

|  |
| --- |
| ENABLING BLOCKCHAIN INNOVATION IN THE U.S. FEDERAL GOVERNMENT  Updated Blockchain Primer |
| EMERGING TECHNOLOGY Community of Interest  *Blockchain Working Group*  Date Released: April 2024 |

|  |
| --- |
| Synopsis  This updated Primer is intended to be a foundational tool in the understanding of blockchain within the United States federal government. To that end, it should help allay the concerns that some may have about this new technology by introducing blockchain and its related technologies, and how blockchain can be safely and securely applied to the right government use cases. Blockchain has the potential to help government to reduce fraud, errors, and the cost of paper-intensive processes, while enabling collaboration across multiple divisions and agencies to provide more efficient and effective services to citizens. Moreover, the adoption of blockchain may also allow governmental agencies to provide new value-added services to businesses and others which can generate new sources of revenue for these agencies. |

**American Council for Technology-Industry Advisory Council (ACT-IAC)**

The American Council for Technology-Industry Advisory Council (ACT-IAC) is a non-profit educational organization established to accelerate government mission outcomes through collaboration, leadership and education. ACT-IAC provides a unique, objective, and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communication between government and industry, collaborative and innovative problem solving, and a more professional and qualified workforce.

The information, conclusions, and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT-IAC vision of a more effective and innovative government. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over forty years of experience, to produce outcomes that are consensus-based.

To maintain the objectivity and integrity of its collaborative process, ACT-IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of technology. For additional information, visit the ACT-IAC website at [www.actiac.org](http://www.actiac.org).

**Name of Community of Interest or other group**

*(This is a description of the COI or other group that prepared the white paper)*

The ACT-IAC Emerging Technology Community of Interest (Blockchain Working Group) mission is to

**Disclaimer**

This document has been prepared to contribute to a more effective, efficient, and innovative government. The information contained in this report is the result of a collaborative process in which several individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product, or vendor. Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, neither ACT-IAC nor its contributors assume any responsibility for consequences resulting from the use of the information herein.

**Copyright**

©American Council for Technology, 2023. This document may not be quoted, reproduced and/or distributed unless credit is given to the American Council for Technology-Industry Advisory Council.

For further information, contact the American Council for Technology-Industry Advisory Council at (703) 208-4800 or [www.actiac.org](http://www.actiac.org).

Contents

[History & Drivers, the New Era of Digital Records 1](#_Toc130899738)

[Foreword 2](#_Toc130899739)

[Executive Summary 3](#_Toc130899740)

[Distributed Ledger / Blockchain Technology Overview 3](#_Toc130899741)

[Blockchains, Directed Acyclic Graphs (DAGs), and more 5](#_Toc130899742)

[Public and Private DLT’s 6](#_Toc130899743)

[Consensus Mechanisms 7](#_Toc130899744)

[Examples of consensus mechanisms 8](#_Toc130899745)

[Smart Contracts 8](#_Toc130899746)

[Governance 9](#_Toc130899747)

[Digital Assets 9](#_Toc130899748)

[Web 3.0 (aka Web3) and Decentralization 11](#_Toc130899749)

[Next Steps 12](#_Toc130899750)

[Glossary 13](#_Toc130899751)

[Authors & Affiliations 14](#_Toc130899752)

[References 14](#_Toc130899753)

[***Published Content Review Process*** 15](#_Toc130899754)

[***Distribution of Draft Content*** 15](#_Toc130899755)

*This page is blank.*

*(Author, please delete the manual page break and the text on this page if your paper’s TOC spans two pages.)*

# History & Drivers, the New Era of Digital Records

*"A gentleman named Hans Bethe who was one of the OGs of quantum mechanics… One day he figured out for the first time the actual process that led to the thermonuclear fusion in stars at night. He goes out on a date. At one point in the evening his date is looking up at the night sky and says, 'Oh look at the stars, how beautiful they are.' And Bethe says, 'Yes, and I'm the only person in the world that knows how they work.'*

*And for one brief shining moment that was how I felt. I turned to my wife, and I said, 'I think I just figured out something important.'*

*‘...I considered it a true shot heard round the world because no longer did we have to trust a central authority, and even one individual could stand up for the truth and have the gravity of what's right on their side. It allowed us to hold a collective power that had never been possible before.’”*

W. Scott Stornetta, PhD - Keynote Speech

Government Blockchain Association - Blockchain & Infrastructure, October 2021.

# Foreword

Innovation sits at the heart of the U.S. economy and is critical to support government missions. Distributed ledger technologies are a part of that story of American and global innovation, with interesting applications across fields like finance, supply chain, identity, and healthcare. However, as with any other technological advancement, responsible innovation does not mean unchecked technological advancement without regard to implications for society, security, and democratic values.

