

# Blockchain Task Force

## USE CASE ASSESSMENT

# Blockchain Task Force

## Technical Framework— Justice and Public Safety

**Akbar Farook**  
*Global Justice Solutions*

**Josh Jackson**  
*Emory University*

**Jim Kita**  
*Analysts*

**Anil K. Sharma**  
*IBM*

**Anne Thompson**  
*Thompson | Finn LLC*

**Steven White**  
*Missouri State Highway Patrol*



**IJIS Institute**

# Acknowledgments

This document is an IJIS Institute product, which is a nonprofit alliance working to promote and enable technology in the public sector and expand the use of information to maximize safety, efficiency, and productivity.

## IJIS Mission

To drive public sector technology innovation and empower information sharing to promote safer and healthier communities.

## IJIS Blockchain Task Force Team

Maria Cardiello <i>IJIS Institute</i>	Tom Messerges <i>Motorola Solutions</i>
Paul Embley <i>National Center for State Courts</i>	Greg Park <i>City of Livermore</i>
Akbar Farook <i>Global Justice Solutions</i>	Anil Sharma <i>IBM</i>
Alex McAdoo <i>IJIS Institute</i>	Andrew Owen <i>SEARCH</i>
Di Graski <i>National Center for State Courts</i>	Anne Thompson <i>Thompson   Finn LLC</i>
Josh Jackson <i>Emory University</i>	Eric Tumperi <i>CorrectTech</i>
Jim Kita <i>Analysts</i>	Steven White <i>Missouri State Highway Patrol</i>

## Additional Contributors

The following individuals provided invaluable review and feedback.

Steve Albonico <i>Blockchain Engineer, Boeing</i>	Susan Keilitz <i>National Center for State Courts</i>
Ashwini Jarra <i>IJIS Institute</i>	Shelley Spacek <i>National Center for State Courts</i>
Bob Kaelin <i>MTG Management Consultants</i>	Iveta Topalova <i>Microsoft Corporation</i>

## Comments and Questions

Your comments and questions are welcome! Please contact the IJIS Institute at [info@ijis.org](mailto:info@ijis.org) or 1-703-726-3697.

## Executive Summary

This document aims to help those in information management and exchange roles within the justice and public safety communities to better understand how blockchain technology addresses challenges when managing and sharing information among agencies at the local, state, and federal levels.

Specifically, it provides a high-level view of blockchain technology, including a business assessment framework, technology and regulatory considerations, and a case study for warrant issuance and management.

The IJIS Blockchain Task Force set out to:

- Attempt to explain the technology that supports blockchain frameworks;
- Provide a high-level understanding of what to consider when establishing a new blockchain or using an existing blockchain;
- Help evaluate technical considerations to determine whether the blockchain technology is appropriate for a use case of interest; and
- Describe how to evaluate whether blockchain technology can support:
  - Specific business needs not met by other technologies; and
  - Current and potential regulatory considerations.

The task force used the following definition for blockchain from *Hackernoon*<sup>1</sup>:

*“A blockchain is a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks (rather like collating them on to a single sheet of paper). Each block is then ‘chained’ to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions.”*

Our working hypothesis is that blockchain technology offers the potential to meet stakeholders’ needs who manage and share information related to sensitive data, which ensures that shared information is:

- Authoritative (i.e., pertaining to signing authority, jurisdiction, and available services);
- Authentic (i.e., valid and current); and
- Auditable (i.e., accurate record and timeline of document interaction).

Various organizations, such as SEARCH and the National Center for State Courts (NCSC), completed work that establishes a basis for awareness and usage standards related to data exchange regardless of technology.

### Benefits of Blockchain for Justice and Public Safety

The major benefits of using blockchain technology for information sharing include:

- Immediate access to an authoritative record;
- High level of data security and ability to see who accessed or updated a record;
- Assurance of the record’s validity or integrity; and
- Assurance of the record’s authority and status.

While implementing this technology among justice partners requires additional collaboration and governance, the value of independently operating agencies’ ability to immediately access an authoritative, valid, and auditable record, such as a protective order, cannot be understated. Blockchain Business Assessment Framework cost elements for implementing blockchain to manage data exchange between agencies resemble those involved for an individual agency managing its

<sup>1</sup> Jordan Odinsky. “Blockchain Dictionary.” Hackernoon.

own records and technology infrastructure.

They cover various areas, including:

- On-premise or cloud-based software;
- Governance and identity, as well as access management;
- Number of required participating nodes;
- Initial and ongoing development;
- Network infrastructure and management;
- Business process continuity and disaster recovery;
- Operation and maintenance; and
- Licensing.

Agencies will likely have different “value drivers” for ensuring that records remain authoritative, current, and auditable. These “value drivers” include:

- Safety perspectives for law enforcement and / or victims;
- An obligation to monitor and report on data security;
- Greater transparency in a justice/law enforcement information exchange process; and
- More accurate evidence-based reporting, etc.

A useful first step includes agencies working together to define shared value compared with current business processes.

### **Blockchain Technology Considerations**

Several architecture considerations are necessary when building a blockchain system. Fundamentally, many considerations remain the same (e.g., network, hardware, etc). However, a few considerations differ, including:

- Participant organization guides blockchain structure decision-making;
  - Public – A large number of equally untrusted parties exists.
  - Private – All participants are known and trusted.
  - Consortium – All participants are known with limited trust.
- Consensus Protocols are the fundamental rules for how the blockchain runs and builds trust in the blockchain ledger;
- SMART Contracts are the business logic for interacting with the blockchain;
- The On-Chain vs. Off-Chain discussion examines how much data can realistically be maintained by the blockchain and how to manage unincorporated chain data;
- Throughput determines how fast the blockchain can record new transactions;
- Identity Management governs how parties in transactions prove who they are and what authority they must have to participate in blockchain transactions; and
- Interoperability determines the extent in which standards exist for blockchain platforms to interface with line-of-business systems and between blockchain platforms.

Platform options condense the above considerations and apply the factors to current and commonly available blockchain platforms.

<sup>2</sup> George ‘Geo’ Bellas. “Blockchain as Evidence.” Illinois State Bar Association.

<sup>3</sup> Ibid.

## Regulatory Considerations

Regulatory considerations for agencies considering blockchain technologies to exchange sensitive data include evidentiary and data privacy rules, regulation, and legislation. Agencies contracting with blockchain technology providers must clearly understand who bears responsibility for accurate code and data quality assurance.<sup>2</sup> For example, does your state have legislation in place that defines the digital record created using blockchain technologies as authoritative?<sup>3</sup>

## Case Study

In order to better understand the benefits and challenges of applying blockchain technology to the justice and public safety domain, Global Justice Solutions developed a proof-of-concept application called “JustChain,” which demonstrates warrant management (e.g., search warrants, bench warrants, and arrest warrants), along with a white paper discussing the exercise. A summary of the proof-of-concept is included as a case study (See Section 13), along with diagrams and screenshots showing the application behavior.

## Conclusion

There is an increasing demand to share information among agencies at the local, state, and federal levels and a need to comply with data privacy and security requirements.

The Task Force concluded that the benefits of ensuring an authoritative source, maintaining an up-to-date and valid document, and auditing a document’s history for interaction justify additional investigations. This can be achieved by bringing stakeholders together to discuss the development of a limited scope proof of concept.

Along with technical feasibility experimentation, a proof of concept would help explore optimal funding and procurement, data governance, and organizational models among participating local, state, and federal agencies and their vendors. The steps to create a business case for using blockchain technology are no different than those required for any technology investment. What is unique when considering blockchain technology is that the business case requires establishing “shared value” across participating agencies, all of which likely have different priorities and resources. What may be the most important use case or priority for law enforcement may be different than those for court, corrections, victim services providers, or other partners.

Focusing on how the solution benefits the constituent (e.g., the petitioner for a protective order<sup>4</sup>) may be a way to work through each agency’s priorities and agree upon the shared value and benefits across organizations.

<sup>4</sup> IJIS Institute. “Use Case—Protective Orders.”

# Table of Contents

- 1** Introduction..... 8
  - 1.2 Purpose* ..... 8
  - 1.3 Task Force*..... 8
  - 1.4 Audience*..... 8
  - 1.5 Blockchain Definition*..... 8
  - 1.6 Justice and Public Safety Challenges* ..... 8
  - 1.7 Benefits of Blockchain for Justice and Public Safety* ..... 9
- 2** Blockchain Business Assessment Framework..... 10
- 3** Blockchain Technology Considerations..... 12
  - 3.1 Private, Public, Consortium* ..... 12
  - 3.2 Consensus Protocols*..... 13
  - 3.3 SMART Contracts*..... 21
  - 3.4 On-Chain vs. Off-Chain* ..... 21
  - 3.5 Throughput* ..... 23
  - 3.6 Identity and Access Management*..... 23
  - 3.7 Interoperability*..... 31
  - 3.8 Platform Options* ..... 35
- 4** Regulatory Considerations ..... 37
- 5** Potential Justice and Public Safety Use Cases ..... 38
- 6** Case Study: Search Warrant, Bench Warrant, Arrest Warrant on Blockchain™ ..... 39
  - 6.1 Introduction*..... 39
  - 6.2 Use Case*..... 39
  - 6.3 Blockchain Implementation Details*..... 40
- 7** Conclusion..... 43
  - Appendix A. Acronyms ..... 44
  - Appendix B. Glossary..... 47
  - Appendix C. References..... 47

## Table of Figures

<i>Figure 1. Examples of Blockchain Models.....</i>	<i>12</i>
<i>Figure 2. SMART Contract Snippet in Solidity .....</i>	<i>21</i>
<i>Figure 3. Blockchain Structure: Block Frame .....</i>	<i>22</i>
<i>Figure 4. Block Structure: Chained Blocks.....</i>	<i>22</i>
<i>Figure 5. Pure Identity Model .....</i>	<i>25</i>
<i>Figure 6. High-level Illustration of the Federal PKI Certification Authorities .....</i>	<i>26</i>
<i>Figure 7. The Anatomy of a Digital Certificate.....</i>	<i>27</i>
<i>Figure 8. How Decentralized Identity Works (Microsoft) .....</i>	<i>28</i>
<i>Figure 9. Sample DID Scenario (Microsoft).....</i>	<i>29</i>
<i>Figure 10. Using Channels to Manage Access .....</i>	<i>30</i>
<i>Figure 11. Using Smart Contracts and Channels to Manage Access .....</i>	<i>31</i>
<i>Figure 12. Search Warrant Use Case from JUSTICE CHAIN LLC.....</i>	<i>40</i>
<i>Figure 13. Arrest / Bench Warrant from JUSTICE CHAIN LLC .....</i>	<i>41</i>
<i>Figure 14. Arrest / Bench Warrant from JUSTICE CHAIN LLC .....</i>	<i>40</i>
<i>Figure 15. Arrest / Bench Warrant from JUSTICE CHAIN LLC .....</i>	<i>42</i>
<i>Figure 16. Arrest / Bench Warrant from JUSTICE CHAIN LLC .....</i>	<i>42</i>

## Table of Tables

<i>Table 1. Consensus: Key Concepts, Categories and Protocols.....</i>	<i>14</i>
<i>Table 2. Most Common Consensus Protocols .....</i>	<i>15</i>



# 1 Introduction

## 1.2 Purpose

This document provides a technical framework for public sector justice organizations to understand blockchain or distributed ledger technologies, as well as how and in what instances they should be considered when evaluating solutions for use cases and appropriate characteristics (e.g., security and transparency, shared (peer-to-peer) network, immutability, and method for achieving consensus on transactions).

## 1.3 Task Force

The IJIS Blockchain Task Force was established in July 2018 following the 2018 annual IJIS Symposium. At the symposium, we produced ten potential use cases (see section on Potential Justice and Public Safety Use Cases) that could benefit from the unique characteristics distributed ledger technology provides, such as security, transparency, immutability, auditability, shared administration, and governance.

The Task Force has two goals:

- Provide an assessment regarding technology suitability for one of the identified use cases and an evaluation framework for other use cases; and
- Provide a high-level technical framework focused on the specific challenges and opportunities when adopting the technology for justice and public safety organizations.

The focus and scope of this document remain on the second goal: It is a companion document to the use case assessment document and provides a high-level view of the technology framework.

## 1.4 Audience

This document was developed for public sector executives and managers who oversee and share information related to protective orders. They include judicial officers, court administrators and technology employees, local, state, and federal law enforcement, corrections and advocacy officials, and victim support agencies. The use case for blockchain is discussed in the companion document “Use Case Assessment—Protective Orders.” This document explains the technology and how it might be applied to existing records management technologies to better manage and audit information exchange among justice sector agencies.

## 1.5 Blockchain Definition

There are many definitions for blockchain. For clarification, we use the following from Hackernoon:

*“A blockchain is a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks (rather like collating them on to a single sheet of paper). Each block is then “chained” to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions.”*

## 1.6 Justice and Public Safety Challenges

Any problem involving interagency records management presents a challenge for proposed changes to existing processes and systems, specifically where the records in question are highly sensitive, the validity, authority, accuracy, and timeliness are critical, and the repercussions from errors are significant. Contributing factors include:

- **Organizational:** Is the organization structured to make change? Complex organizations with hierarchical, formal structures provide additional challenges to achieving stakeholder buy-in and decision-making;
- **Funding / Procurement:** How are budget decisions for technology determined? Who is involved in the decision-making process? How does the cost / benefit of a proposed alternative technology sit alongside other priorities for your department / organization? Are there alternative funding sources?

<sup>5</sup> Jordan Odinsky. “Blockchain Dictionary.” Hackernoon.



- **Data:** The data contained in interagency records is highly sensitive and may be subject to regulatory and legislative requirements with respect to dissemination (time standards), access, availability, management, and governance (controls and auditing). Federal versus state requirements need to be considered regarding sensitive online agency data, as well as requirements related to sealed records and expungement. This is non-trivial and an area where IJIS could inform on regulatory, legislative, and policy changes that benefit all stakeholders;
- **Technology and Standards:** Is the proposed alternative technology developed? Are there standards in place? For example, governance (controls and audit capabilities)? The benefits of an improved process for issuing protective orders must be measurable and account for the above factors in order to provide incentive for change. The key differentiator in using blockchain technology is the potential it provides in simultaneously providing a trusted, authoritative source to multiple parties (e.g., court, law enforcement, petitioner, and service providers);
- **Jurisdictional Considerations:** Some jurisdictions may be a better fit than others depending on whether the state follows a decentralized or centralized model in terms of technology and funding;
- **Decentralized:** For decentralized states, various solutions and stakeholders may make implementation and interoperability more challenging. Decentralized states may have more budgetary flexibility that are not subject to election cycles; and
- **Centralized:** Funding cycles for centralized states may depend on state-level administration and be subject to legislative requirements for budget approval. Competing priorities may make it challenging to prioritize investment, especially involving emerging technologies.

### ***1.7 Benefits of Blockchain for Justice and Public Safety***

While blockchain technology offers many benefits, the following benefits set it apart for justice and public safety agencies:

- **Instant data sharing:** Since everyone on the network has the same copy of the ledger, real-time data sharing is achieved without manually updating partner systems, unlike in traditional centralized systems;
- **Transaction security:** All information on the ledger is cryptographically signed and provides a high level of data security. In addition, participating nodes can use SMART Contracts and Wallets assignments (digital identities) to assist with access control;
- **Integrity:** Since information can only be added to a blockchain, it is practically impossible to modify the information on the ledger, thereby providing a high level of data integrity in the blockchain; and
- **Self-verifiable data:** Since any information on the blockchain can be instantly verified using the data provider's identities, agencies and participants on the chain can be confident that the information comes from the stated source (e.g., protective order signed by a judge), and that there is no room for non-repudiation, which may exist in traditional systems.

## 2 Blockchain Business Assessment Framework

A blockchain network has similar cost elements with any enterprise system. As previously mentioned, given that we are discussing using blockchain as a value add to, or even fully automating current justice/law enforcement processes, the identities of all persons participating in such processes are known before hand as only authorized personnel and organizations may participate in these justice/law enforcement processes. Thus, each authorized participant is required to be provisioned on the blockchain network. Additionally, as part of this provisioning and ongoing management, all users/organizations are assigned process-based roles where every transaction on this blockchain network is associated with a known participant.

For the purposes of cost development, a blockchain network is defined as a group of peer organizations with a set of common needs, processes, and use cases, and a common governing body that provides overall governance. It is a technical infrastructure that provides a distributed ledger and smart contract services to applications, among others.

Primarily, smart contracts generate transactions that are distributed to every peer node on the network where they are immutably recorded on their copy of the ledger. Application users might be end users on client applications or blockchain network administrators. For example, in IJIS' protective order use case, the courts, various lawyers, and law enforcement agencies would be considered as "peer organizations," and organization members would have single identities on the network, but roles vary depending on the specific process or contract. Additionally, as blockchain uses Public Key Infrastructure (PKI) technologies to include PKI-based digital certificates, provisioning and managing are needed.

