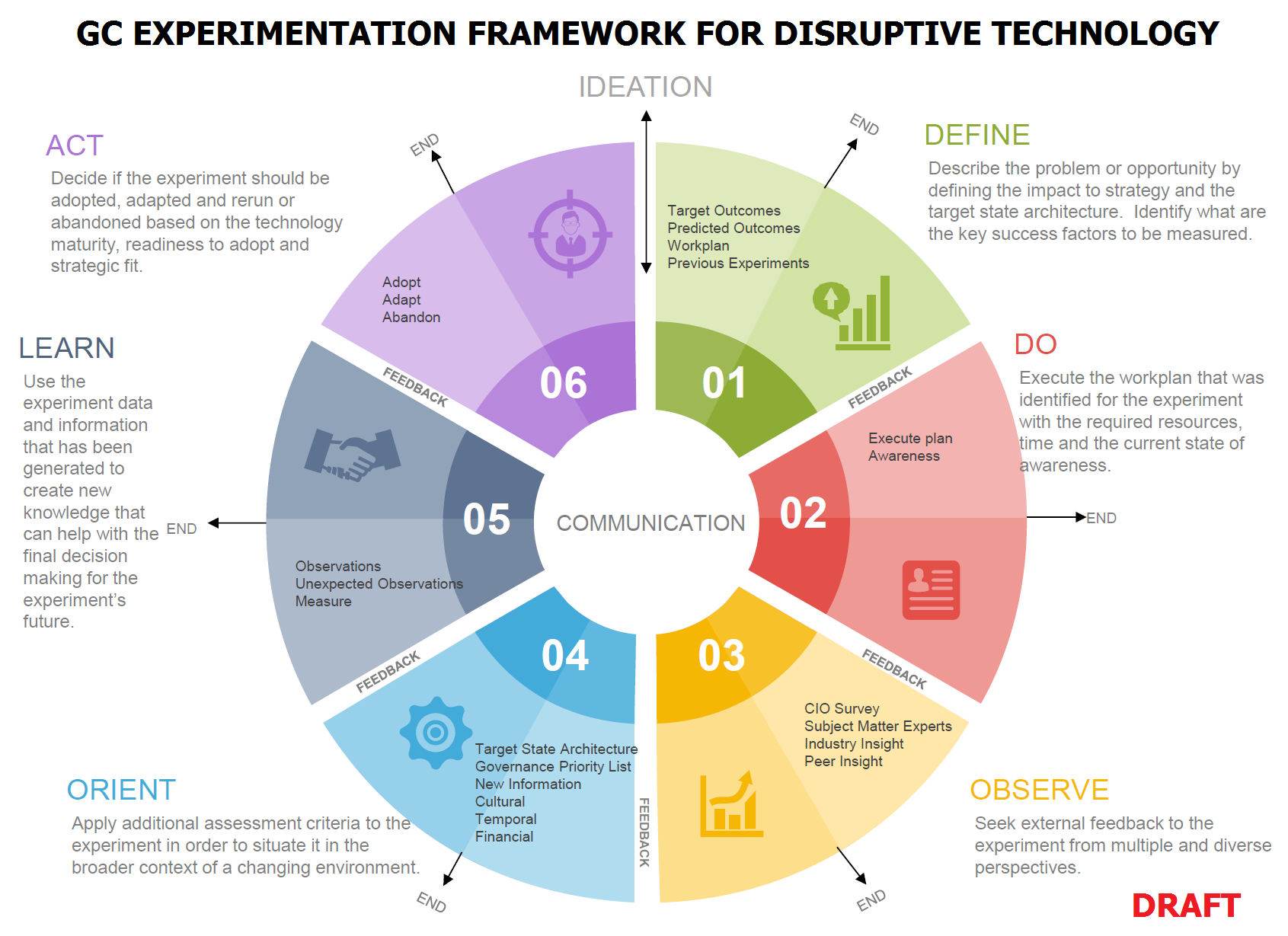
KEY POINTS

 FUTURE WORK

 FIND MORE INFORMATION



**Figure 17: Government of Canada Operating Model for Disruptive Technology**



**Figure 18: Government of Canada Experimentation Framework for Disruptive Technology**

1. <https://www.coindesk.com/irs-overhaul-bitcoin-tax-strategy/> [↑](#footnote-ref-0)
2. https://www.coindesk.com/gsa-official-blockchain-procurement-prototype-moving-forward/ [↑](#footnote-ref-1)
3. World Economic Forum – Realizing the Potential of Blockchain, June 2017 [↑](#footnote-ref-2)
4. http://fortune.com/2017/04/27/estonia-digital-life-tech-startups/ [↑](#footnote-ref-3)
5. http://www.reuters.com/article/nasdaq-blockchain/nasdaq-successfully-completes-blockchain-test-in-estonia-idUSL1N1FA1XK [↑](#footnote-ref-4)
6. http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367 [↑](#footnote-ref-5)
7. https://dupress.deloitte.com/dup-us-en/industry/public-sector/understanding-basics-of-blockchain-in-government.html [↑](#footnote-ref-6)
8. <https://www.coindesk.com/indian-state-partners-build-public-sector-blockchain-applications/> [↑](#footnote-ref-7)
9. https://www.coindesk.com/australian-delivery-service-exploring-blockchain-identity-services/ [↑](#footnote-ref-8)
10. https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080 [↑](#footnote-ref-9)
11. http://www.reuters.com/article/us-dubai-fintech/dubai-government-companies-team-up-with-ibm-on-blockchain-project-idUSKBN15M0RR [↑](#footnote-ref-10)
12. https://www.coindesk.com/emirates-nbd-enlists-uae-central-bank-blockchain-check-trial/ [↑](#footnote-ref-11)
13. https://dupress.deloitte.com/dup-us-en/industry/public-sector/understanding-basics-of-blockchain-in-government.html#endnote-6 [↑](#footnote-ref-12)