An incredibly complex landscape of policy, legal, national security, economic, and technological issues serve as the strategic backdrop for blockchain and digital asset development at this moment in history. There are critical challenges that continue to present themselves in distributed ledger technology ecosystems around identity, privacy, discoverability, consumer protections, resilience, and regulation. These challenges are only compounded by the complexity of these systems – for example, their ability to support value transfer *and* information transfer, activities that traditionally have very different policy frameworks and expectations applied to them, via the same rails. The benefits and vulnerabilities of these systems also vary widely based on countless potential implementations across the systems of aspects of governance, operation, and the underlying technologies. *It’s all about the design.*

Exploring these technologies and addressing the key issues presented are also not the responsibility of just one sector – both the public and private sectors hold the capabilities, *and* responsibilities, to help ensure the responsible development of these technologies and related assets. Technologists and policymakers must work together to continuously enhance their understanding of the technologies as well as policy and operational equities at play to drive responsible innovation. This primer from ACT-IAC gives evidence to ongoing efforts across industry and government representatives to try to strengthen that understanding and lay the groundwork to shape a more positive future that leverages DLT and decentralized networks.

Carole House

Executive in Residence, Terranet Ventures, Inc.

Nonresident Senior Fellow, Atlantic Council

Former National Security Council Director for Cybersecurity and Secure Digital Innovation

# Executive Summary

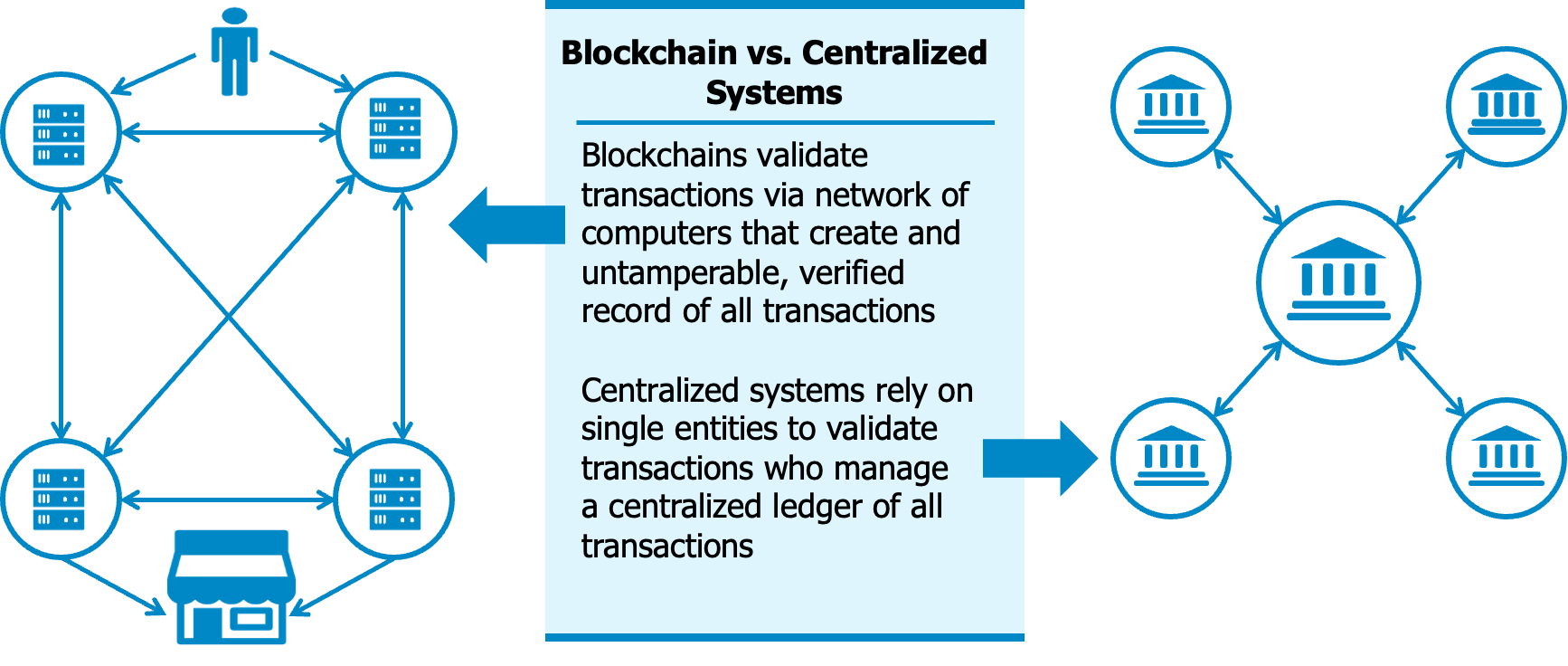
This Primer provides an overview of Distributed Ledger Technology (DLT, commonly called blockchain), digital assets, key definitions, a description of the ways these technologies come to a consensus in a decentralized ecosystem, the distinction between public and private DLTs, smart contracts that can be integrated into blockchains and how the governance of these DLT / blockchain networks functions.