At a high level, some costs elements include:

- **Server Costs:** Costs for the total number of servers on a blockchain network; also include server software costs;
- **Network Costs:** Network infrastructure and bandwidth costs;
- **Storage Costs:** Data storage costs, including backup media costs;
- **Organization Costs:** Costs related to onboarding and managing different organizations onto the network;
- **High Availability (HA) and Disaster Recovery Costs:** Additional costs for duplicating infrastructure, enabling data replications, and configuring for failover; There are initial setup and ongoing sustainment costs for this;
- **Initial Platform Implementation Costs:** Services and software costs to design, configure, and launch a blockchain network; Note that these include the costs of setting up different peers on the blockchain, with peers being the different blockchain replication elements;
- **Initial Process or Contract Implementation Costs:** Services and software costs to implement the first process on the blockchain network once launched;
- **Ongoing Platform Costs (Sustaining Engineering):** Ongoing sustainment, operations, and maintenance costs of the blockchain network; and
- **Ongoing Process Contract Costs:** Ongoing process management costs; These may also include implementation and management costs for additional processes on the blockchain network.

The above cost elements are included for organizations seeking to launch and operate their own blockchain network on their own infrastructure. Other items that affect costs include the number of environments that organizations may require (e.g., development, testing, production, pre-production, etc.). However, organizations may also use cloud-based blockchain services when costs are on a usage basis. The Cloud Service Provider (CSP) incurs all costs outlined above but provides a cheaper price to its customers. For example, the IBM Blockchain Platform (IBP), a Software as a Service (SaaS) offering based on the Open Source HyperLedger Fabric project, offers the following cost elements<sup>6</sup>:

- **Number of Organizations:** The number of distinct and peer organizations (two or more) that create transactions on the blockchain network for implementation. For each organization, a set of recommended IBP components and supported elements will be set. These organizations are like peers in a consortium that is formed to transact business on the blockchain network;

<sup>6</sup> Open document. "Pricing for IBM Blockchain Platform for IBM Cloud." IBM.

- **Number of Certificate Authorities (CAs) per Organization:** Digital certificates within an organization;
- **Number of RAFT Ordering Service Nodes:** The IBP uses the RAFT protocol and orders validated transactions by peers into blocks and returns them to their peers to be written to their ledgers. Remember that each organization will require at least one copy of the ledger;
- **Number of Peers per Organization:** At a physical level, a blockchain network comprises primarily peer nodes (or peers). Peers are the fundamental network elements because they host ledgers and smart contracts. The peer hosts instances of the ledger and smart contracts. Because smart contracts and ledgers are used to condense shared processes and information in a network, these peers aspects make them a good starting point to understand what a fabric network actually does. An organization has one or more peer nodes depending on workload and High Availability and Disaster Recovery needs. IBP allows peer nodes to be distributed across different zones to facilitate this;
- **Number of CPUs (Cores) per Peer:** This is driven by the peer's processing needs and transaction volumes, as well as the number and complexity of smart contracts;
- **Ongoing Network Costs:** Ongoing network and bandwidth utilization costs;
- **Number of IBM Kubernetes Service (IKS) Zones:** IKS provides the underlying management platform for IBP, as IBP is a container-based platform. For example, three zones allow for disaster recovery configuration;
- **Ongoing Storage Costs:** Ongoing storage utilization costs across all peers;
- **High Availability (HA) and Disaster Recovery Costs:** Additional costs for duplicating infrastructure, enabling data replications, and configuring for failover; There exist initial setup and ongoing sustainment costs for this;
- **Initial Platform Implementation Costs:** Services costs to design, configure, and launch a blockchain network. Note that these costs also include setup costs for different peers on the blockchain – peers being the different replication elements of the blockchain. It also includes any services costs for onboarding different organizations. Infrastructure costs are included in other cost elements as priced by the CSP;
- **Initial Process or Contract implementation Costs:** Services and software costs to implement the first process on the blockchain network once launched;
- **Ongoing Platform costs (Sustaining Engineering):** Ongoing sustainment, operations, and maintenance costs of the blockchain network; While the CSP will provide support for most of these costs, some growth and planning tasks that require technical services support are needed; and
- **Ongoing Process Contract Costs:** Ongoing process management costs; These also include costs for implementing and managing additional processes on the blockchain network.

Note that costs increase as more peers are added. The entire blockchain also needs to be distributed to and replicated for each peering organization so that each organization has its own copy – an underlying principle of the blockchain network. Additionally, from a CSP perspective, most of these cost elements are on a periodic basis.

### 3 Blockchain Technology Considerations

The landscape for blockchain technology and frameworks continues to evolve. When it comes to selecting the right blockchain technology for your organization(s), it is imperative that you take a holistic view before starting the program. There are a few things to consider from a planning perspective. For example, depending on the nature of the program (e.g., protective order), agencies might want to consider whether they need a private, public, or a consortium-based blockchain, what consensus protocols will be used, how documents will be stored (e.g., protective order), if any, identity management for participating entities, etc.

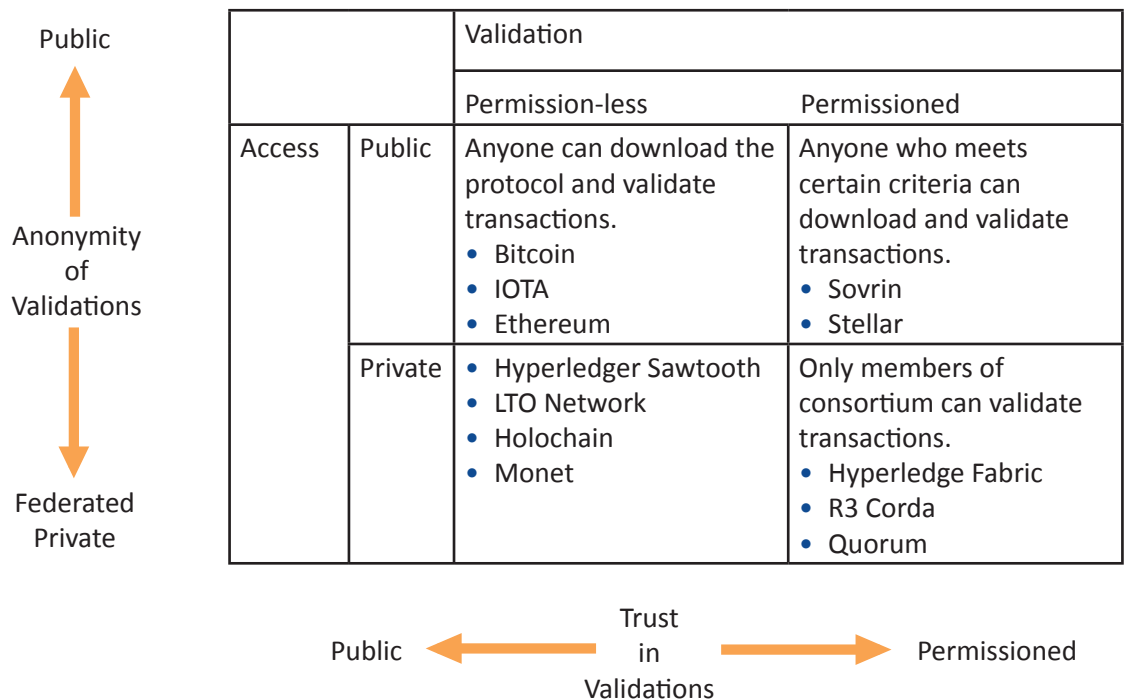
The following section describes common consensus protocols, the method used, and the advantages and disadvantages of each.

#### 3.1 Private, Public, Consortium

One of the first things to consider when implementing a blockchain technology is to determine if it is going to be a private, public, or consortium-based blockchain solution. These are:

- **Private:** In a private blockchain environment, all entities on the chain are pre-determined and only those entities can transact on the blockchain. No other party outside the network can view or transact with the blockchain. This is common if the entities only want to share information within their organization or enterprise;
- **Public:** In a public blockchain, everything on the chain is open to the public (e.g., Bitcoin network, Ethereum network, etc.). Anyone can create an identity on the blockchain and also view information on the public blockchain. It is only useful if an agency wants to send information to the general public (e.g., wanted people, notarizations, etc.); and
- **Consortium:** Consortium blockchains are like private blockchains except with shared permissions between the blockchain entities. Multiple organizations (e.g., criminal justice partners) can form a consortium and share permission access for network transactions. No single organization owns or controls the network.

Figure 1. Examples of Blockchain Models<sup>7</sup>



<sup>7</sup> NeonVest. "The Scalability Trilemma in Blockchain." Medium.

### 3.2 Consensus Protocols

The following section discusses key considerations when selecting a consensus protocol, key concept definitions, and some of the main protocols with examples and characteristics.<sup>8,9,10</sup> Consensus protocols are use case-specific, and this document cannot recommend a specific approach.

#### 3.2.1 Key Considerations

##### 3.2.1.1 Use Case

Assuming you have satisfied the business case for blockchain, a clearly defined use case is the basis for determining the type of consensus protocol. Questions to consider include:

- What type of data are you seeking to exchange?
- What guarantees are required for message delivery among partners (synchronous / asynchronous)?
- Do verified blocks need to be finalized immediately?

##### 3.2.1.2 Blockchain “Trilemma”

The blockchain “trilemma” involves the three concepts of blockchain technology: security, scalability, and decentralization.<sup>11</sup> The term refers to the claim that a blockchain can only have two of these properties. For example, many participants provide more security but with limited scalability.

- Security
  - For justice and public safety organizations using a private, permissioned network, security concerns about how access is determined and managed and who is authorized to create and verify blocks are mitigated by governance. Of course, security must also be considered from the cybersecurity viewpoint of all network participants.
- Scalability
  - How fast do blocks need to be written to the chain? There can be a lot of “hype” around Transactions per Second (TPS). Constituents should consider what speed is required rather than concluding that faster is better.
- TPS may also be represented differently by different sources. For example, R3 Corda compares TPS for a single node (created and verified locally) at 1678 TPS against 170 TPS (for a created and verified block including all participating nodes).
- A trade-off for faster TPS includes larger block sizes or a more compute-intensive protocol, and therefore, impact scalability.<sup>12</sup> As noted above, performance depends on many variables, many of which can be configured and tuned.<sup>13</sup>
- Decentralization
  - How many participants are required to create and verify blocks? Is one node required by all participating agencies? Too many nodes can drastically affect performance.<sup>14</sup>

<sup>8</sup> Ibid.

<sup>9</sup> “Glossary of Blockchain Terms.” Blockchain Training Alliance.

<sup>10</sup> Nick Youngson. “Blockchain Consensus Encyclopedia.” GitBook.

<sup>11</sup> NeonVest. “The Scalability Trilemma in Blockchain.” Medium.

<sup>12</sup> Aat de Kwaasteniet. “The nonsense of ... TPS (transactions per second).” Medium.

<sup>13</sup> Christopher Ferris. “Answering your questions on Hyperledger Fabric performance and scale.” IBM Blockchain Blog.

<sup>14</sup> David Hyland-Wood, Roberto Saltini, Franck Cassez, Joanne Fuller. “Key Factors to Consider When Choosing a Blockchain Consensus Protocol.” Pegasys.

### 3.2.2 Key Definitions

Key concepts and categories for different consensus protocols are defined below.<sup>15</sup>

**Table 1. Consensus: Key Concepts, Categories, and Protocols**

Term	Definition
<b>Protocols</b>	Protocols refer to sets of formal rules describing how to transmit or exchange data, especially across a network. <sup>16</sup> Consensus refers to the approach to reach agreement and validate that exchange (i.e., creating and verifying a block).
<b>Consensus Process</b>	A group of peers responsible for maintaining a distributed ledger used to reach consensus on the ledger's contents.
<b>Proof of Work</b>	All participants can create blocks. The first participant (miner) who provides an answer (or proof) to a specific computational challenge can confirm a transaction and enter it onto the blockchain.
<b>Proof of Stake</b>	Participants who hold either coins or smart contracts, or “stakes,” can create and verify blocks. Those with the highest “stakes” verify new blocks.
<b>Proof of Capacity / Space</b>	Participants who allocate a non-trivial amount of memory, or space, to solve a challenge can create and verify blocks.
<b>Proof of Burn</b>	Participants who prove that they allocated resources (e.g., coins) can create and verify blocks.
<b>Hybrid Models</b>	Models that comprise mostly a combination of existing consensus algorithms.
<b>Trusted Computing Algorithms</b>	These are consensus protocols used with other protocols to ensure fairness during block creation and verification. For example, PoET used in REM and Sawtooth, which require specialized hardware (Intel)
<b>Directed Acyclic Graph</b>	Any participant can create a block, and all participants verify blocks (e.g., transactions and timestamp of transactions) through a randomized process of sending, receiving, and confirming messages with a timestamp about the transactions.
<b>Byzantine Fault Tolerance (BFT)</b>	Voting-based protocol that achieves consensus despite one or more participants failing or behaving maliciously. Crash fault tolerance (CFT) based algorithms, also a voting-based protocol, solve for node failure problems but not malicious attacks. BFT-based protocols include practical byzantine fault tolerance (PFBT), delegated byzantine fault tolerance (dBFT), federated byzantine agreement (FBA), and combined delegated proof-of-stake (DPoS) and byzantine fault tolerance. <sup>17</sup>

### 3.2.3 Examples and Characteristics of Different Protocols

The following table categorizes some of the most common consensus protocols defined by the above groupings and includes:

- **Method:** How blocks are created and verified;
- **Computing Power:** Refers to the amount of processing, e.g., millions of instructions per second (MIPS) required to create, execute, and verify the transaction; and
- **Transaction Throughput:** How many transactions can be created and verified per second, which are based on definition, network architecture, and testing scenarios<sup>18,19</sup>.

Protocols continue to evolve and with respect to performance and scale, there is “no single metric that applies to all use cases and in all circumstances.”<sup>20</sup> For more information, refer to the “Blockchain Consensus Encyclopedia.”<sup>21</sup>

<sup>15</sup> Nick Youngson. “Blockchain Consensus Encyclopedia.” GitBook.

<sup>16</sup> Jordan Odinsky. “Blockchain Dictionary.” Hackernoon.

<sup>17</sup> Leila Ismail and Huned Materwala. “A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions.” Symmetry.

<sup>18</sup> Daily Hodl. “Cryptocurrency Transaction Speeds: The Complete Review.” Daily Hodl.

<sup>19</sup> CoinSutra. “Top 10 Cryptocurrencies With Fast Transaction Speeds.” CoinSutra.

<sup>20</sup> Christopher Ferris. “Answering your questions on Hyperledger Fabric performance and scale.” IBM Blockchain Blog.

<sup>21</sup> Nick Youngson. “Blockchain Consensus Encyclopedia.” GitBook.

**Table 2. Most Common Consensus Protocols**

Protocol	Method	Examples	Computing Power (high, med, low)	Transaction Throughput	Other Considerations
<b>Pure Proof of Work (PoW)</b>	<b>Node with highest computing power creates and verifies block<sup>22</sup></b>	<b>Cryptocurrency</b> <ul style="list-style-type: none"> <li>Bitcoin</li> <li>Litecoin</li> <li>Dogecoin</li> </ul>	<ul style="list-style-type: none"> <li>High</li> </ul>	<ul style="list-style-type: none"> <li>Bitcoin (3-7 TPS)</li> <li>Litecoin (26 TPS)</li> <li>Dogecoin (33 TPS)</li> </ul>	<ul style="list-style-type: none"> <li>A miner can influence timestamps.</li> <li>A miner can influence transaction access and order.</li> <li>DDoS resistance</li> <li>Immutable audit trail</li> <li>Firewall partitioning attacks</li> <li>Coarse-grained timestamps</li> </ul>
<b>Delayed Proof of Work (dPoW)</b>	<b>Hybrid Notary nodes are elected by participants to verify created blocks; Used in combination with either PoW or PoS</b>	<ul style="list-style-type: none"> <li>Komodo (platform for blockchain developers, uses native KMD currency)</li> </ul>	<ul style="list-style-type: none"> <li>Medium</li> </ul>	<ul style="list-style-type: none"> <li>Komodo (20,000 TPS)</li> </ul>	<ul style="list-style-type: none"> <li>Increased security</li> <li>Only blockchains using PoW or PoS can be participants.</li> <li>Hash rates need to be calibrated.</li> </ul>
<b>Proof of Stake (PoS)</b>	<b>Node with highest stake creates and verifies block<sup>23</sup></b>	<ul style="list-style-type: none"> <li>R3 Corda (enterprise open source blockchain platform)</li> <li>Enterprise Ethereum Alliance (EEA)</li> <li>Quorum (based on Ethereum)</li> </ul>	<ul style="list-style-type: none"> <li>Medium</li> </ul>	<ul style="list-style-type: none"> <li>R3 Corda (170 TPS)</li> <li>EEA</li> <li>Classic (14 TPS)</li> <li>Ethereum (50 TPS)</li> <li>Quorum (15-20 TPS)</li> </ul>	<ul style="list-style-type: none"> <li>Immutable audit</li> <li>Leader can influence transaction access and order.</li> <li>Fault tolerant</li> <li>Not attack tolerant <ul style="list-style-type: none"> <li>IP address of leader can be obtained and network brought down. Members may find another leader, but attacker can keep following the leader as members need to always know the IP address.</li> </ul> </li> </ul>

<sup>22</sup> Ibid.<sup>23</sup> Shijie Zhang, Jong-Hyouk Lee. "Analysis of the main consensus protocols of blockchain." p2. ScienceDirect.