14. https://www.coindesk.com/sweden-taking-chance-blockchain-land-registry/ [↑](#footnote-ref-13)
15. https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#7a0127ae4dcd [↑](#footnote-ref-14)
16. http://www.moneycontrol.com/news/business/real-estate/blockchain-technology-use-to-bring-down-cases-of-benami-transactions-2362737.html [↑](#footnote-ref-15)
17. https://www.coindesk.com/debate-factom-land-title-honduras/ [↑](#footnote-ref-16)
18. https://www.ethnews.com/uk-government-considers-expanding-blockchain-trial-for-benefits [↑](#footnote-ref-17)
19. http://fortune.com/2017/08/22/irs-tax-cheats-bitcoin-chainalysis/ [↑](#footnote-ref-18)
20. <https://sencanada.ca/content/sen/Committee/412/banc/rep/rep12jun15-e.pdf> [↑](#footnote-ref-19)
21. <https://www.thestar.com/business/2017/02/28/ottawa-explores-potential-of-blockchain-billed-as-next-generation-internet-tech.html> [↑](#footnote-ref-20)
22. http://www.budget.gc.ca/2017/docs/plan/budget-2017-en.pdf [↑](#footnote-ref-21)
23. Bill C-31 ([An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures](http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6684616) (Bill C-31), STATUES OF CANADA 2014, Ch. 20) [↑](#footnote-ref-22)
24. <https://www.coindesk.com/quebec-province-bitcoin-regulation/> [↑](#footnote-ref-23)
25. World Economic Forum – Realizing the Potential of Blockchain, June 2017 [↑](#footnote-ref-24)
26. <http://www.itworldcanada.com/article/blockchain-research-institute-gains-support-from-three-levels-of-government-and-private-sector/393907> [↑](#footnote-ref-25)
27. <http://www.cbc.ca/news/business/cryptocurrency-regulators-1.4262279> [↑](#footnote-ref-26)