This updated version also includes what has evolved in the industry from 2017 to the present. During this time, several different types of distributed ledger technologies have been created, cryptocurrency tokens and non-fungible tokens (NFTs) have captured the public imagination, and experts believe that these DLT technologies are forming the foundation of Web 3.0, or next generation of the Internet.

This Primer is intended to set the baseline knowledge of the reader for further discussion of the blockchain and orientates their understanding for using the Blockchain Playbook when deciding if and how to integrate the technology at a U.S. Government agency.

# Distributed Ledger / Blockchain Technology Overview

Many people have heard of the term ‘blockchain,’ and associate it with digital currency, but that is only one of the many uses of this emerging technology. **Blockchain** is only one type of distributed ledger technology **(DLT).**

****

***Source: Value Technology Foundation***

DLT uses a set of replicated, shared, and synchronized digital data which is spread across a network of independently owned and operated computing **nodes**. There is no individual data administrator, but a collection of individuals spread across the network that work together who confirm data transactions. Although this is unlike centralized data storage (often governed by a data administrator or team), this system is also widely customizable. The development team for a DLT may create a private network to maintain the familiar checks and balances found in the traditional database.

In a centralized application (such as a typical database), a responsible party (data administrator or team) determines who has access to the data and what they are allowed to do with it. In a decentralized application, (such as a distributed ledger) the data cannot be changed and is shared with every authorized user. While new records may be added, but only with approval from the network. Distributed ledger technology **(DLT)** accomplishes this.

The general properties of DLT’s are Tamper-Resistance, Transparency, Zero-Trust, Anonymity, “Single Source of Truth,” and Decentralization.

* **Tamper-Resistant** – it is unfeasible to change or delete records – only the addendum of new records occurs
* **Transparency** – any user may view the activity of public networks (and any user with the appropriate permissions may view it on private networks)
* **Zero-Trust** – a majority of the network nodes (51% or more) must agree on which transactions occur. This is called **consensus**.No one has to trust any one specific entity.
* **Anonymity** - although network transactions are viewable, there is no personal nor private information shared with the network
* **“Single Source of Truth**” – after a consensus, all nodes on the network have the same copy of data records – everyone’s “books” will look the same
* **Decentralization** - no one entity has the authority to change any transactions or records after they are confirmed by the network

Once information is stored in a distributed ledger, it is essentially tamper-proof, and cannot be removed. To add a record to this ledger, the participants of the network must agree in a majority that the information is correct. This agreement is called consensus. In short, it is a distributed network, and once at least 51% of the devices on the network agree that a transaction happened, the network reaches consensus, the addition is considered confirmed, and the data is added to the record. There are various consensus methods, and they may be tailored for public, permissioned, or private networks.

## Blockchains, Directed Acyclic Graphs (DAGs), and more

The solution to a zero-trust, distributed system was created in 1991 by Dr. Stuart Haber and Dr. Scott Stornetta. This system was created as a method to digitally time stamp documents, but much has changed. Bitcoin, which many think of when the term ‘blockchain’ is used, took the idea of ‘crowd verification’ and used this as an attempt to solve online payments in the early days of the commercial internet. As innovations continue to demand more eloquent answers to an evolving landscape, there are several types of distributed networks, but the two most common are the blockchain and the directed acyclic graph (DAG).

*Diagram

Description automatically generated*

*Image Source: Wikimedia Commons*

**Blockchain** is elegant in its simplicity – all transactions are individually **hashed** (converted into a random number of a fixed size), then those hashes are paired and hashed again, but together. This hashing brings extra layers of protection to the data – both with privacy and security. After this step, the block is then time stamped by the network, a random number used only once (Nonce) is generated. The last ingredient is the “Prev\_Hash” which is the hashed value of the previous block. Once these four items are generated, this “block” of information is ‘minted’ and added to the growing chain of “blocks.” In this way, each block of information is dependent on the previous – this is how the term Blockchain was created.

*Diagram

Description automatically generated*A **Directed Acyclic Graph** structure is also a distributed network of nodes, but it operates in a much different fashion. DAG structures vary considerably, which is one of the strengths of this style of network. In a blockchain network, each block is dependent on the previous one (for the previous block’s hash) to maintain a ‘chain’ of immutable records, but a DAG allows for different pathways for different workflows. DAG structures allow for data to be specifically driven to node or through a pathway, as opposed to one continuous *Image Source: Wikimedia Commons*

chain. Like how a CEO might send an email company-wide, rather than send the information to her directors to forward necessary bits to their managers, and on downward – a DAG allows for direct transmission of data through a specific pathway or to specific nodes, as opposed to a single chain.