**Table 2. (Continued)**

Protocol	Method	Examples	Computing Power (high, med, low)	Transaction Throughput	Other Considerations
					<ul style="list-style-type: none"> <li>Susceptible to distributed denial of service (DDoS) attacks</li> </ul>
<b>Delegated Proof of Stake (DPoS)</b>	<b>Nodes who hold stake vote to elect block creator and verifier<sup>24</sup></b>	<ul style="list-style-type: none"> <li>Steemit (social media platform uses Steem currency)</li> <li>EOS (dAPP platform using BFT and DPoS and native EOS)</li> </ul>	<ul style="list-style-type: none"> <li>Medium</li> </ul>	<ul style="list-style-type: none"> <li>Steemit</li> <li>EOS (+100,000)</li> </ul>	<ul style="list-style-type: none"> <li>Immutable audit</li> <li>Leader can influence transaction access and order</li> <li>Fault tolerant</li> <li>Not attack tolerant</li> </ul>
<b>Proof of Stake Velocity (PoSV)</b>	<b>Node with both stake and activity creates and</b>	<ul style="list-style-type: none"> <li>Reddcoin (social currency platform)</li> </ul>	<ul style="list-style-type: none"> <li>Medium</li> </ul>	<ul style="list-style-type: none"> <li>Reddcoin</li> </ul>	<ul style="list-style-type: none"> <li>Addresses tendency of participating nodes hoarding coins</li> </ul>
<b>Proof of Space (PoC / PoSpace)</b>	<b>Nodes that commit a non-trivial amount of “space” create and verify blocks.</b>	<b>Cryptocurrency</b> <ul style="list-style-type: none"> <li>Burstcoin</li> <li>SpaceMint</li> <li>Chia (based on PoSpace and Proof of Time)</li> </ul>	<ul style="list-style-type: none"> <li>Low</li> </ul>	<ul style="list-style-type: none"> <li>Burstcoin (3-7 TPS)</li> <li>SpaceMint (unknown)</li> <li>Chia (unknown)</li> </ul>	<ul style="list-style-type: none"> <li>Space-heavy</li> <li>Hashes stored in a way that is vulnerable to malware</li> <li>Malicious users</li> </ul>
<b>Proof of Reputation (PoR)</b>	<b>Stronger form of PoAuthority, validators are approved organizations</b>	<ul style="list-style-type: none"> <li>GoChain (smart contract dApp platform, uses native GO currency)</li> <li>Menlo One (blockchain for creating dApps; uses native ONE currency)</li> </ul>	<ul style="list-style-type: none"> <li>Low</li> </ul>	<ul style="list-style-type: none"> <li>GoChain (1,300 TPS)</li> <li>Menlo One (unknown)</li> </ul>	<ul style="list-style-type: none"> <li>Subject to 51% attack, though unlikely</li> </ul>
<b>Proof-of-Retrievability</b>		<ul style="list-style-type: none"> <li>Microsoft</li> <li>PermaCoin</li> </ul>	<ul style="list-style-type: none"> <li>Low</li> </ul>	<ul style="list-style-type: none"> <li>Unknown</li> </ul>	<ul style="list-style-type: none"> <li>Public blockchain</li> <li>Used for efficient peer-to-peer data storage, transfer, and</li> </ul>

<sup>24</sup> Ibid.

**Table 2. (Continued)**

Protocol	Method	Examples	Computing Power (high, med, low)	Transaction Throughput	Other Considerations
					retrieval in cloud computing
<b>Proof of History (PoH)</b>	Based on complex verifiable delay function to ensure the node creating the block was chosen fairly.	<ul style="list-style-type: none"> <li>Solana</li> </ul>	<ul style="list-style-type: none"> <li>Medium</li> </ul>	<ul style="list-style-type: none"> <li>Solana (50,000 TPS)</li> </ul>	
<b>Proof of Activity (PoA)</b>	Hybrid based on PoW and PoS. Nodes use PoW to create the new block and randomly selected nodes based on PoS to verify the block.	<b>Cryptocurrency</b> <ul style="list-style-type: none"> <li>Decred (DCR)</li> </ul>	<ul style="list-style-type: none"> <li>Medium</li> </ul>	<ul style="list-style-type: none"> <li>Decred</li> </ul>	
<b>Proof of Weight (PoWeight)</b>	Combination of methods. Nodes assigned different 'weight' based on data users are storing. These nodes can subsequently randomly assign users to create and validate blocks.	<ul style="list-style-type: none"> <li>Algorand (platform for blockchain developers)</li> </ul>	<ul style="list-style-type: none"> <li>Low</li> </ul>	<ul style="list-style-type: none"> <li>Algorand (1 block of 1,500 200B messages in &lt;40 secs) TPS</li> </ul>	
<b>RAFT</b>	Blocks are created by elected leaders. Blocks are verified by endorsing peers.	Usually used by private, permissioned networks <ul style="list-style-type: none"> <li>IPFS Private Cluster</li> <li>Quorum</li> </ul>	<ul style="list-style-type: none"> <li>Medium</li> </ul>	<ul style="list-style-type: none"> <li>Quorum</li> <li>IPFS Private</li> </ul>	<ul style="list-style-type: none"> <li>CFT-based</li> <li>Less data integrity when a node behaves maliciously</li> </ul>

**Table 2. (Continued)**

Protocol	Method	Examples	Computing Power (high, med, low)	Transaction Throughput	Other Considerations
					<ul style="list-style-type: none"> <li>Eliminates communication issues of BFT-based systems by only communicating between leader and nodes (no node to node)</li> </ul>
<b>Hybrid Models Proof of Authority (PoAuthority)</b>	<b>Validators are formally approved accounts whose identify is verified by an authorized public notary.</b>	<b>Cryptocurrency</b> <ul style="list-style-type: none"> <li>POA network (based on Ethereum, framework for smart contracts, uses native POA)</li> <li>VeChain (platform for supply chain, uses VET and VeChain Thor: VTHO tokens)</li> <li>Ethereum Kovan testnet (for developer community)</li> </ul>	<ul style="list-style-type: none"> <li>Low</li> </ul>	<ul style="list-style-type: none"> <li>POA network (unknown)</li> <li>VeChain (25 TPS)</li> <li>Kovan (unknown)</li> </ul>	
<b>Proof of Burn</b>	<b>Nodes who commit coins (unspendable) earn chance to be selected to create and verify blocks</b>	<ul style="list-style-type: none"> <li>Slimcoin</li> <li>TGCoin</li> </ul>	<ul style="list-style-type: none"> <li>Unknown</li> </ul>	<ul style="list-style-type: none"> <li>Unknown</li> </ul>	<ul style="list-style-type: none"> <li>Those who invest more have more chance of being selected.</li> </ul>
<b>Trusted Computing Models Proof of Elapsed Time (PoET)</b>	Participating nodes are assigned a random time before they can begin creating and validating blocks. After this, the first to finish “wins” the right	<ul style="list-style-type: none"> <li>Hyperledger Sawtooth</li> </ul>	<ul style="list-style-type: none"> <li>Low</li> </ul>	<ul style="list-style-type: none"> <li>Hyperledger Sawtooth</li> </ul>	<ul style="list-style-type: none"> <li>Specialized hardware required</li> <li>Intel is the controlling authority.</li> <li>Vulnerable to malicious attacks</li> </ul>

**Table 2. (Continued)**

Protocol	Method	Examples	Computing Power (high, med, low)	Transaction Throughput	Other Considerations
	to commit the block.				
<b>PBFT and BFT-Based Proof of Stake Practical Byzantine Fault Tolerance (PBFT)</b>	<b>Nodes use a phased process that tolerates failure of a node when creating and verifying block<sup>25</sup></b>	<ul style="list-style-type: none"> <li>• Hyperledger Fabric</li> <li>• Hyperledger Iroha</li> <li>• Oracle</li> <li>• Hydrachain</li> <li>• BigchainDB</li> </ul>	<ul style="list-style-type: none"> <li>• Low</li> </ul>	<ul style="list-style-type: none"> <li>• Hyperledger Fabric</li> <li>• Hyperledger Iroha</li> <li>• Oracle</li> <li>• Hydrachain</li> <li>• BigchainDB</li> </ul>	<ul style="list-style-type: none"> <li>• Provides finality</li> <li>• Less decentralized <ul style="list-style-type: none"> <li>▪ Authority service required to select leader and backup nodes</li> </ul> </li> <li>• Public network <ul style="list-style-type: none"> <li>▪ Scalability issues</li> <li>▪ PBFT prone to sybil attacks (one entity can create multiple faulty identities and control a big part of the network)</li> </ul> </li> </ul>
<b>Byzantine Fault Tolerance (BFT)</b>	<b>Voting-based</b>	<b>Private permissioned networks</b> <ul style="list-style-type: none"> <li>• Hyperledger Fabric</li> <li>• Ripple</li> <li>• Dispatch</li> <li>• EOS (dAPP platform using BFT and DPoS)</li> </ul>	<ul style="list-style-type: none"> <li>• Low</li> </ul>	<ul style="list-style-type: none"> <li>• Hyperledger Fabric)</li> <li>• Stellar (2,000 TPS)</li> <li>• Ripple (1,500 TPS)</li> <li>• Dispatch</li> </ul>	<ul style="list-style-type: none"> <li>• Provides finality</li> </ul>

<sup>25</sup> Ibid. p 3.

**Table 2. (Continued)**

Protocol	Method	Examples	Computing Power (high, med, low)	Transaction Throughput	Other Considerations
		and native EOS currency)			
<b>Delegated Byzantine Fault Tolerance (DBFT)</b>	<b>Voting-based</b>	<ul style="list-style-type: none"> <li>• NEO</li> <li>• Byteball</li> </ul>	<ul style="list-style-type: none"> <li>• Low</li> </ul>	<ul style="list-style-type: none"> <li>• 1,000 TPS</li> <li>• Confirmation 15-20 seconds</li> </ul>	<ul style="list-style-type: none"> <li>• Provides finality</li> <li>• Nodes may vote for themselves</li> <li>• Communication and sybil attacks still exist</li> </ul>
<b>Kafka</b>	<b>Blocks are created by elected leaders. Blocks are verified by endorsing peers.</b>	<b>Usually used by private, permissioned networks</b> <ul style="list-style-type: none"> <li>• Hyperledger Fabric</li> </ul>	<ul style="list-style-type: none"> <li>• Low</li> </ul>		<ul style="list-style-type: none"> <li>• CFT not BFT</li> </ul>
<b>Solo</b>	<b>Single ordering node creates blocks. Endorsing peers verify blocks.</b>	<ul style="list-style-type: none"> <li>• Usually only used by developers as it involves a single ordering node</li> </ul>	<ul style="list-style-type: none"> <li>• Low</li> </ul>		<ul style="list-style-type: none"> <li>• Does not provide CFT</li> </ul>
<b>Directed Acyclic Graph (DAG)</b>	<b>DAG</b>	<ul style="list-style-type: none"> <li>• Casper</li> <li>• EOS</li> <li>• IOTA (DAG plus Tangle)</li> <li>• Tezos</li> <li>• RaiBlocks / Nano (Block-lattice)</li> </ul>	<ul style="list-style-type: none"> <li>• Low</li> </ul>	<ul style="list-style-type: none"> <li>• Casper</li> <li>• EOS</li> <li>• IOTA (1,500 TPS)</li> <li>• Tezos</li> <li>• Nano (7,000 TPS)</li> </ul>	<ul style="list-style-type: none"> <li>• Smart contracts via bridge to Hyperledger Fabric (IOTA)</li> <li>• Public</li> <li>• Immutable audit</li> <li>• DDoS resilient</li> <li>• Not byzantine</li> <li>• No certainty of consensus</li> <li>• Not possible to formally analyze security of network as the system is too complex (technically chaotic)</li> </ul>
<b>DAG / Asynchronous Byzantine Fault Tolerant (aBFT)</b>	<b>DAG with aBFT</b>	<ul style="list-style-type: none"> <li>• Hashgraph</li> </ul>	<ul style="list-style-type: none"> <li>• Low</li> </ul>	<ul style="list-style-type: none"> <li>• Hashgraph (50,000 – 500,000 TPS)</li> </ul>	<ul style="list-style-type: none"> <li>• Private / proprietary</li> <li>• Immutable audit</li> <li>• DDoS resilient</li> <li>• Firewall / virus attack resilient</li> </ul>

### 3.2.4 Summary

Rather than focusing on a certain metric, such as computing power or TPS, organizations should choose the most suitable protocol while assuming business value based on use case requirements and how the agreement on what constitutes a final, authoritative transaction will be established and audited.

### 3.3 SMART Contracts

SMART Contracts are essential to blockchain implementation, since they apply the business logic for the blockchain application running on the blockchain network. SMART Contracts are used to automatically implement business actions based on the transaction's state or condition. For example, if a protective order is issued by a judge, a SMART Contract can trigger certain actions, such as sending the granted protective order to the petitioner, respondent, and law enforcement agency. Depending on which blockchain technology is used, SMART Contracts can be written in different languages. For example, if an Ethereum blockchain is used, SMART Contracts are written in a language known as Solidity (see sample below). If Hyperledger Fabric is the blockchain platform used, then SMART Contracts, or "Chaincode," can be written in languages that include Go, Node.js, C#, Javascript, etc. There can be multiple SMART Contracts running at the same time on the blockchain network.

**Figure 2. SMART Contract Snippet in Solidity**

```
// call this function to send a response
function WarrantAction(bool warrantAction) public
{
    require (msg.sender == Officer);

    /* if (Officer == msg.sender)
        {
            State = StateType.Executed;
        }
    /* if (Officer != msg.sender)
        {
            revert();
        }
    */

    // call ContractUpdated() to record this action
    WarrantAction = warrantAction;
    State = StateType.Executed;
}
```

**SMART Contract Code snippet courtesy of JUSTICE CHAIN LLC**

© JUSTCHAIN 2020

### 3.4 On-Chain vs. Off-Chain

The word "blockchain" comes from the fact that the underlying technology stores transaction data in a series of blocks that are cryptographically linked to form a "chain," which is depicted in Figure 3.

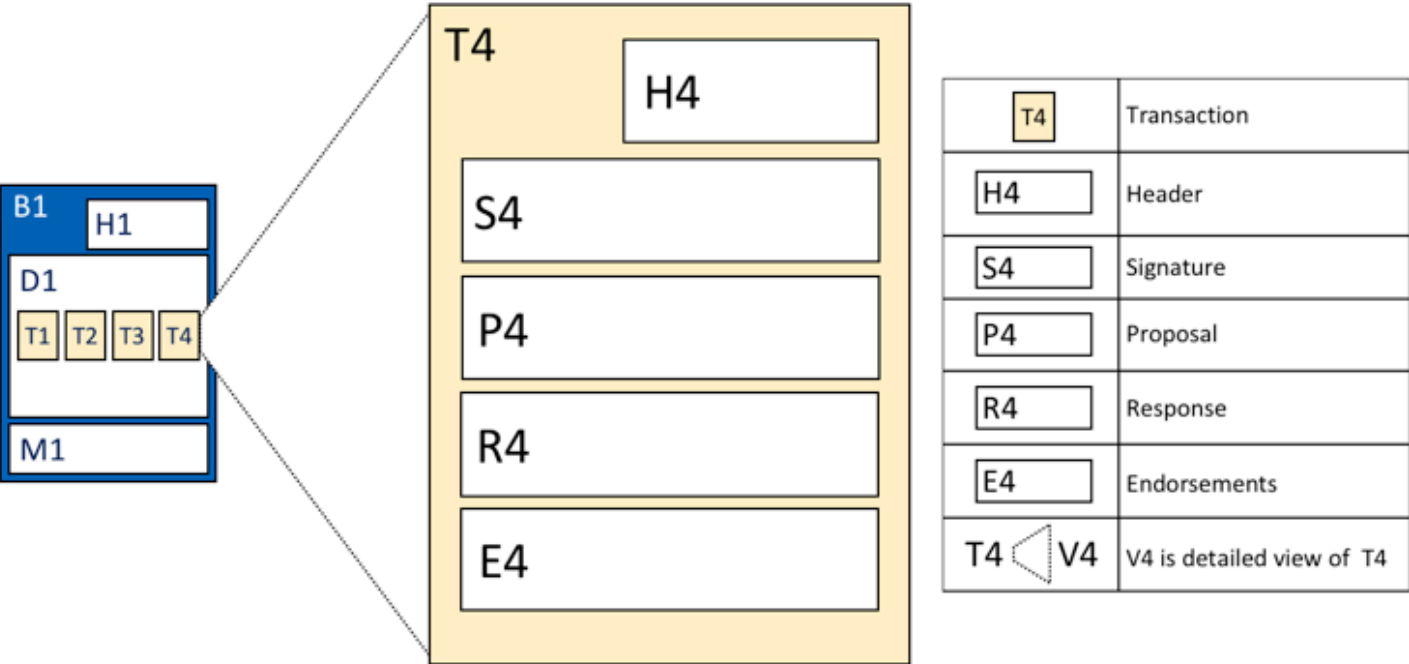


Figure 3. Blockchain Structure: Block Frame

Each block contains a header, which includes the block number, the hash for all transactions in the current block, and the hash for all transactions in the previous block. The block also includes a set of transactions along with associated data. Contents of those transactions, as well as the size of the transactions, depend on the application.