As such, DAGs typically process data more quickly and records and nodes may be built simultaneously.

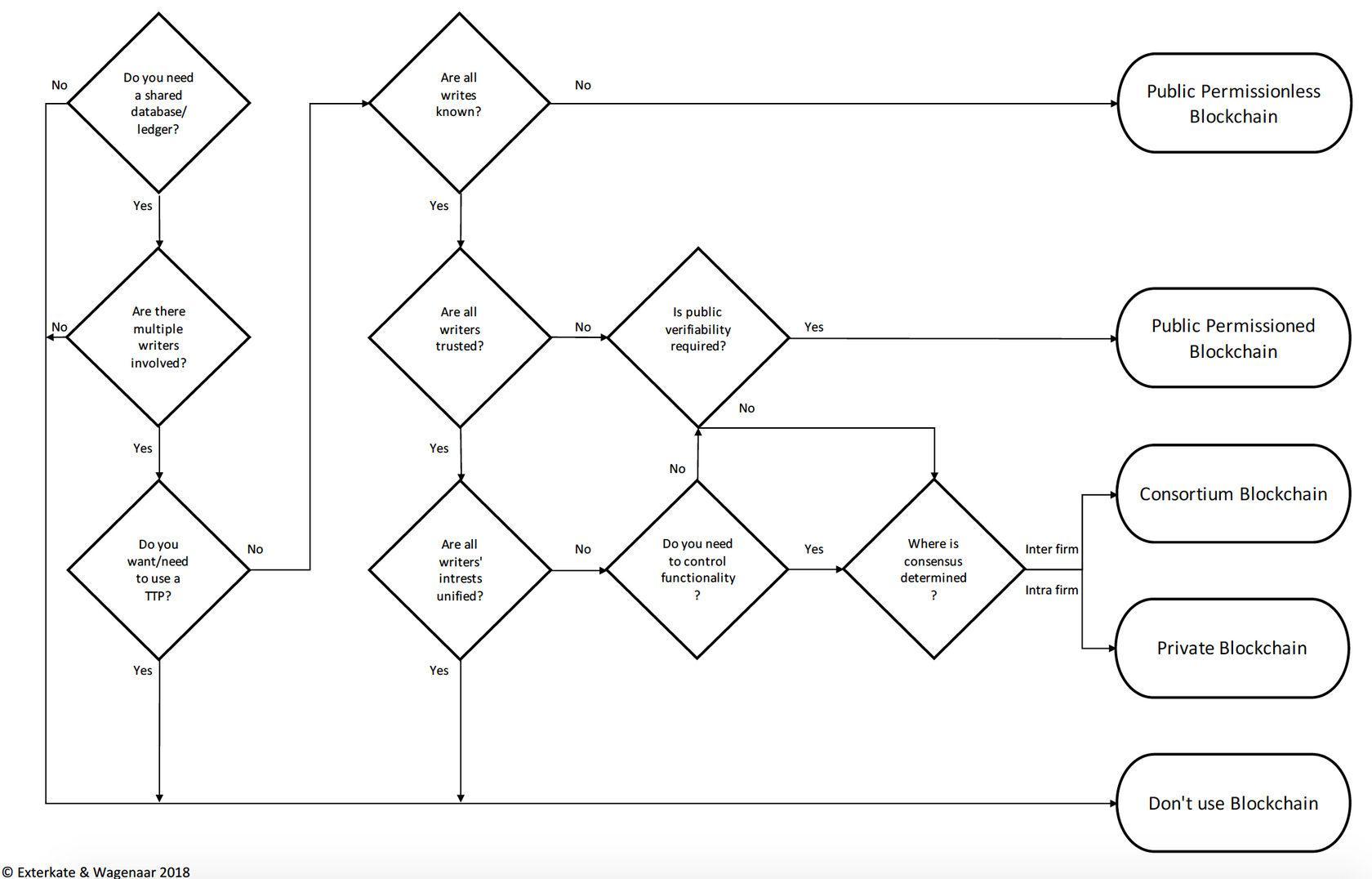
The world of distributed ledgers is rapidly changing to suit the needs of a market that is still seeking solutions to use cases that until recently only had complex and bottlenecked solutions.

# Public and Private DLT’s

Common distributed networks are either public or private. Public, permissionless networks allow anyone to verify transactions and participate in consensus building by being a node. Most cryptocurrencies are run on networks such as these. Private networks, on the other hand, are typically used for small groups of people where permissions may be granted for handling sensitive data.

In the case of private blockchains, or permissioned blockchains, participants must be invited to the network. They need the proper credentials to join the network and to participate in its transactions. The participant’s identity and assigned permissions determine what information the participant may access or record on the ledger. An example of a private DLT network for federal agencies could consist of one or more agencies, departments, commercial service providers, industry partners, and other regulatory bodies. There are also network options that could be used to allow public visibility of tasks, discussions, and data. This type of network, for example, could allow for governance by officials and verified, up-to-date information to the public.