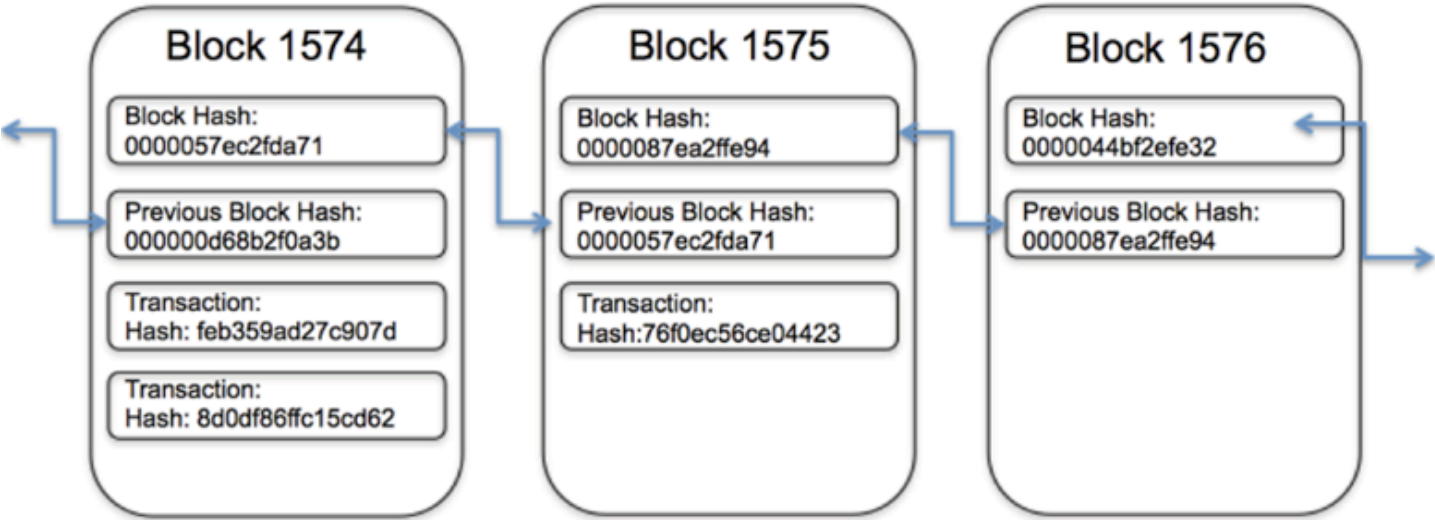


Figure 4. Block Structure: Chained Blocks

Each transaction typically contains a:

- **Header:** Some basic metadata; it varies based on the transaction type;
- **Signature:** A cryptographic digital signature, also called a hash, of the transaction data; it ensures that the contents of the transaction are not altered;
- **Proposal or Transaction Details:** The actual transaction data stored on the chain for each transaction; and
- **Endorsements:** Approvals from each participating organization of the transaction; typically, these are the digital signatures of the transaction from each participating organization.



Note that once written, transaction data can never change. Additionally, transactions often contain large amounts of static data (e.g., pictures, videos, documents, etc.), and a static data element is often the target of multiple transactions (e.g., read, viewed, moved, deleted, etc.). It is often much more efficient to store the large static data off the blockchain and keep a reference (i.e., pointer) to the static data's storage location, along with a hash of the static data on the blockchain. This approach reduces the storage requirement for a static data element to a storage reference plus element hash.

An off-chain repository maintains data relevant to the blockchain transaction without requiring the data to be embedded in the transaction. Typically, this involves a hash value on the blockchain that references an external repository, such as a PDF containing a signed protective order maybe 1 MB in size, whereas a storage reference plus element hash may only be 1K in size.

Using the off-chain storage approach, each transaction for that document would only need to store one kilobyte of data for each transaction on the blockchain versus one megabyte of data. Additionally, the overall blockchain is also duplicated for each participating organization, adding to overall storage needs. Using off-chain storage would significantly reduce overall blockchain storage requirements.

### **3.5 Throughput**

Throughput of a records management system represents the amount of records that can be processed at any given time. Implementing such a system on a transaction-based blockchain network can be measured using the Transactions Per Second (TPS) benchmark. There also exists a certain amount of variability for how a blockchain architecture can process transactions, which affects overall throughput. For example, the Bitcoin blockchain is limited to approximately seven transactions per second while the public Ethereum blockchain can support 20 transactions per second. By comparison, the Visa credit card network processes 1700 transactions per second on average. The PayPal network processes around 200 transactions per second on average.

On the other hand, estimates show that courts issue around 1.7 million protective orders annually for Protective Order (PO) use cases. Of these, 1.2 million are estimated to be active, which translates to about 2.3 POs every minute.<sup>26</sup> The chart in section 10.6 highlights the expected throughput of the available blockchain technologies. Given the current state of blockchain technology, it remains clear that blockchain may not be ready for credit card transaction processing but should be sufficient for most justice and public safety use cases.

### **3.6 Identity and Access Management**

Identity and access management is a well-documented topic outside the blockchain domain. Identity management in the blockchain domain reflects many of the same requirements and issues as the other domains. In many blockchain applications, the identity of the users and the blockchain nodes are not required or even desired. In a typical blockchain scenario, there are also several mechanisms to add nodes to the network, such as proof of work. In the case of the protection order blockchain, adding nodes may require agreements or other documented procedures.

In typical blockchain implementations, a user creates a wallet to handle an identity and to initiate transactions. Third parties are developing various types of wallets that can integrate with any blockchain implementation. For private blockchain implementation, such as protection orders, a wallet may not be necessary, but methods for users to initiate blockchain transactions are required.

The blockchain discussed in this document is considered a private blockchain and is a permissioned blockchain. This means that only users with special authorization can perform operations on the chain. With blockchains, there are typically read, write, and audit permissions for the blockchain. Depending on the blockchain goals, read access may be granted individually or to all members of the private blockchain organization. Write and audit permissions would only be assigned to those who can add blocks to the chain, such as court officials or law enforcement. Blockchain nodes also need to be defined, and a process would need to be implemented to add nodes to the blockchain.

<sup>26</sup> Communicating with prisoners collective. "Restraining Orders Issued and In Effect in the U.S."

In the protection order example, the parties would need to agree on how many nodes are needed and how those nodes would be added. As previously discussed in this document, there are pros and cons to adding additional nodes to the network. For a state, the number of nodes necessary to successfully implement the blockchain would need to be determined by the governing body and by the technical requirements or cost limitations. A state would not want to host a node at every court jurisdiction but may want a node of the courts, law enforcement, attorneys, and the public. This would ensure functionality but would not be cost-prohibitive or technically challenging.

In summary, justice and public safety organizations using blockchain technologies need to consider how they will agree and maintain policies, procedures, and technologies for managing individuals or identities. This includes the authentication of specific roles and providing authorization to those who perform actions on the blockchain.

### 3.6.1 Identity Management (Defines Individual Users)

The following section describes high-level identity management and includes considerations for identity management when using blockchain technologies to exchange information among agencies at local, state, and federal levels. For this framework, entities who perform operations on the blockchain need to be identified and granted explicit permissions.

*“Thus, the overarching goal of identity management is to “grant access to the right enterprise assets to the right users in the right context, from a user’s system onboarding to permission authorizations to the offboarding of that user as needed in a timely fashion,” according to Yassir Abousselham, senior vice president and chief security officer for Okta, an enterprise identity and access management provider.”<sup>27</sup>*

#### Definitions

Identity management is defined as “the organizational process for identifying, authenticating and authorizing individuals or groups of people to have access to applications, systems or networks by associating user rights and restrictions with established identities.”<sup>28</sup>

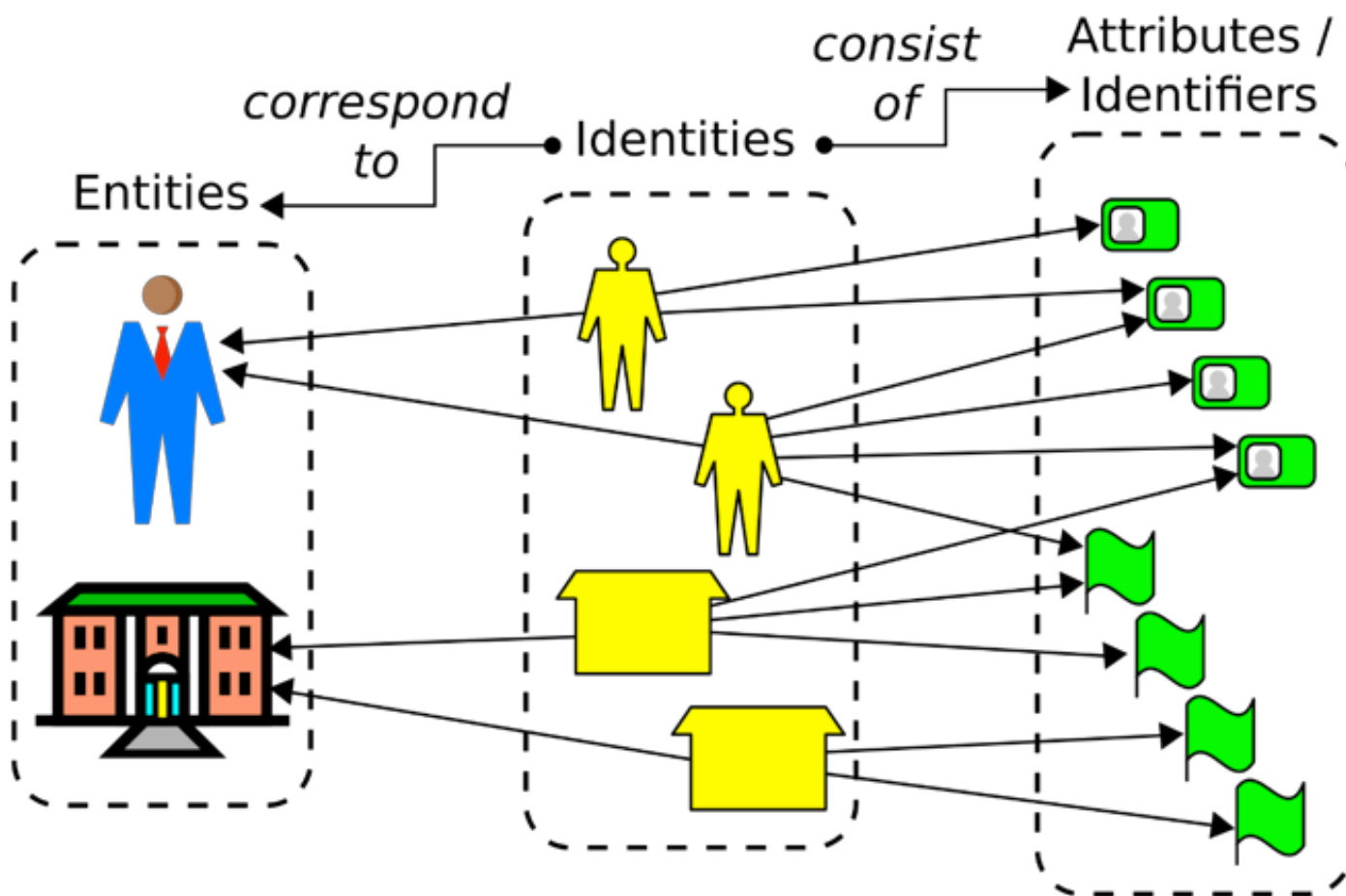
- **Identity:** “a set of attributes related to an entity” (ISO/IEC 24760-1)<sup>29</sup>
  - Contains a finite set of properties;
  - Managed entities: Content, hardware, network resources, and applications may also be included.<sup>30</sup>
- **Authentication:** verifies user’s identity based on an agreed set of rules;
- **Authorization:** defines what operations an entity can perform regarding a specific application (One user can issue a protective order one user can view, and one user can update service.);
- **Roles:** groups of operations and related to job or job function; Roles are granted authorizations, such as law enforcement, judge, sheriff, corrections, etc.;
- **Delegation:** enables modifications by a local administrator or by one user on behalf of another (e.g., law clerk on behalf of a judge);
- **Entities:** may have multiple identities. (e.g., a person or an organization);
- **Identities:** a finite set of properties (attribute values); The opposite of this “pure” model is a digital signature, which is used internally and is not semantically independent.

<sup>27</sup> James A. Martin and John K. Waters. “What is IAM? Identity and access management explained.” CSO Online.

<sup>28</sup> Wikipedia. “Identity management.”

<sup>29</sup> International Organization for Standardization / International Electrotechnical Commission. Prepared by Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security Techniques.

<sup>30</sup> Ibid.

**Figure 5. Pure Identity Model<sup>31</sup>**

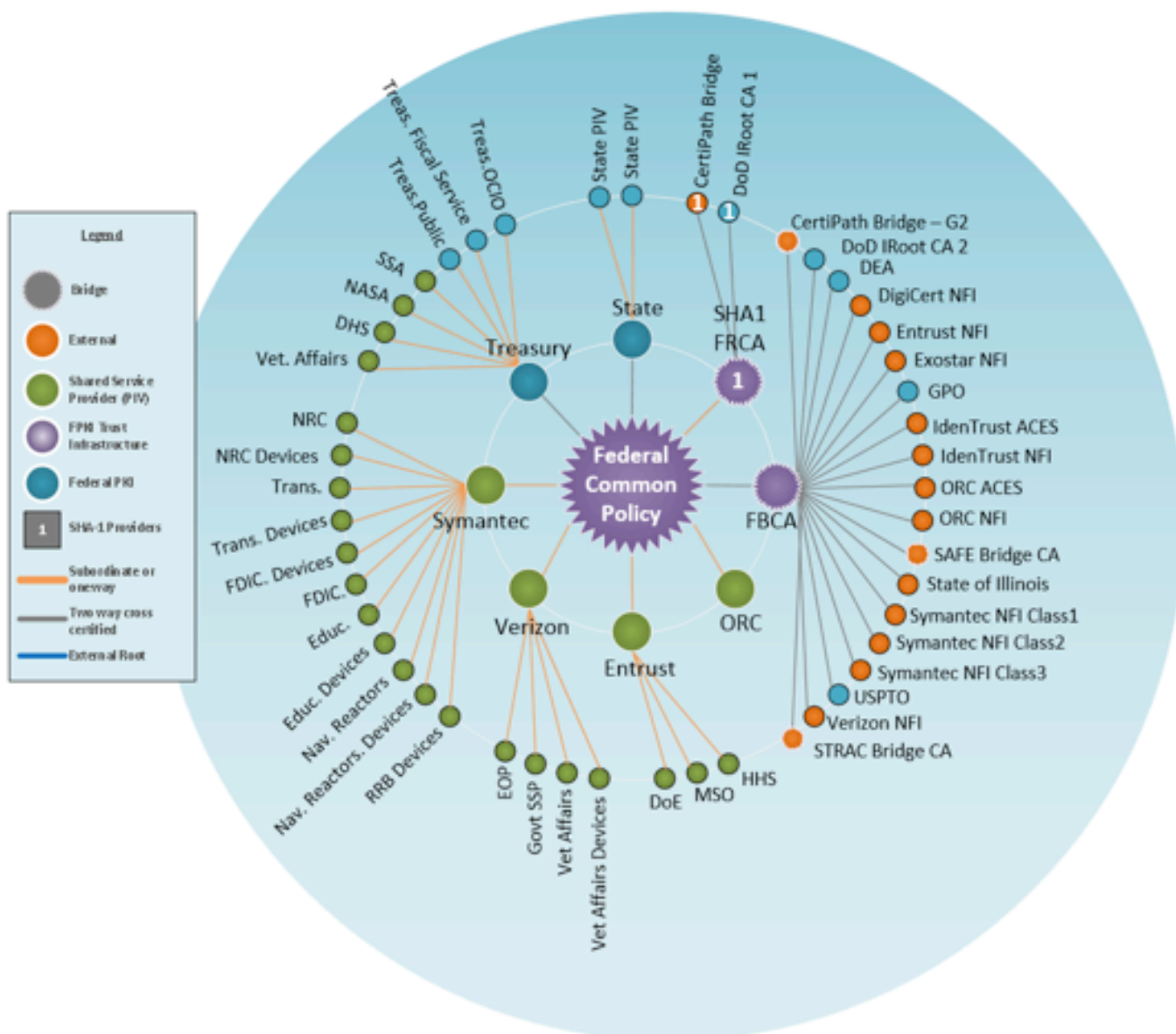
### 3.6.2 Considerations for Justice and Public Safety

The most important considerations for managing blockchain identities in the justice and public safety domains are governance and trust. The identity management domain is evolving, especially as users from different systems need to trust each other virtually and as it becomes more difficult for each organization to vet every system user.

Identity Federation is now a way to partially overcome the vetting and trust issues with technology users. Identity Federation allows users to log in to all systems if they have access to one that is participating, which is called the Circle of Trust. One system can act as the Identity Provider (IdP) and another as the Service Provider (SP). When a user logs in, a request is sent to the IdP, which authenticates the individual. It then sends an assertion back to the SP acknowledging the individual requesting access to the service.

There are still issues to overcome, but through Identity Federation models, one organization can trust the users of another organization. In the public domain, users are vetted through commercial vendors. The use of Public Key Infrastructure (PKI) is part of a federated process. However, organizations using the blockchain need to ensure they are comfortable with the vetting process of the other organization and are willing to accept a user's identity.

<sup>31</sup> Ibid.