In summary, permissionless ledgers do not require authorization and are accessible to the public for use. Private DLT networks require authorization to perform a particular activity or activities and are accessible for use only to a limited group of known users.

*Image Source: Wikimedia Commons*

# Consensus Mechanisms

One of the critical aspects of a DLT is to ensure that the information maintained by the nodes of the network eventually becomes identical. For this to occur, the state of the data in the ledger needs to be proposed, decided, approved, accepted, and validated by the different nodes. This is the role of the consensus mechanism. In other words, consensus is an umbrella term given to the variety of ways to assure the accuracy of a distributed ledger and accept or reject changes across the network.

Different DLT networks may use different consensus mechanisms to update the state of their network. These protocols focus on a certain number of properties to come to consensus on the state of the network.

The choice of consensus mechanism may also have an impact on things like transactions throughput (the number of the transactions that can be added to the ledger per unit of time), validator centralization (e.g., having a small number of validator nodes in a delegated consensus model compared to the rest of the nodes in the network) or resource usage (does it require a lot of energy, storage, etc.). The field of consensus mechanisms is still an active research area. There are many different mechanisms that have been proposed ranging from theories, test, development to battle tested.

## Examples of Consensus Mechanisms

Popular cryptocurrencies Bitcoin, and Ethereum until recently, uses a Proof-of-Work (PoW) method. In PoW, the nodes use their resources to solve a cryptographic puzzle (a difficult math problem). The first to solve the puzzle is rewarded for verifying the network. The Proof-of-Stake (PoS) method is becoming more common, and it is the consensus mechanism found in Ethereum now, as well as other popular chains such as Cardano. In PoS, people stake a digital asset to have the chance to be chosen as a validator of a new block, collecting the transaction fees from the block as a reward. So, PoW uses computing power for verification - whoever solves the equation first is rewarded, and PoS uses a random method for choosing the validator to reward, and incentivizes nodes on the network hold assets, rather than trade them, because the more assets they stake, the greater the chance of being selected as the validator and rewarded.

These are currently the two most common consensus mechanisms, but there are many more being developed. This can quickly become a very complex topic; however, the important point is that the consensus mechanism used by a distributed network is how additions are agreed upon and accepted.

Timeline

Description automatically generated

*Image Source: Value Technology Foundation*

# Smart Contracts

The term “smart contract” is attributed to Nick Szabo, an American computer scientist, who coined the term in 1998. In its simplest form, it may be thought of as an ‘if, then’ function. A smart contract verifies that preconditions of an event are met, and then carries out the determined action. In its most basic form, this is like a vending machine. Money is added, a selection is chosen, the machine checks that those preconditions are met, and then delivers the product.

The confirmation of a smart contract falls to a consensus of participants. It is recorded on the network and executed. A single smart contract can only be used for one type of transaction; thus, most decentralized applications bundle smart contracts together to create a synergistic, functional set of actions. By using a set of smart contracts, one may even prepare an intermediary contract which would contain transaction details, create caveats, and implement an option to allow for reversibility - essentially, bundled smart contracts can be used as an arbitrator, escrow, closing agent, all at the same time. This type of model allows for the flexibility of interested parties to further negotiate, all without involving a third party, and the participants can do this instantaneously. These functions may allow for building permits, government grants, marriage licenses, and, of course, financial transactions.

# Governance

DLT offers the opportunity to unify around fair rules and regulations, which are automatically enforced and visible to everyone. This transparency allows participants to feel confident in a system that does not require a trusted third party - such as a bank. It extends to a broad array of areas in the administrative and operational side of government which include policymaking, oversight, and enforcement mechanisms.

Blockchain network design employs various governance methods found in enterprise architecture, application architecture, and interoperability. It also features various decision-making mechanisms that include the incentive structure and the consensus protocol. Lastly, there are also organizations, accountability, and control of governance at the micro, macro, and global levels.

Understanding DLT-enhanced policymaking and the frameworks, the business processes, stakeholders, and desired outcomes requires a holistic approach, as applications of decentralized ledger technologies in the public sector overlap political, societal, managerial, and legal arenas.

# Digital Assets

Blockchain technology is called DLT because it acts as a ledger in the traditional sense. Transactions are logged in a secure, immutable, and transparent way. These transactions occur in a peer-to-peer network. This uniquely enables a system where programmable digital assets, or tokens, can be used and accounted for in transactions. These tokens are either native to a blockchain protocol, being programmed initially with the network and part of the infrastructure, or tokens may be independently developed and used on various networks. Some networks are faster, more reliable, having different ways to verify transactions, and may be preferable to developers.

With the advent of Bitcoin in 2009, the ‘purpose’ of DLT shifted focus to financial transactions since the ownership of tokens is verifiable. Much like today’s commonplace electronic payments, Bitcoin was invented to allow people to purchase things electronically in a digital age, but globally – without boundaries, borders, or currency exchanges. In the years since, different types of tokens have been ideated, created, and used for different things. Tokens may be used as payments, consensus rewards, to operate smart contracts, or even as art or music. The two types of tokens may be classified as fungible or non-fungible.

1. **Fungible** tokens are tokens which are completely interchangeable. Fungibility is one of the key properties of currency – although each U.S. Dollar has a different serial number, they all represent the exact same thing. Fungible tokens are the same way – all digital assets have different and unique ID’s, but fungible tokens serve as digital coins and enable payment systems. They may also be broken down into portions (like the U.S. dollar to coins) where they represent a portion of the whole.
   1. **Cryptocurrency tokens** are fungible tokens and refer to any tokens that are used as a medium of exchange or payment. This would include bitcoin itself, as well as the many thousands of ‘altcoins.’
      1. **Stablecoins** are a specific type of cryptocurrency which are designed to hold a specific value, such as a token which represents $1 U.S. Stablecoin tokens should minimally fluctuate in value.
   2. **DeFi (Decentralized Finance) tokens**are a new world of cryptocurrency-based protocols that aim to reproduce traditional financial-system functions (lending and saving, insurance, trading). Some have been developed as an alternative to these systems, and other have been designed to transform these systems to eliminate the need for third parties. DeFi tokens are characterized by utilizing smart contracts to achieve these goals.
   3. **Governance tokens** give people that hold them voting rights for the direction of the network. Because these applications are decentralized, there is no CEO or Board of Directors. The people holding governance tokens vote on different projects or upgrades on the network. Typically, the more governance tokens that someone holds, the more votes they have.
2. **Non-Fungible Tokens (NFTs)** NFTs represent ownership rights to a unique digital or real-world asset. NFTs are designed to be unique, like a painting, rather than fungible, like a currency. Nearly any digital file may be made into an NFT – pictures, art works, music, videos, electronic games, documents, etc. As such, NFTs have some special properties that have been widely touted amongst creators: they may be created so that any secondary sales of the items automatically pay the creator a small percentage of the sale price.

It is worth noting that NFTs do not convey ownership rights of the content, but only ownership rights of the code itself. For example, a musician may make a song, record it, and turn it into an NFT for sale. Anyone who purchases the NFT does not necessarily own the rights to the song – those stay with the creator. The purchaser in this case would simply own a piece of music on DLT rather than on vinyl.

# Web 3.0 ([aka Web3](about:blank)) and Decentralization Text Description automatically generated

Distributed ledger networks have been revolutionizing the world with cryptocurrency, smart contracts, and, more recently, NFTs; but wait, there’s more. One of the landmark transitions that emerged in 2021, we witnessed the advent of Web 3.0. Web 3.0 is the next generation of the Internet – one running on a decentralized system and dubbed “The Internet of the future.” Web 3.0 is a transformative way of delivering the Internet based on Blockchain technology.

Web 1.0 was when the Internet was first introduced - it enabled access to information. Web 2.0, the era we are currently in, has enabled us to interact with one another. Email, search engines, social media, and vendor-enabled marketplaces. This has led to an information explosion, but also data exploitation by tech giants who provide these platforms. There is a growing concern about data privacy. An increasing number of the many applications use emerging technologies, such as artificial intelligence, with products designed to influence our citizenry on the way we think, act, and interact with each other.

This growth has led to the concept of having a decentralized version of the Internet that could empower consumers to own their data which could only be possible with the power of DLT. This technology would allow for access and identity management with its integral properties of immutability, data integrity, and security. The ability to provide individual users the control of their own data, without any platform owners, makes it possible to equalize the Internet for everyone. Applications of Web 3.0 would include enhanced versions of search engines, marketplaces, and social media platforms built on top of DLT where users own their data. This may even allow development of a **metaverse**, which could position the internet for Spatial web.

Web 1.0 was based mostly on click and type websites with a read-only architecture, and Web 2.0 started with the ability to email and chat – currently, it is largely driven by mobile applications. Web 3.0 will be a truly transformational experience in terms of an immersive environment which combines gestures using IoT (Internet of Things), sensors, and augmented and virtual realities within the UI (User interface) layer. The foundational layer of Web 3.0 is the distributed ledger. The middle layer, currently cloud computing, would change to decentralized computing, and the UI could be the metaverse, providing a rich, contextual sensory experience. By default, and design, Web 3.0 provides privacy, trust, immutability, as well as interoperability; however, Web 3.0 is not without its challenges.