**Figure 6. High-level Illustration of the Federal PKI Certification Authorities<sup>32</sup>**

There can also be levels of trust involved with the federation process. An organization may accept an identity from a commercial provider to access the blockchain with a public read role but would not accept it for a role that would allow adding information to the blockchain. The blockchain technology can be implemented to accept different certificates or certificate methods. However, governance is necessary to accept various user identities.

### 3.6.3 Identity Policies and Technologies

Criminal justice organizations that use blockchain need to agree upon a process to identify blockchain users. The process can be as simple as providing a valid user with a username and password through a wallet process, or it can rely on a PKI that uses current federal, state, or industry standards to confirm user identities. One example is the federal PKI.

Depending on the blockchain community policy, each agency could be responsible for vetting and providing identification credentials to their users with an implicit trust that each agency is following the policy. For public users, there would be a need to develop a process to gain public access.

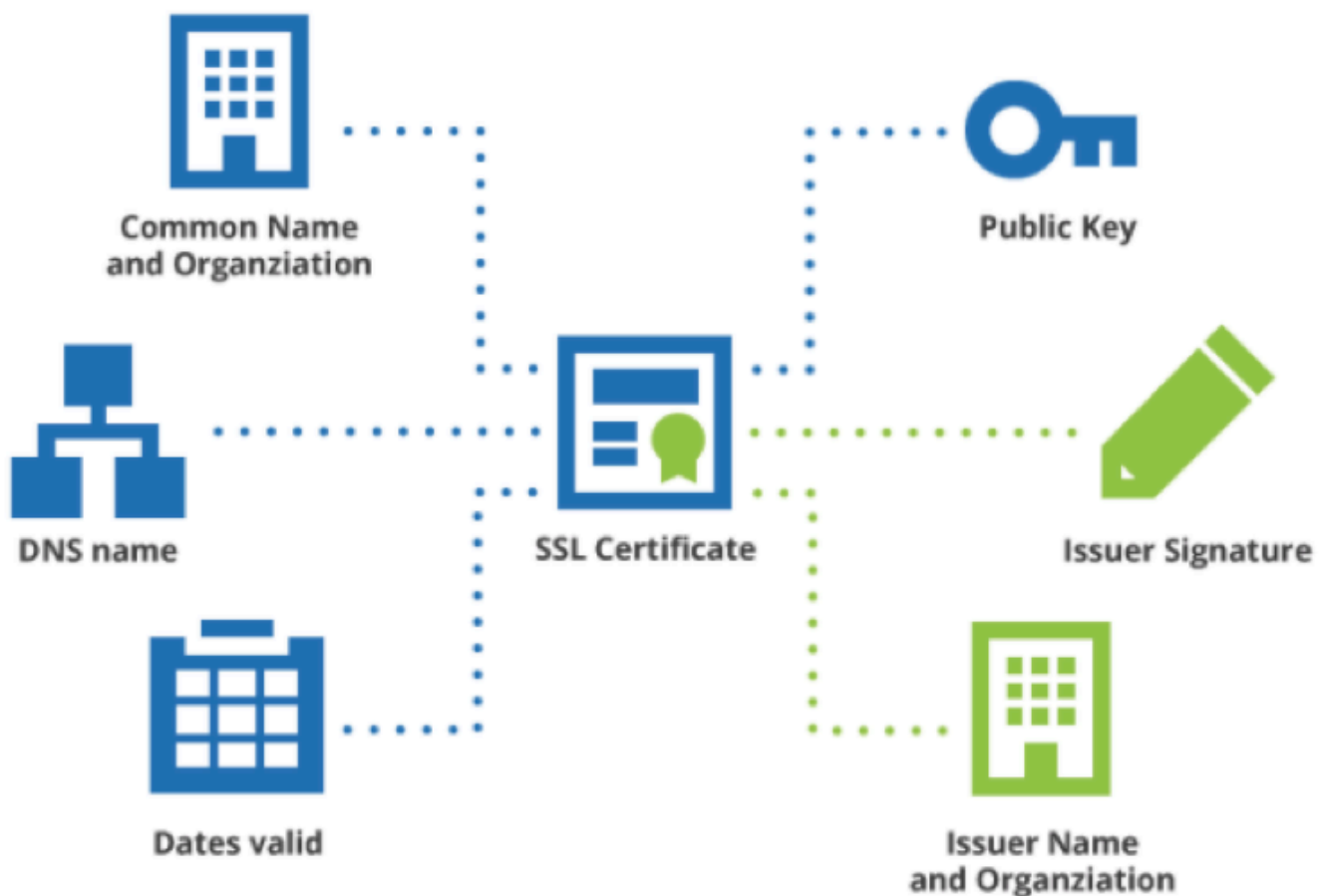
<sup>32</sup> Federal Public Key Infrastructure Guides. “High-level Illustration of the Federal PKI Certification Authorities.”

### 3.6.4 Example Identity Provider Solutions - Public Key Infrastructure (PKI)

One potential solution to use at all levels is PKI. This type of solution allows organizations to implement identity provider services. PKI's use would likely be by courts, law enforcement, and prosecuting attorneys who use state and federal systems.

*“A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.”<sup>33</sup>*

**Figure 7. The Anatomy of a Digital Certificate.<sup>34</sup>**



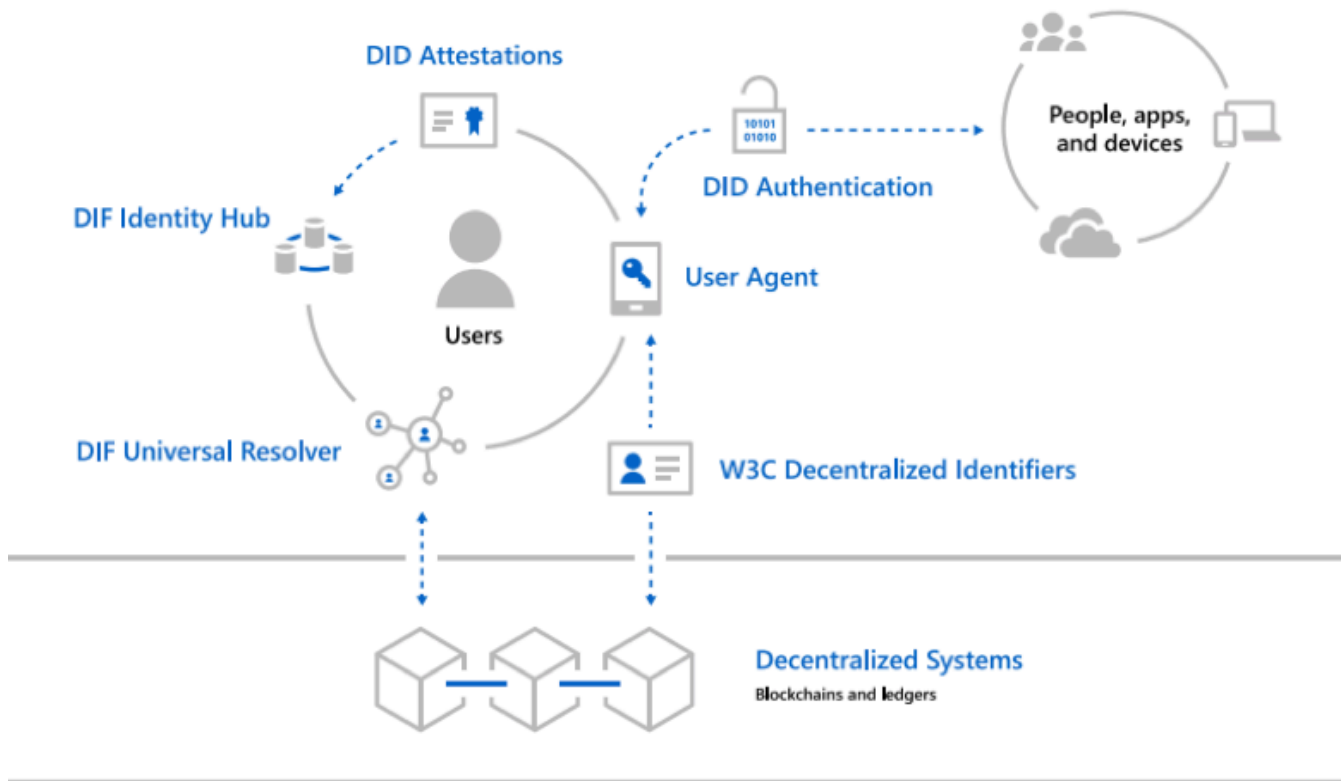
<sup>33</sup> Wikipedia. “Public key infrastructure.”

<sup>34</sup> Nick Sullivan. “The anatomy of a certificate.” Cloudflare.

### 3.6.5 Decentralized Identity

PKI is one approach that could be used by private citizens, victim advocacy groups, and others, but there could be a cost. Individuals might also have to be associated with a specific organization to gain access to their PKI process. Another example of a PKI solution would be a Decentralized Identity, as outlined below.

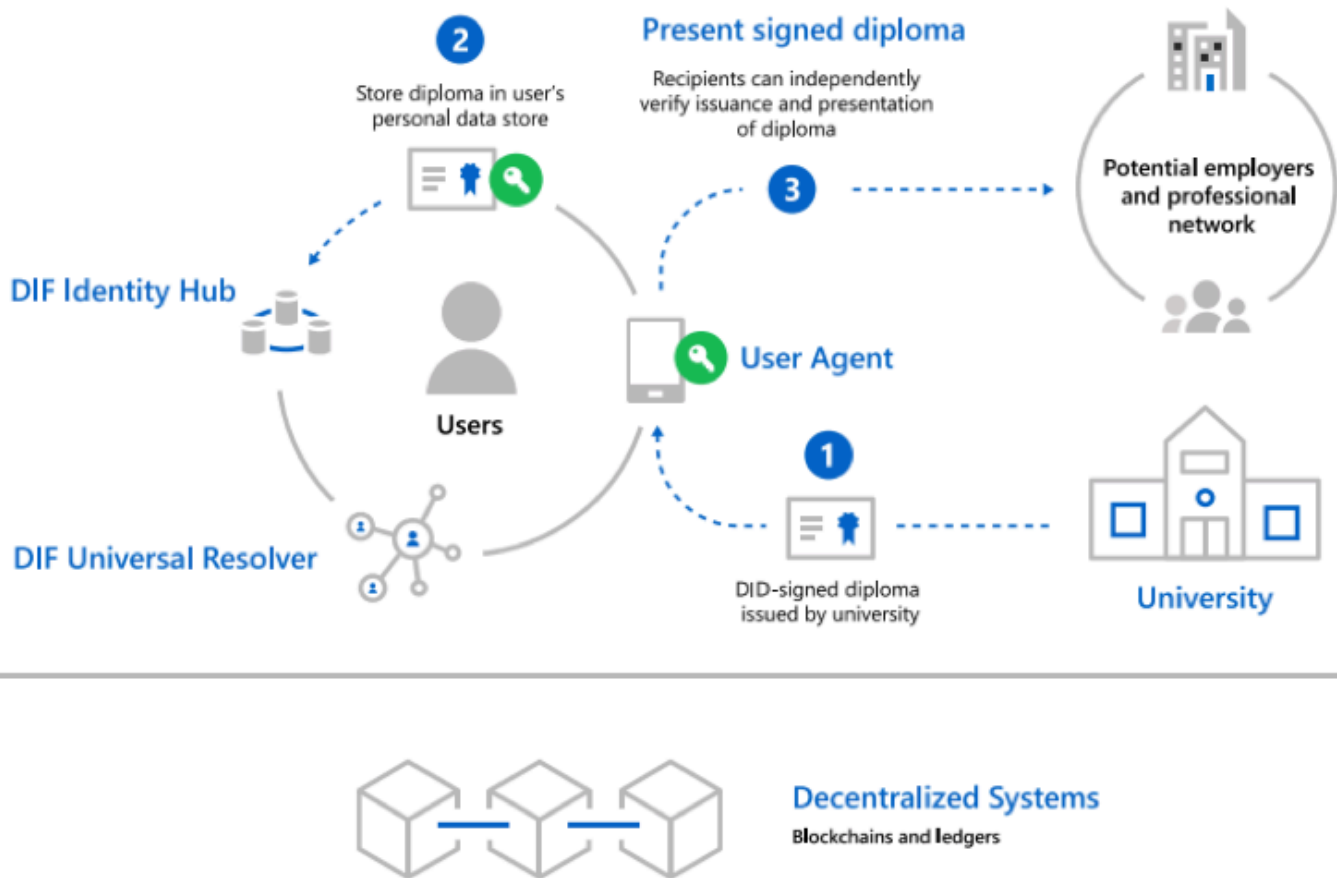
**Figure 8. How Decentralized Identity Works (Microsoft)<sup>35</sup>**



- **W3C Identifiers:** IDs that users create, own, and control independently of any organization, such as a non-governmental user;
- **Decentralized Systems:** blockchains that provide the mechanism and features for Digital Identities (DIDs);
- **DID User Agents:** a user wallet application that supports the creation of Digital Identities that manages data, permissions, signing, and validating Digital Identity linked claims;
- **DIF Universal Resolver:** a server that provides standard method for lookup and resolution across various systems which returns a Digital Identity Document Object that holds the Decentralized Public Key Infrastructure (DPKI) metadata associated with that Digital Identity;
- **DIF Identity Hubs:** encrypted personal data stores (e.g., cloud and edge instances) that provide identity data storage and interactions (e.g., mobile phones, PCs, smart speakers);
- **DID Attestations:** signed verifications based on standard formats and protocols that allow users to generate, present, and verify claims about their identity while forming trust between systems;
- **Decentralized Apps and Services:** DIDs paired with Identity Hub personal data stores that enable a new class of apps and services;

<sup>35</sup> Microsoft. "Decentralized Identity." Microsoft.



**Figure 9. Sample DID Scenario (Microsoft)**

### 3.6.6 Authentication

Authentication within blockchain is based on an identity that requires a public and private key. Those keys can be created based on a PKI, as discussed above, or they can be self-signed keys that are created through the wallet or DID process. In the protection order example, the authentication would be handled through a single PKI or a federation, where the various entities trust each other through technical and governance mechanisms.

### 3.6.7 Authorization

There are only two authorization roles for a blockchain: users who can read the blockchain and users who can add transactions to the blockchain. Any user with access to the blockchain can read the information on the blockchain unless transaction details are hidden through the blockchain variant. Any user with blockchain access can read the public key of the block to determine who authored the information in the block.

Other technologies, such as encryption, could also be used to hide the information written on blocks. The encryption also uses PKI to encrypt and decrypt the information in the block.

Channels and Smart Contracts are primary mechanisms to share information among consortium members. Smart Contracts are computer coding that sets the parameters for the exchange of information between two parties. The computer coding sets the timing for the information, who can see the information, and other relevant computer operations between the parties. Smart Contracts can involve multiple parties, but they must agree to the rules before the Smart Contract is in place. Blockchain technology ensures the transparency of transactions, and appropriate parties can audit the smart

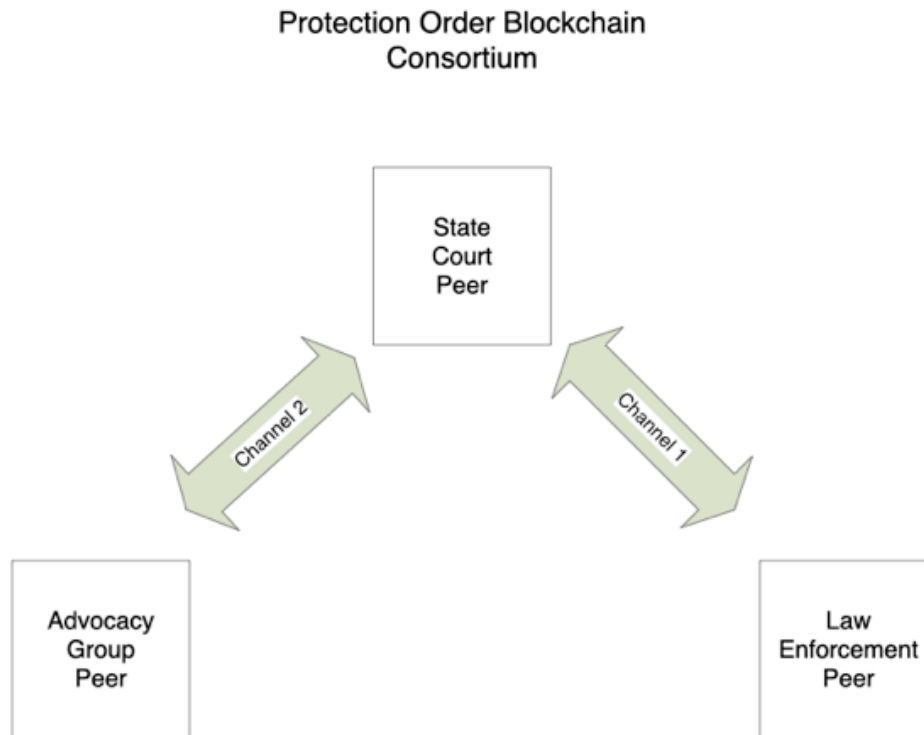


contracts to ensure they are correct and followed.

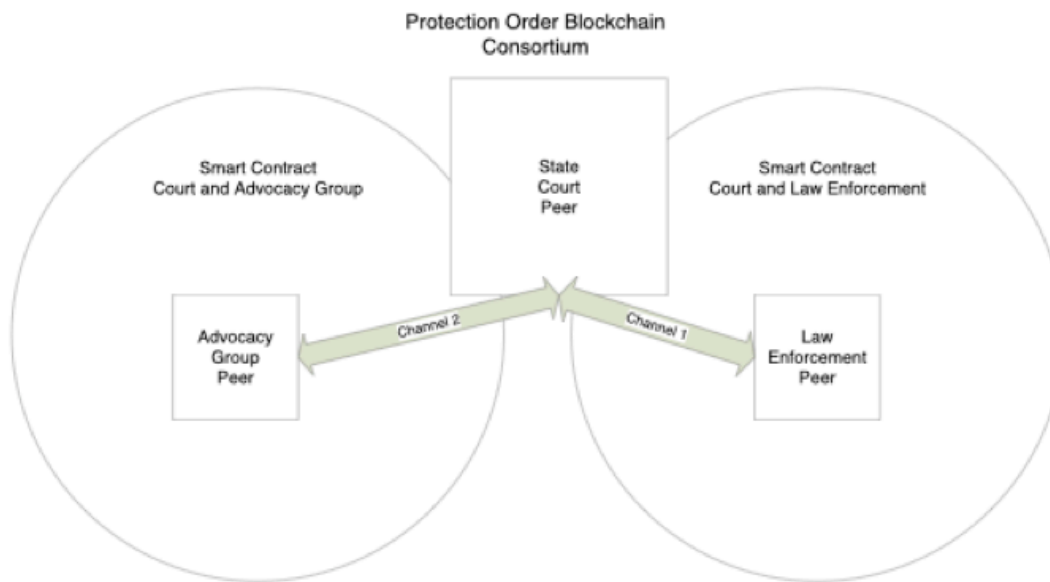
Channels are used for data isolation, which allows for blockchain confidentiality. Channels require Smart Contracts to define the interactions of the channel peers. They appear as an additional layer on the blockchain network.

Creating a channel between courts and law enforcement is one example that allows two members to share details about a protection order while at the same time creating another channel between the courts and an advocacy group. This only provides basic details about a protection order. A blockchain contains numerous channels, as defined by the consortium.

**Figure 10. Using Channels to Manage Access**



Channels use Smart Contracts to define a business process. Smart Contracts are computer code that uses cryptographic techniques to define the relationship of the blockchain members or peers and the channel. The Smart Contract is associated with a channel and is applied to peers or members. It also defines what the peer or member can see on the blockchain and the transactions they perform.

**Figure 11. Using Smart Contracts and Channels to Manage Access**

Peers or members can belong to multiple channels and belong to multiple Smart Contracts. Each Smart Contract defines peer authorizations for the data and the transaction completed in that channel. In the protection order example, a channel exists between courts and law enforcement. The Smart Contract determines that the court peer or member has read and write abilities to issue, change, and revoke a protection order. The law enforcement peer or member uses the same Smart Contract but can only read the protection order, as well as add a transaction for serving the defendant with the protection order. At the same time, the court has a different Smart Contract for a different channel between the court and advocacy agency. This authorizes the court peer or member to issue, change, and revoke protection orders. The same Smart Contract is applied to the advocacy group peer or member but only authorizes it to read basic protection order information.

Blockchain use the same traditional authentication and authorization concepts and processes but uses Smart Contracts and channels.

### 3.7 Interoperability

Interoperability can be defined as “a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, at present or in the future, in either implementation or access, without any restrictions.”<sup>36</sup>

Regardless of what technology is being used, interoperability remains an important consideration, given the variety of productivity tools and records management systems used by any organization. Users must move between applications that share data within and across organizations. Organizations lean on vendors to provide interoperability as a foundational capability.

#### 3.7.1 Blockchain and Standards

Blockchain technologies must address this expectation for interoperability. Ken Krechmer, a recognized expert in the field of standards,<sup>37</sup> talks about three ways to look at time phases for standards development:<sup>38</sup>

<sup>36</sup> Wikipedia. “Interoperability.”

<sup>37</sup> Ken Krechmer. “About Ken Krechmer.” Isology.com.

<sup>38</sup> James Barry. “Blockchain Standards Part 2 of 5 – The International Standards Organizations.” Medium.



The key question justice and public safety organizations must ask is how comfortable they are moving ahead with blockchain technology when standards are developed in parallel with the technology or are “behind.” According to James Barry,<sup>39</sup> blockchain has moved past the anticipatory phase. At the time of publication he identified more than 150 blockchain “platforms,” even though many come from Bitcoin or Ethereum.

The approach to standards development is also worth noting:

- Traditional standards bodies (See table below.);
- Transformation tools (translation between different platforms);
- Country-specific (e.g., Australia<sup>40</sup>, China);
- Platform standards (at risk of becoming massive and cumbersome); and
- Enterprise Ethereum Alliance, which describes itself as a “global standards organization,” yet the standards are only useful if you use Ethereum.

Of the traditional standards bodies, all have separate data standards that are emerging. The following table identifies the approach the major standards bodies are taking. Note that this information is sourced from November 2018.<sup>41</sup>

Standards Body	Time Phase	Comments
<b>International Telecommunication Union (ITU)</b>	<b>Anticipatory standardization</b> <b>Examples:</b> <ul style="list-style-type: none"> <li>• ITU – Focus Group on Digital Currency including Digital Fiat Currency</li> <li>• ITU – Focus Group on Application of Distributed Ledger Technology</li> </ul>	
<b>Internet Engineering Task Force (IETF)</b>	<b>Participatory standardization; Request for Comments (RFC) requires two implementations.</b> IETF – Overall group looking at blockchain ETF – Experimental Draft – Blockchain Transaction Protocol for Constraint Nodes	<b>Core internet networking protocols</b>  <b>Well-defined mission statement</b>
<b>ISO (International Organization for Standardization)</b>	<b>Responsive standardization</b> <b>Examples:</b> <ul style="list-style-type: none"> <li>• ISO/CD 22739 –Terminology</li> <li>• ISO/NP TR 23244 – Overview of privacy and personally identifiable information (PII) protection</li> <li>• ISO/NP TR 23245 – Security risks and vulnerabilities</li> </ul>	<b>Wide breadth</b>

<sup>39</sup> Ibid.

<sup>40</sup> Standards Australia. “Roadmap for Blockchain Standards: Report March 2017.”

<sup>41</sup> James Barry. “Blockchain Standards Part 2 of 5 – The International Standards Organizations.” Medium.

Standards Body	Time Phase	Comments
	<ul style="list-style-type: none"> <li>• ISO/NP TR 23246 – Overview of identity management using blockchain and distributed ledger technologies</li> <li>• ISO/AWI 23257 – Reference architecture</li> <li>• ISO/AWI TS 23258 – Taxonomy and Ontology</li> <li>• ISO/AWI TS 23259 – Legally binding smart contracts</li> <li>• ISO/CD TR 23455 – Overview of and interactions between Smart Contracts in blockchain and distributed ledger technology systems</li> <li>• ISO/NP TR 23576 – Security of digital asset custodians</li> <li>• ISO/NP TR 23578 – Discovery issues related to interoperability</li> <li>• ISO/NP TS 23635 – Guidelines for governance</li> </ul>	
IEEE (Institute of Electrical and Electronics Engineers)	<b>Vertical industries</b> <b>Examples:</b> <ul style="list-style-type: none"> <li>• P2418.2 – Standard Data Format for Blockchain Systems</li> <li>• P2418.1 – Standard for the Framework of Blockchain Use in the Internet of Things (IoT)</li> <li>• P2418.3 – Standard for the Framework of Distributed Ledger Technology (DLT) Use in Agriculture</li> <li>• P2418.4 – Standard for the Framework of Distributed Ledger Technology (DLT) Use in Connected and Autonomous Vehicles (CAVs)</li> <li>• P825 – Guide for Interoperability of Transactive Energy Systems with Electric Power Infrastructure (Building the Enabling Network for Distributed Energy Resources)</li> </ul>	<b>Danger of developing different foundation than foundation stack; Data format within a vertical may conflict with horizontal format.</b>
W3C (World Wide Web Consortium)	<b>Examples</b> <ul style="list-style-type: none"> <li>• W3C Web Community Draft Report – The Web Ledger Protocol</li> <li>• W3C Web Community Draft Report – Decentralized Identifiers (DIDs) v0.11</li> </ul>	

Justice and public safety organizations that see the value of more efficient, timely, secure, and auditable interagency data exchange using blockchain technology need to address system abilities and software to exchange and use data between

disparate and independently managed software and systems.

Currently, no standard approach for interoperability between major ledger technologies, such as Hyperledger Fabric and Enterprise Ethereum, exists. Common standards for identification and data sharing are essential to address interoperability challenges.

*“Defining application definition within a single system stack, restrains creativity and will eventually lose out to worldwide standards.”<sup>42</sup>*

The data standards work completed by organizations working in justice and public safety includes:

- **National Incident-Based Reporting System (NIBRS)**
  - Evolved from Uniform Crime Reports (UCR) established by the International Association of Chiefs of Police (IACP) in 1927;
  - NIBRS began in South Carolina and approved for general use in 1988;
  - Under FBI jurisdiction;
- **NIEM (National Information Exchange Model)**
  - Launched by CIOs of DHS and DOJ; built on the Global Justice Information Sharing Initiative responsible for the Global Justice XML Data Model GJXDM (released in 2003);
  - Common vocabulary enabling efficient information exchange between public and private sector organizations and used as the backbone of e-filing / e-filing manager / case management system interoperability;
- **National Open Data Standards (NODS)**
  - Conference of State Court Administrators (COSCA) and National Center for State Courts (NCSC) will develop business and technical court data standards to support the creation, sharing, and integration of court data.

This work created a solid foundation for fostering a standards-based approach in the justice and public safety community regarding blockchain. Components for standardization may be logical, such as coin, consensus, ledger, Smart Contract, identity, wallet, peer-to-peer network (how nodes are discovered and validated), cryptography, gateway services (APIs), etc.<sup>43</sup>

Even if standards are established following the logical abstract layers suggested above, the underlying agreed standards—not siloed within any particular technology platform—are those that help justice organizations assess readiness for use, as James Barry concludes in his post:

*“Look for robust interoperable set of components that meet internationally approved standards that create fast, scalable networks with robust components.”<sup>44</sup>*

In addition to engaging with current standards initiatives, justice partners can collaborate on identifying shared value. Some key questions to ask include:

- What use cases both span and / or resonate across agencies?
- Who are the key users?
- What are the existing processes for data exchange, and where are the opportunities from a user perspective?
- What are the common data sharing problems?
- Where can the biggest gains be made in terms of efficiency?
- What rules and policy changes are needed?

<sup>42</sup> James Barry. “Interoperability will change what a blockchain means and upend the order of the blockchain industry.” Medium.

<sup>43</sup> Ibid.

<sup>44</sup> James Barry. “Interoperability will change what a blockchain means and upend the order of the blockchain industry.” Medium.

### 3.8 Platform Options

The previously mentioned platforms were selected based on the need to support distributed application code and/or Smart Contracts. The Bitcoin blockchain can be ruled out because it only supports the Bitcoin cryptocurrency and cannot support distributed applications

Platform	Ethereum	Hyperledger Fabric	Corda (R3)	Quorum
<b>Description</b>	Blockchain based on bitcoin protocols <ul style="list-style-type: none"> <li>• Open source</li> <li>• Mature</li> <li>• Widely supported</li> <li>• Commonly available tools               <ul style="list-style-type: none"> <li>▪ GETH</li> <li>▪ Digital Wallets</li> </ul> </li> </ul>	Independent blockchain implementation <ul style="list-style-type: none"> <li>• Not based on Bitcoin or Ethereum</li> <li>• Built from the ground up</li> <li>• Transaction validation versus block validation</li> </ul>	Breaks the distributed ledger paradigm <ul style="list-style-type: none"> <li>• Shared facts</li> <li>• Each node has a “vault”</li> <li>• No globally shared database</li> <li>• Only parties to transaction maintain data</li> <li>• High data security</li> <li>• Regulatory and supervisory observer nodes</li> <li>• Notary service confirms uniqueness</li> </ul>	Domain specific implementation of Ethereum <ul style="list-style-type: none"> <li>• Financial Sector (J.P. Morgan)</li> <li>• All capabilities of Ethereum blockchain</li> <li>• Public and private transactions / contracts</li> </ul>
<b>Permission</b>	Permissionless No authentication	<b>Permissioned</b> <ul style="list-style-type: none"> <li>• Certificate Authority               <ul style="list-style-type: none"> <li>▪ Distributed and open</li> <li>▪ Shared trust but not centralized</li> </ul> </li> </ul>	<b>Permissioned</b> <ul style="list-style-type: none"> <li>• Permission Service</li> <li>• X.500 PKI</li> </ul>	<b>Permissioned</b> <ul style="list-style-type: none"> <li>• Permissions enforced by Enclave/permitted nodes</li> </ul>
<b>Fuel</b>	Native cryptocurrency <ul style="list-style-type: none"> <li>• Ether</li> <li>• Supports application-specific crypto currencies</li> <li>• ERC-20 Token Standard</li> </ul>	Native cryptocurrency <ul style="list-style-type: none"> <li>• None</li> <li>• Supports application-specific crypto currencies</li> <li>• ERC-20 Token Standard</li> </ul>	Native cryptocurrency <ul style="list-style-type: none"> <li>• None</li> <li>• Supports application-specific crypto currencies</li> </ul>	Native cryptocurrency <ul style="list-style-type: none"> <li>• Quorum-Ether</li> <li>• Supports application specific crypto currencies               <ul style="list-style-type: none"> <li>▪ ERC-20 Token Standard</li> <li>▪ Z-token</li> </ul> </li> </ul>
<b>Through-put</b>	Dependent on implementation Approx. 20 transactions per second	Dependent on implementation Approx. 750 – 1000 transactions per second	Dependent on implementation Approx. 170 transactions per second	Dependent on implementation ~140 Transactions per second

Platform	Ethereum	Hyperledger Fabric	Corda (R3)	Quorum
<b>Public / Private</b>	Public implementation <ul style="list-style-type: none"> <li>• Proof-of-work consensus protocol</li> <li>• Network of public mining nodes</li> <li>• Private implementations available</li> <li>• Proof-of-work or Proof-of-authority consensus protocols</li> <li>• Cloud implementations               <ul style="list-style-type: none"> <li>▪ AWS</li> <li>▪ Azure</li> <li>▪ IBM</li> </ul> </li> </ul>	Private implementations available <ul style="list-style-type: none"> <li>• Proof-of-authority consensus protocol               <ul style="list-style-type: none"> <li>▪ Permission based voting</li> </ul> </li> <li>• Cloud implementations               <ul style="list-style-type: none"> <li>▪ AWS</li> <li>▪ Azure</li> <li>▪ IBM</li> </ul> </li> </ul>	Enterprise implementation <ul style="list-style-type: none"> <li>• Commercial, supported distribution</li> <li>• Consensus by parties to transaction</li> <li>• Open source implementation</li> <li>• Community supported</li> <li>• Cloud implementations               <ul style="list-style-type: none"> <li>▪ AWS</li> <li>▪ Azure</li> </ul> </li> <li>• Interoperable with enterprise implementations</li> </ul>	Open source implementation <ul style="list-style-type: none"> <li>• Proof-of-authority (voting) consensus (resource efficient)</li> <li>• Cloud implementations</li> <li>• Azure</li> </ul>
<b>Distributed Application (DAPP)</b>	Distributed Application Language (Smart Contracts/ EVM) <ul style="list-style-type: none"> <li>• Solidity (almost exclusively)</li> </ul>	Distributed Application Language (Chaincode) <ul style="list-style-type: none"> <li>• NodeJS</li> <li>• Java</li> <li>• Go</li> </ul>	Distributed Application Language (JVM) <ul style="list-style-type: none"> <li>• Java</li> <li>• Kotlin</li> </ul>	Distributed Application Language (Smart Contracts/ EVM) <ul style="list-style-type: none"> <li>• Equivalent to Ethereum</li> <li>• Solidity (almost exclusively)</li> </ul>



## 4 Regulatory Considerations

The government response to blockchain developments is a work in process. As we know, the law is ever-changing, and the task of matching innovation and proper regulations with innovative blockchain technology is moving forward in the United States – even though more slowly than we might wish. Much of the progress to date has been at the state level. Many blockchain-related legal topics fall under primary or shared state authority.

These include:

- Evidentiary rules;
- Treatment of tokens as property;
- Blockchain in business governance and governmental processes;
- Contracting;
- Money transfer;
- Banking;
- Insurance; and
- Privacy.

The laws and regulations now emerging from the states fall into the “enabling” category, although there are also regulatory aspects.

At the federal level, the early application in cryptocurrency captured a great deal of attention, particularly from the Securities and Exchange Commission (SEC), which has been fixated on how business formations and crypto trading fit within the Federal securities laws.