The main challenge is scale, especially in the context of organizations. The other crucial challenge is the ethical aspects of the various emerging technologies that are used in conjunction with each other – AR (Augmented Reality), VR (Virtual Reality), Metaverse, IoT sensors, etc. Ensuring every component upholds the ethical aspects would be a large task for any organization. Lastly, distributed ledger has tamper-resistant records, so it could be extremely difficult if a record needs to be edited or removed.

# Next Steps

Planning for an evolving future requires foresight, knowledge, and a team approach that breaks down silos of information. It is not fiscally sound nor prudent to reinvent the wheel with what others have already done. DLTs such as blockchain have been successfully utilized, researched, and reviewed, by countries around the world.

This document is simply meant to*: inform, to compare, contrast, review lessons learned, and identify best practices* to start the process of considering what the possibilities are. The next step is evaluation and implementation – [the ACT-IAC Blockchain Playbook is found at this link](about:blank).

# Glossary

**Blockchain:** A digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network.

**Centralization (and Decentralization):** Centralization occurs in a system where a small number of people involved in a project are the exclusive decision makers of the direction of the project. Decentralization is when everyone involved in the project are considered decision makers or voters.

**Consensus**: Consensus is an agreement among DLT nodes that 1) a transaction is validated and 2) that the distributed ledger contains a consistent set and ordering of validated transactions. It is an umbrella term given to the variety of ways to assure the accuracy of a distributed ledger and accept or reject changes across the network.

**Cryptographic Hash**: A cryptographic hash functions as a digital fingerprint of data. These fingerprints can be generated and used to very easily determine if two data sets match. This allows two or more parties to verify the accuracy of data without sharing the actual data.

**Cryptography:** Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.

**Cryptocurrency**: Any form of currency that only exists digitally. This usually has no central issuing or regulating authority, but instead uses a decentralized system to record transactions and manage the issuance of new units. It also relies on cryptography to prevent counterfeiting and fraudulent transactions.

**Digital Asset**: A digital asset as an asset that exists only in digital form, or which is the digital representation of another asset. Digital assets exist in a computerized, binary format and all come with the right to use. Anything without the right to use is not a digital asset. These include but are not exclusive to digital documents, audio content, motion picture, and other relevant digital data that are currently in circulation or are or will be stored on digital appliances.

**Distributed Ledger**: A distributed ledger (also called a shared ledger or distributed ledger technology or DLT) is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. Unlike with a centralized database, there is no central administrator.

**Node**: In communication networks, a node is either a redistribution point or a communication endpoint. In a peer-to-peer, distributed system like blockchain, every server touch-point is a node. Within blockchain, it is the computer connected to the blockchain network using a client that performs the task of validating and relaying transactions.

**Permissionless or Public Distributed Ledgers**: Permissionless is not requiring authorization to perform activities, and public DLT is a system which is accessible to the public for use. Participants maintain the integrity of the ledger by reaching a consensus about its state. Public ledgers are used as a tamper-resistant record in a trustless and broad network.

**Permissioned or Private Distributed Ledgers**: These are ledgers where participants must be invited to join and various permissions requiring authorization to perform certain activities. In other words, a permissioned distributed ledger allows access to identical copies of a ledger to a limited number of preselected trusted participants only. Private ledgers may have one or more owners and are most suitable for inter/intra organization use cases, requiring simplicity, speed, and greater transparency, where there is some level of trust between participants.

**Smart Contracts**: A smart contract as a computer program stored in a DLT system wherein the outcome of any execution of the program is recorded on the distributed ledger. In other words, smart contracts are small computer programs operate on a DLT. They render transactions traceable, transparent, and irreversible.

**Stablecoin**: A digital currency which is pegged to a stable (fiat) currency.

**Transaction:** A transaction is the smallest unit of a work process, which is one or more sequences of actions required to produce an outcome that complies with governing rules. In the context of blockchain, a transaction is a transfer of assets between parties.