On February 6, 2020, Commissioner Hester M. Peirce proposed a new securities act rule that puts a time-limited exemption for tokens.<sup>45</sup> The SEC and the FinHub, which is the SEC’s Strategic Hub for Innovation and Financial Technology, have submitted this proposal to the community first, without going through formal rule-making, because it is still early in understanding this technology and its implementation. However, Commissioner Peirce stated that she does “not expect the approach taken to date in Commission enforcement cases addressing digital assets to change in light of my safe harbor proposal.”<sup>46</sup>

This innovation is admirable from any agency but particularly from the SEC. Like the SEC, the U.S. Department of Health and Human Services (HHS) uses blockchain technology under the guidance of José Arrieta, who was appointed as the Chief Information Officer (CIO) for the Department in May 2019. One of the core values for using the technology is with provenance. This is “important in healthcare because it helps a person or entity receiving data be confident in its authenticity, trustworthiness, and reliability.”<sup>47</sup>

The provenance understanding of financial institutions and healthcare organizations sharing and receiving data operates under ethical standards as well. We have seen this happen at the intersection of emerging technologies and national security. With respect to artificial intelligence, the U.S. Department of Defense announced in February 2020 that their “principles will apply to both combat and non-combat functions and assist the U.S. military in upholding legal, ethical and policy commitments.”<sup>48</sup> In addition to emerging legislative and regulatory activity, the courts have begun to see blockchain-related cases. The common law is often credited with helping to align legacy legal principles with emerging activities. We see the emergence of court-related cases driving the regulatory and legislative activity even more throughout the next decade.

<sup>45</sup> Commissioner Hester M Peirce. “Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization.” U.S. Securities and Exchange Commission.

<sup>46</sup> Ibid.

<sup>47</sup> Health and Human Services. “HHS Announces Health Data Provenance Challenge Winners.”

<sup>48</sup> U.S. Department of Defense. “DOD Adopts Ethical Principles for Artificial Intelligence.” U.S. DOD.

## 5 Potential Justice and Public Safety Use Cases

The following use cases provided the incentive for the Blockchain Task Force. They were elicited from participants at a workshop at the IJIS Institute Symposium in February 2018.

1. **Digital assets:** validation of associated metadata and transactions
2. **Arrest/Bench warrants:** issue to dissemination
3. **Protection orders:** issue to dissemination
4. **Criminal history:** disposition recording
5. **Criminal history:** validation of data as part of dissemination
6. **Law enforcement:** sharing of officer testing and certification
7. **Dispatch:** resource sharing between agencies
8. **Information sharing:** API for digital notarization of documents
9. **Law enforcement:** interagency de-confliction

## 6 Case Study: Search Warrant, Bench Warrant, Arrest Warrant on Blockchain™

Reproduced with permission from JUSTICE CHAIN LLC (JUSTCHAIN – Arrest Warrant, Bench Warrant on Blockchain™ Whitepaper)

### 6.1 Introduction

Search warrants, bench warrants, and arrest warrants have traditionally been issued by judicial officers in paper form (with inked signatures), and in some cases electronically, to the law enforcement agency (LEA) executing the warrant. There are some inherent challenges to both approaches (with the latter being the least challenging), which include lack of real-time visibility of the warrant status, such as a judge overturning the warrant after it is issued to the LEA, manually entering data of warrant information and statuses into multiple systems, uploading the warrant into the LEA's system, FBI's Warrant system, etc., all of which can lead to wrongful arrests and costly lawsuits. An additional challenge is not quickly apprehending the criminal, due to delays in sending warrant information to authorities. The blockchain solution addresses these issues and more, which are discussed below.

### 6.2 Use Case

The following use case for a search warrant includes a law enforcement agency, judge or magistrate, and justice partners (FBI, sheriff, state police, etc.), with each having its own node on the blockchain network. The use case follows these steps:

- LEA submits a request for a search warrant along with the complaint and probable cause statement to a judicial officer (judge or magistrate), and in some cases, to a prosecutor.
- The transaction is instantly and securely recorded into the blockchain network, and, since it is a shared ledger, it is readily available to all interested participants, including the judge, prosecutor (depending on the nature of the warrant), and the LEA.
- A judge or magistrate acts on the request, either to grant or deny.
  - This information, along with any uploaded order for the Search Warrant, is again recorded on the blockchain network; all participants are instantly notified and can see the statuses in real-time, as well as the search warrant from the judicial officer.
  - If the warrant is granted, the LEA executes the warrant immediately.
  - If the warrant is overturned by a judge, the LEA can find out in real-time through the blockchain network without completing a "white-card" check to see if the warrant is still active with the records division.
- Justice partner agencies with authorized access can view the status and provide assistance in real-time, avoiding the need to manually enter the data into their own systems.

**Figure 12. Search Warrant Use Case from JUSTICE CHAIN LLC**

Arrest / Bench Warrant on Blockchain							
Status	ORI	Defendant Name	Date of Birth	Gender	Requested Date	Issued Date	Execution Date
Status	ORI	Defendant Name	Date of Birth	Gender	Requested Date	Issued Date	Execution Date
Executed	10001	Peter Parker	1985-01-26	Female	2020-02-11	2020-02-12	2020-02-12
Issued	10002	Spider Man	1986-02-22	Male	2020-02-11	2020-02-11	
Executed	10003	Sherlock Holmes	1958-01-26	Male	2020-02-11	2020-02-11	2020-02-11
Requested	10004	Iron Man	1968-11-15	Male	2020-02-11		
Executed	10005	Wonder Women	1990-10-09	Female	2020-02-11	2020-02-12	2020-02-12
Requested	10006	James Bond	1989-05-10	Male	2020-02-11		
Requested	10007	Captain America	1985-10-10	Male	2020-02-11		

Since all transactions are recorded on the blockchain, authorized users on the blockchain network can view a search warrant's history and updated transactions (Refer to Figures 6–9 below).

### 6.3 Blockchain Implementation Details

#### 6.3.1 Blockchain Technology Used

- Hyperledger Fabric – Permissioned and Ethereum Blockchain Permissioned

#### 6.3.2 SMART Contract

- The SMART Contract / Chaincode was developed in Solidity and Go.

### 6.3.3 Consensus Protocol

- Proof of Work (Ethereum) and Byzantine Fault Tolerance (PBFT)

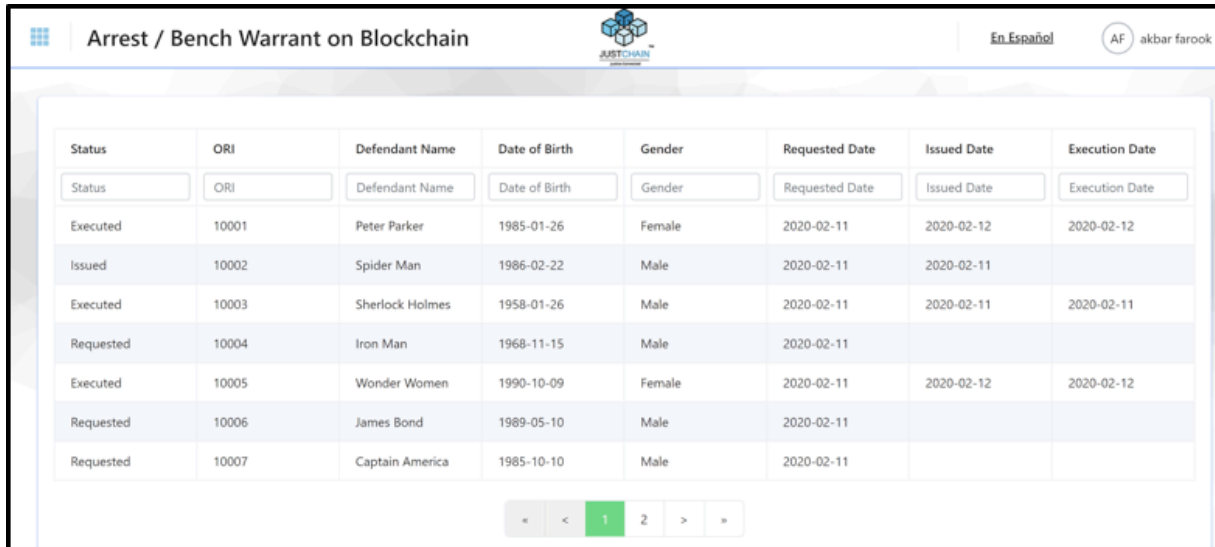
### 6.3.4 Identity and Access Management

- Identity Access Management: Wallets and Active Directory

### 6.3.5 Application User Interface Screenshots

Below are a few screenshots from the Arrest Warrant, Search Warrant, Bench Warrant Blockchain™ Application.<sup>49</sup>

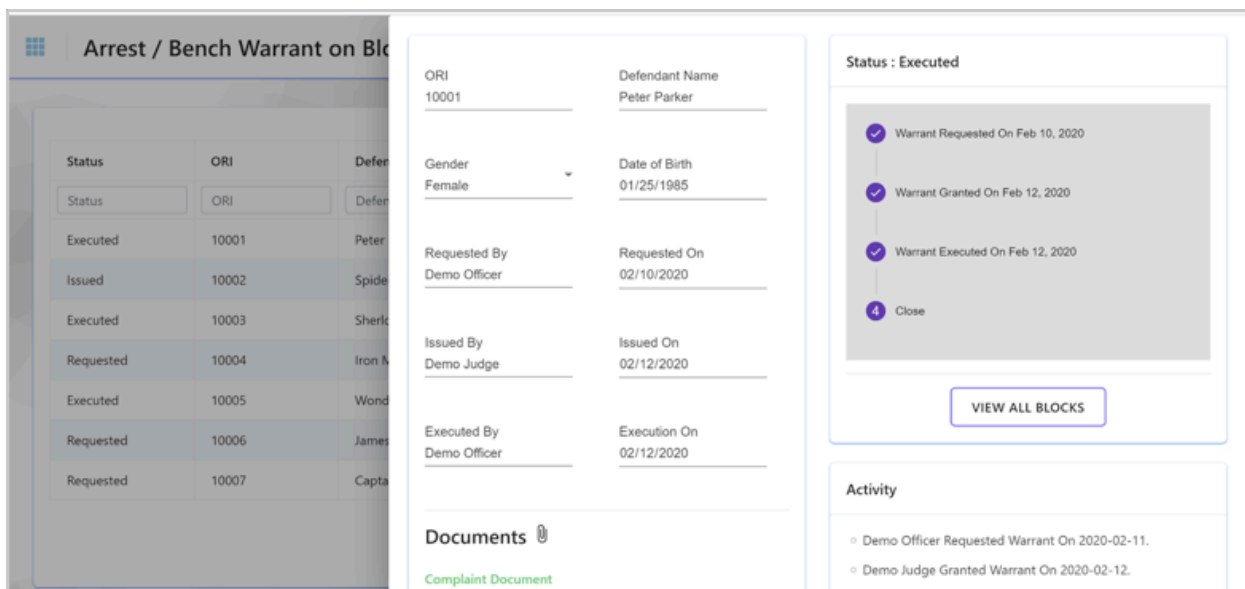
**Figure 13. Arrest / Bench Warrant from JUSTICE CHAIN LLC**



Status	ORI	Defendant Name	Date of Birth	Gender	Requested Date	Issued Date	Execution Date
Executed	10001	Peter Parker	1985-01-26	Female	2020-02-11	2020-02-12	2020-02-12
Issued	10002	Spider Man	1986-02-22	Male	2020-02-11	2020-02-11	
Executed	10003	Sherlock Holmes	1958-01-26	Male	2020-02-11	2020-02-11	2020-02-11
Requested	10004	Iron Man	1968-11-15	Male	2020-02-11		
Executed	10005	Wonder Women	1990-10-09	Female	2020-02-11	2020-02-12	2020-02-12
Requested	10006	James Bond	1989-05-10	Male	2020-02-11		
Requested	10007	Captain America	1985-10-10	Male	2020-02-11		

© JUSTCHAIN 2020

**Figure 14. Arrest / Bench Warrant from JUSTICE CHAIN LLC**



Status	ORI	Defendant Name	Date of Birth	Gender	Requested Date	Issued Date	Execution Date
Executed	10001	Peter Parker	1985-01-26	Female	2020-02-11	2020-02-12	2020-02-12

**Status : Executed**

- Warrant Requested On Feb 10, 2020
- Warrant Granted On Feb 12, 2020
- Warrant Executed On Feb 12, 2020
- Close

[VIEW ALL BLOCKS](#)

**Activity**

- Demo Officer Requested Warrant On 2020-02-11.
- Demo Judge Granted Warrant On 2020-02-12.

**Documents**

[Complaint Document](#)

© JUSTCHAIN 2020

<sup>49</sup> Source: JUSTICE CHAIN LLC – © JUSTCHAIN 2020

Figure 15. Arrest / Bench Warrant from JUSTICE CHAIN LLC

Transaction overview

Channel details

Block history

ID	Created	Transactions	Block hash
68	2/23/2020, 1:10:53 PM	1	6P44oQz3TAo+fsp3Uxib8wD+miQHdNu/WpKOuB77Mo=
67	2/11/2020, 11:57:23 PM	1	bKxvk/Y+YwxC5P4c3zB8nVDILE80K7oo1BMriy9Buks=
66	2/11/2020, 11:56:52 PM	1	CScXe8qBVCvPhSNaq9yeS2B39ADaT7HOQGbBJxr2ywI=
65	2/11/2020, 10:59:18 PM	1	5n+SwbjnWRuiHjhdhih0BoE7PjGELRx+2KQEntKORsU=
64	2/11/2020, 10:39:01 PM	1	KTuwwtCSh/ZIrgfcD5oODEDTb0ZnbDXNbs7WLAvoE4U=
63	2/11/2020, 10:38:56 PM	1	7r96v1d0ByxrneJew9GrX7JO7v/UhLfj3r1bRqhDEkw=
62	2/11/2020, 10:38:46 PM	1	HZf6N0Z9Y5z4Ry9FOITY2tWQY3G9W2gRnDmyKMCVHe0=
61	2/11/2020, 10:38:24 PM	1	/00B3PIdgOPoqNDhD5v/GCk2d9l7l130pi5r4MEJ2iQ=
60	2/11/2020, 10:38:07 PM	1	BM0RiCSbGQw9S9lFO8aOE4pHrmXA6fwnllUp91GWeME=

© JUSTCHAIN 2020

Figure 16. Arrest / Bench Warrant from JUSTICE CHAIN LLC

Block 68

Block created 2/23/2020, 1:10:53 PM

Transactions

Transaction ID	Created
77db962d3df52cac32feda55e7b60f340d170d51b5bd2a16e4b8e02821681739	2/23/2020, 1:10:53 PM

77db962d3df52cac32feda55e7b60f340d170d51b5bd2a16e4b8e02821681739

Smart contract ID  
warrants 1.0.1

Input  
["GetAllWarrants","1"]

Output  
There are no outputs for the smart contract.

© JUSTCHAIN 2020

## 7 Conclusion

There exists an increased demand to share information among agencies at the local, state, and federal levels and a need to comply with data privacy and security requirements.

The Task Force concluded that the benefits of ensuring an authoritative source, maintaining an up-to-date and valid document, and auditing a document's history for interaction merit additional investigations by bringing stakeholders together to discuss the development of a limited scope proof-of-concept.

Along with technical feasibility experimentation, a proof-of-concept would help explore optimal funding and procurement, data governance, and organizational models among participating local, state, and federal agencies and their vendors.

The steps to create a business case for using blockchain technology are no different than those required for any technology investment. What is unique when considering blockchain technology is that the business case requires establishing “shared value” across participating agencies, all of whom likely have different priorities and resources. What may be the most important use case or priority for law enforcement may differ for court, corrections, victim services providers, or other partners.

Focusing on how the solution will benefit the constituent, such as the petitioner for a protective order,<sup>50</sup> may be a way to work through each agency's priorities where they can agree on the shared value and benefit across organizations.

<sup>50</sup> IJIS Institute. “Use Case—Protective Orders.”



## Appendix A. Acronyms

Following is a list of some blockchain related acronyms.