# Additional Recommended Reading

1. ACT-IAC Blockchain Playbook
2. How to Time Stamp a Digital Document – Dr. Stuart Haber and Dr. Scott Stornetta
3. Bitcoin Whitepaper - Satoshi Nakamoto
4. Government Office for Science: Distributed Ledger Technology: Beyond Blockchain (A report by the UK Government Chief Scientific Adviser)
5. White House Executive Order on Ensuring Responsible Development of Digital Assets
6. United States Government Accountability Office Technology Assessment of Blockchain
7. NIST: Blockchain Networks: Token Design and Management Overview
8. 2018 Public-Private Analytic Exchange Program: Blockchain and Suitability for Government Applications (DHS)
9. MITRE: Assessing the Potential to Improve Grants Management Using Blockchain Technology
10. Coinbase: Crypto Basics
11. The Blockchain Blockbuster: Yapese Stones to Central Bank Digital Currencies (Macro Strategy)
12. Blockchain Glossary of Terms: 128 Blockchain Terms and their Definitions
13. Blockchain Technology in Healthcare: A Systematic Review (NIH)
14. [Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges | U.S. GAO](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gao.gov%2Fproducts%2Fgao-22-104625&data=05%7C01%7C%7C3604ee9bc0814b2d0f6208db05fec10e%7Ce95f1b23abaf45ee821db7ab251ab3bf%7C0%7C0%7C638110363955058787%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=jSs7iMuNcVxlRyE0P86jFHooGwKrnYOGot4gGtnJwXA%3D&reserved=0)
15. [Science & Tech Spotlight: Blockchain & Distributed Ledger Technologies | U.S. GAO](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gao.gov%2Fproducts%2Fgao-19-704sp&data=05%7C01%7C%7C3604ee9bc0814b2d0f6208db05fec10e%7Ce95f1b23abaf45ee821db7ab251ab3bf%7C0%7C0%7C638110363955068761%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=A8T0cRNnUJHvgMOnVCOggfmuDHVsL0Qjft74Qfabbhg%3D&reserved=0)
16. [Science & Tech Spotlight: Non-Fungible Tokens (NFTs) | U.S. GAO](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gao.gov%2Fproducts%2Fgao-22-105990&data=05%7C01%7C%7C3604ee9bc0814b2d0f6208db05fec10e%7Ce95f1b23abaf45ee821db7ab251ab3bf%7C0%7C0%7C638110363955078721%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=t0OxMplXEt7unBLeavo8M2xsyxozgkBv%2BlcOw6J7UOY%3D&reserved=0)
17. [Trafficking: Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking | U.S. GAO](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gao.gov%2Fproducts%2Fgao-22-105101&data=05%7C01%7C%7C3604ee9bc0814b2d0f6208db05fec10e%7Ce95f1b23abaf45ee821db7ab251ab3bf%7C0%7C0%7C638110363955088669%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=WDRWa83SxRNr637wTN0DqFd6amlNQyRg8a%2FIJUd7Viw%3D&reserved=0)
18. [Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking [Reissued with Revisions Feb. 7, 2022] | U.S. GAO](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gao.gov%2Fproducts%2Fgao-22-105462&data=05%7C01%7C%7C3604ee9bc0814b2d0f6208db05fec10e%7Ce95f1b23abaf45ee821db7ab251ab3bf%7C0%7C0%7C638110363955108581%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=ijJcYYrQ3SI8ELdklOihwEZyXlhs9z%2FdTd7fujlM02o%3D&reserved=0)
19. [Virtual Currencies: Additional Information Reporting and Clarified Guidance Could Improve Tax Compliance | U.S. GAO](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gao.gov%2Fproducts%2Fgao-20-188&data=05%7C01%7C%7C3604ee9bc0814b2d0f6208db05fec10e%7Ce95f1b23abaf45ee821db7ab251ab3bf%7C0%7C0%7C638110363955118532%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=L9sfzDFXItr279f9hQ4O%2BlqWGTmGT6XeafBTcyWjWoQ%3D&reserved=0)

# Authors & Affiliations

This white paper was written by a consortium of government and industry. The organizational affiliations of these contributors are included for information purposes only. The views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development.

Style = No Spacing. List names here.

# References

***Published Content Review Process***

Below are the stages of the ACT-IAC review process. Once all comments from the paper’s current review stage have been addressed it moves on to the next review stage.

Stage 1 – Peer review by COIs involved

Stage 2 – three independent (meaning not part of the project team); report sponsor/ government stakeholders members of the paper’s target audience.

Stage 3 – COI/Working Group internal leadership (Chairs/Vice chairs, Advisor, Advocate).

Stage 4 – ACT-IAC Staff support, which typically creates some changes to ensure alignment with policies and procedures for white papers and executive reports; then on to the Sr Director of Strategic initiatives, and the Executive Director for final release. Typically following the review of the assigned EC Advocate and the ACT-IAC Staff support, the Sr. Director of Strategic Initiatives and the Executive Director review is cursory in nature.

***Distribution of Draft Content***

White papers, issue papers, and other documents produced by a COI that are not yet final shall only be available to those parties working on the documents. Once the work product has been finalized and gone through the approval process, it will be available to the public via the ACT-IAC website and through other distribution channels as appropriate. The following guidelines outline the handling of the draft paper during the review period:

A draft white paper shall have the following statement in the header of every page: “*This is a draft document provided solely for review purposes. This document may not be cited, quoted, distributed or otherwise used prior to release of the final version by ACT-IAC.*”

Each page shall also include a watermark reading **ACT-IAC DRAFT**.

Every copy sent for review shall include a cover page that says “*Please note that this is a draft version submitted for your review only; further distribution or publication is expressly prohibited by ACT-IAC policy.*”