Acronym	Description
2FA	Two-Factor Authentication
ABAC	Access-based Access Control
ALT	Alternative Cryptocurrency
AML	Anti-Money Laundering
ASIC	Application Specific Integrated Circuit
BFT	Byzantine Fault Tolerance
BJS	Bureau of Justice Statistics
BYOID	Bring Your Own Identity
CA	Certificate Authority
CCJ	Conference of Chief Justices
CCPA	California Consumer Privacy Act
CDC	Cloud Data Center
CEX	Centralized Exchange
CIO	Chief Information Officer
CITOC	Court Information Technology Officers Consortium
CJIS	Criminal Justice Information Services
COSCA	Conference of State Court Administrators
CPU	Central Processing Unit
CSO	Chief Security Officer
CSP	Cloud Service Provider
DAC	Discretionary Access Control
DAG	Directed Acyclic Graph
DAO	Decentralized Autonomous Organization
DAPP	Decentralized Application
DbAAS	Database as a Service
dBFT	Delegated Byzantine Fault Tolerance
DDO	DID Document Object
DDoS	Distributed Denial of Service
DEX	Decentralized Exchange
DIF	Decentralized Identity Foundation
DIDs	W3C Decentralized Identifiers
DLT	Distributed Ledger Technology
DPoS	Delegated Proof of Stake
DPKI	Distributed Public Key Infrastructure
ERC	Ethereum Request for Comments
EVM	Ethereum Virtual Machine
FBA	Federated Byzantine Agreement

FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GJXDM	Global Justice XML Data Model
HA	High Availability
HIPAA	Health Insurance Portability and Accountability Act
HW	Hardware Wallet
IAAS	Infrastructure as a Service
IACP	International Association of Chiefs of Police
IAM	Identity and Access Management
IdAM	Identity and Access Management
IBC	Inter-blockchain Communication
IBFT	Istanbul Byzantine Fault Tolerance
IBFT 2.0	Istanbul Byzantine Fault Tolerance (newer version of IBFT)
ICO	Initial Coin Offering
IDAAS	Identity as a Service
IdP	Identity Provider
IEPD	Information Exchange Package Documentation
IGA	Identity Governance and Administration
IJIS	Integrated Justice Information Systems
IdM	Identity Management
IOT	Internet of Things
ITO	Initial Token Offering
IWA	Integrated Windows Authentication
JPS	Justice and Public Safety
JTC	Joint Technology Committee
Kafka	Formal name of consensus protocol used by Hyperledger Fabric
KYC	Know Your Customer
LEA	Law Enforcement Agency
LN	Lightning Network
MAC	Mandatory Access Control
MCAP	Market Capitalization
MIPS	Millions of Instructions per Second
MoE	Medium of Exchange
NACM	National Association for Court Management
NCIC	National Crime Information Center
NCSC	National Center for State Courts
NIBRS	National Incident Based Reporting System
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NODS	National Open Data Standards
NONCE	Number Used Only Once

OAuth	Open Authorization
OID	Object Identifiers
OTC	Over the Counter
PAAS	Platform as a Service
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance
PBN	Public Blockchain Network
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PnD	Pump-and-Dump
PO	Protective Order
PoA	Proof of Authority (consensus algorithm)
PoET	Proof of Elapsed Time (consensus algorithm)
PoH	Proof of History (consensus algorithm)
PoS	Proof of Stake (consensus algorithm)
POST	Peace Officer Standards and Training
PoW	Proof of Work (consensus algorithm)
RA	Registration Authority
RAFT	Formal name of consensus algorithm
RBAC	Role-based Access Control
REM	Resource-Efficient Mining
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SC	Smart Contract
SEC	Securities and Exchange Commission
SegWit	Segregated Witness
SoV	Store of Value
SP	Service Provider
SSI	Self-Sovereign Identity
SSO	Single Sign-on
STO	Securities Token Offering
SUT	System Under Test
TCG	Trusted Computing Group
TPS	Transactions per Second
UCR	Uniform Crime Reporting (retired as of January 1, 2021; replaced by NIBRS)
UoA	Unit of Account
VA	Validation Authority
W3C	World Wide Web Consortium
XaaS	Anything as a Service
ZK	Zero Knowledge

## Appendix B. Glossary

For a glossary of blockchain terms, please see the following two references:

*The Blockchain Training Alliance* provides a downloadable three-page illustrated list of terms:

- Blockchain Training Alliance. “Glossary of Blockchain Terms.” Retrieved from: <https://blockchaintrainingalliance.com/pages/glossary-of-blockchain-terms> Web. April 28, 2019.

*The Blockchain Dictionary* provides a little more detail for blockchain related terms.

- Odinsky, Jordan. “Blockchain Dictionary.” June 28, 2017. Hackernoon. Retrieved from: <https://hackernoon.com/blockchain-dictionary-f4d098c9ef89> Web. February 4, 2019.

*BitInfoCharts* provides a range of statistics on major cryptocurrencies, including blockchain size (in GB), average block creation / hour, hashrate (Ehash/s), and the number of active addresses in the network.

- BitInfoCharts. Retrieved from: <https://bitinfocharts.com/> Web. March 23, 2020.

*The Blockchain Consensus Encyclopedia Infographic* helps make sense of 72 consensus algorithms, grouping them under more widely understood protocols.

- Blockchain Consensus Encyclopedia Infographic. Retrieved from: <https://tokens-economy.gitbook.io/consensus/blockchain-consensus-encyclopedia-infographic> Web. March 26, 2020.

## Appendix C. References

Acronis. “Blockchain, Cryptocurrencies, ICO – Learn the basics.” Retrieved from: <https://www.acronis.com/en-us/articles/blockchain/> Web. March 10, 2020.

All Acronyms. “Blockchain Abbreviations.” All Acronyms. March 2020. Retrieved from: <https://www.allacronyms.com/blockchain/abbreviations> Web. March 19, 2020.

Barry, James. “Blockchain Standards Part 2 of 5 – The International Standards Organizations.” Medium. Nov 11, 2018. Retrieved from: <https://medium.com/blockchain-standards/blockchain-standards-part-2-of-5-the-international-standards-organizations-340c2fc73e1e> Web. April 13, 2020.

Barry, James. “Blockchain Technology Needs Standardization Part 1 of 5.” Medium. Nov 7, 2018. Retrieved from: <https://medium.com/blockchain-standards/blockchain-technology-needs-standardization-596fbea2d0cf> Web. April 13, 2020.

Barry, James. “Interoperability will change what a blockchain means and upend the order of the blockchain industry.” Medium. Mar 11, 2019. Retrieved from: <https://medium.com/blockchain-standards/interoperability-will-change-what-a-blockchain-means-and-upend-the-order-of-the-blockchain-industry-975ded47b313> Web. April 13, 2020.

Bellas, ‘Geo’ George. “Blockchain as Evidence.” Trial Briefs. Vol 66, No. 3. Illinois State Bar Association. November 2019. Retrieved from: <https://www.isba.org/sites/default/files/sections/civilpracticeandprocedure/newsletter/Civil%20Practice%20and%20Procedure%20November%202019.pdf> Web. April 13, 2020.

Bitcoin Magazine. “What Is The Bitcoin Block Size Limit?” Bitcoin Magazine. Retrieved from: <https://bitcoinmagazine.com/guides/what-is-the-bitcoin-block-size-limit> Web. March 26, 2020.

Blockchainhub Berlin. “Smart Contracts.” Blockchainhub Berlin. July 2019. Retrieved from: <http://blockchainhub.net/smart-contracts/> Web. June 1, 2020.

Blockchain Training Alliance. “Glossary of Blockchain Terms.” Retrieved from: <https://blockchaintrainingalliance.com/pages/glossary-of-blockchain-terms> Web. April 28, 2019.

Blockchain Working Group, ACT-IAC Emerging Technology Community of Interest. “Blockchain Primer: Enabling

- Blockchain Innovation in the U.S. Federal Government.” October 17, 2017. NIST. Retrieved from: <https://www.actiac.org/act-iac-white-paper-enabling-blockchain-innovation-us-federal-government> Web. February 4, 2019.
- Blockgeeks. “Basic Primer: Blockchain Consensus Protocol.” Blockgeeks. Retrieved from: <https://blockgeeks.com/guides/blockchain-consensus/> Web. February 4, 2019.
- CoinSutra. “Top 10 Cryptocurrencies With Fast Transaction Speeds.” CoinSutra. September 6, 2019. Retrieved from: <https://coinsutra.com/transaction-speeds/> Web. March 19, 2020
- CWPC (Communicating with prisoners collective). “Restraining Orders Issued and in Effect in the U.S.” Across Walls. Retrieved from: <https://www.acrosswalls.org/statistics/restraining-orders/> Web. March 24, 2020.
- Daily Hodl. “Cryptocurrency Transaction Speeds: The Complete Review.” July 28, 2018. Retrieved from: <https://dailyhodl.com/2018/04/27/cryptocurrency-transaction-speeds-the-complete-review/> Web. March 19, 2020.
- Evernym. “Self-sovereign identity with verifiable claims: simply revolutionary.” Evernym. Retrieved from: <https://www.evernym.com/solution/> Web. February 2, 2019.
- Federal Public Key Infrastructure Guides. “High-level Illustration of the Federal PKI Certification Authorities.” Retrieved from: <https://fpki.idmanagement.gov/> Web. May 31, 2020.
- Ferris, Christopher. “Answering your questions on Hyperledger Fabric performance and scale.” Blockchain Pulse: IBM Blockchain Blog. January 29, 2019. Retrieved from: <https://www.ibm.com/blogs/blockchain/2019/01/answering-your-questions-on-hyperledger-fabric-performance-and-scale/> Web. March 26, 2020.
- Goldstein, Phil. “Blockchain and Identity Management for State Governments.” StateTech. March 31, 2020. Retrieved from: <https://statetechmagazine.com/article/2020/03/blockchain-and-identity-management-state-governments-perfcon> Web. April 27, 2020.
- GS1. “Bridging Blockchains”. GS1. Retrieved from: [https://www.gs1.org/sites/default/files/bridging\\_blockchains\\_-\\_interoperability\\_is\\_essential\\_to\\_the\\_future\\_of\\_da.pdf](https://www.gs1.org/sites/default/files/bridging_blockchains_-_interoperability_is_essential_to_the_future_of_da.pdf) Web. March 24, 2020.
- Hyland-Wood, David, Saltini, Roberto, Cassez, Franck, Fuller, Joanne. “Key Factors to Consider When Choosing a Blockchain Consensus Protocol.” Pegasys. January 23, 2020. Retrieved from: <https://pegasys.tech/key-factors-to-consider-when-choosing-a-blockchain-consensus-protocol/> Web. March 26, 2020.
- Hyperledger. “Hyperledger Architecture, Volume 1: Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus.” Hyperledger. Retrieved from: [https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger\\_Arch\\_WG\\_Paper\\_1\\_Consensus.pdf](https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf) Web. March 22, 2020.
- Hyperledger. “Hyperledger Architecture, Volume 2: Smart Contracts.” Hyperledger. Retrieved from: [https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger\\_Arch\\_WG\\_Paper\\_2\\_SmartContracts.pdf](https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf) Web. March 22, 2020.
- Hyperledger Fabric. “Glossary.” Hyperledger. Retrieved from: <https://hyperledger-fabric.readthedocs.io/en/release-2.0/glossary.html> Web. June 1, 2020.
- Hyperledger Performance and Scale Working Group. “Hyperledger Blockchain Performance Metrics”. Hyperledger. Retrieved from: <https://www.hyperledger.org/resources/publications/blockchain-performance-metrics> Web. March 26, 2020.
- Indu, I., Rubesh Anand, P.M., Bhaskar, Vidhyacharan. “Identity and access management in cloud environment: Mechanisms and challenges.” Engineering Science and Technology, an International Journal, Volume 21, Issue 4, pp 574-588. ScienceDirect. May 23, 2018. Retrieved from: <https://www.sciencedirect.com/science/article/pii/S2215098617316750#f0015> Web. March 30, 2020.
- Ismail, Leila, Materwala, Huned. “Leila Ismail and Huned Materwala. “A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions.” Symmetry. MDPI. September 24, 2019.
- Kreshmer, Ken. “About Ken Krechmer”. Isology.com. Retrieved from: <https://www.isology.com/kens-bio/> Web. July 13, 2020.

- Kwaasteniet, Aat de. "The nonsense of ... TPS (transactions per second)." Medium. November 30, 2018. Retrieved from: <https://medium.com/@aat.de.kwaasteniet/the-nonsense-of-tps-transactions-per-second-2d7156df5e53> Web. March 22, 2020.
- Martin, James A, Waters, John K. "What is IAM? Identity and access management explained." CSO United States. October 9, 2018. Retrieved from: <https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html> Web. April 27, 2020.
- Microsoft. "Decentralized Identity." Microsoft. Retrieved from: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2Djfy> Web. February 4, 2019.
- Mulligan, C., Rangaswami, J.P., Warren, S., & Scott, J. Z. "Blockchain Beyond the Hype." World Economic Forum. 23 April, 2018. Retrieved from: <https://www.weforum.org/whitepapers/blockchain-beyond-the-hype> Web. September 5, 2018.
- Nallathamby, Johann. "What is Federated Identity Management." WSO2. June 18, 2018. Retrieved from: <https://wso2.com/articles/2018/06/what-is-federated-identity-management/> Web. March 31, 2020.
- NeonVest. "The Scalability Trilemma in Blockchain." NeonVest. Medium. October 19, 2018. Retrieved from: [https://medium.com/@aakash\\_13214/the-scalability-trilemma-in-blockchain-75fb57f646df](https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df) Web. April 1, 2020.
- Open document. "Pricing for IBM Blockchain Platform for IBM Cloud." Last Updated 5 February, 2020. Retrieved from: <https://cloud.ibm.com/docs/services/blockchain?topic=blockchain-ibp-saas-pricing#ibp-saas-pricing-scenarios> Web. February 5, 2020.
- Odinsky, Jordan. "Blockchain Dictionary." June 28, 2017. Hackernoon. Retrieved from: <https://hackernoon.com/blockchain-dictionary-f4d098c9ef89> Web. February 4, 2019.
- Peirce, Hester M. "Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization." February 6, 2020. U.S. Securities and Exchange Commission. Retrieved from: <https://www.sec.gov/news/speech/peirce-remarks-blockress-2020-02-06> Web. March 18, 2020.
- Saini, Vaibhav. "ConsensusPedia: An Encyclopedia of 30+ Consensus Algorithms." Hackernoon. June 26, 2018. Retrieved from: <https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f> Web. March 19, 2020.
- Shacklett, Mary. "IT cost / benefit analysis: Why it matters and how to do it right." TechRepublic. October 31, 2017. Retrieved from: <https://www.techrepublic.com/article/the-value-of-it-costbenefit-analysis-and-how-to-do-it-right/> Web. April 27, 2019.
- Simms, Thomas. "Upgraded Hyperledger Fabric Sees 7-Fold Increase in Transaction Speed." Cointelegraph. May 2, 2019. Retrieved from: <https://cointelegraph.com/news/upgraded-hyperledger-fabric-sees-7-fold-increase-in-transaction-speed> Web. March 22, 2020.
- Song, Jimmy. "Why Blockchain is Hard." May 14, 2018. Medium. Retrieved from: <https://medium.com/@jimmysong/why-blockchain-is-hard-60416ea4c5c> Web. April 28, 2019.
- Standards Australia. "Roadmap for Blockchain Standards: Report March 2017." Standards Australia. March 2017. Retrieved from: [https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a2e1/Roadmap\\_for\\_Blockchain\\_Standards\\_report.pdf.aspx/](https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a2e1/Roadmap_for_Blockchain_Standards_report.pdf.aspx/) Web. April 13, 2020.
- Sullivan, Nick. "How to build your own public key infrastructure." Cloudflare. June 24, 2015. Retrieved from: <https://blog.cloudflare.com/how-to-build-your-own-public-key-infrastructure/> Web. March 30, 2020.
- TheBlockBox. "Fundamentals of Hyperledger Fabric." June 25, 2019. Retrieved from: <https://www.theblockbox.io/fundamentals-of-hyperledger-fabric/> Web. March 23, 2020.
- u/JcollinsVect. "Transactions Per Second (TPS)?" reddit. Retrieved from: [https://www.reddit.com/r/CryptoCurrency/comments/8do3au/transactions\\_per\\_second\\_tps/](https://www.reddit.com/r/CryptoCurrency/comments/8do3au/transactions_per_second_tps/) Web. March 19, 2020.
- U.S. Department of Defense. "DOD Adopts Ethical Principles for Artificial Intelligence." U.S. Department of Defense.



- February 24, 2020. Retrieved from: <https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/> Web. March 18, 2020.
- U.S. Department of Health and Human Services. “HHS Announces Health Data Provenance Challenge Winners.” U.S. Department of Health and Human Services. March 13, 2018. Retrieved from: <https://www.hhs.gov/about/news/2018/03/13/hhs-announces-health-data-provenance-challenge-winners.html> Web. March 18, 2020.
- Wahab, Abdul and Memood, Waqas. “Survey of Consensus Protocols.” arXiv.org. Cornell University. Retrieved from: <https://arxiv.org/pdf/1810.03357.pdf> Web. April 1, 2020.
- Wikipedia. “Identity management.” Wikipedia. Retrieved from: [https://en.wikipedia.org/wiki/Identity\\_management#Organization\\_implications](https://en.wikipedia.org/wiki/Identity_management#Organization_implications) Web. March 30, 2020.
- Wikipedia. “Interoperability.” Wikipedia. Retrieved from: <https://en.wikipedia.org/wiki/Interoperability> Web. March 24, 2020.
- Wikipedia. “Public key infrastructure.” Wikipedia. Retrieved from: [https://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](https://en.wikipedia.org/wiki/Public_key_infrastructure) Web. March 30, 2020.
- World Economic Forum. “Building Value with Blockchain Technology: How to Evaluate Blockchain’s Benefits.” WEF. July 2019. Retrieved from: [http://www3.weforum.org/docs/WEF\\_Building\\_Value\\_with\\_Blockchain.pdf](http://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf) Web. April 13, 2020.
- Yaga, Dylan, Mell, Peter, Roby, Nik, Scarfone. “NISTIR 8202. Blockchain Technology Overview.” October, 2018. Retrieved from: <https://csrc.nist.gov/publications/detail/nistir/8202/final> Web. February 4, 2019
- Youngson, Nick. “Blockchain Consensus Encyclopedia.” Consensus. GitBook. Last updated February 2020. Retrieved from: <https://tokens-economy.gitbook.io/consensus/> Web. March 26, 2020.
- Zhang, Shijie, Lee, Jong-Hyoun. “Analysis of the main consensus protocols of blockchain.” ScienceDirect. August 7, 2019. Retrieved from: <https://www.sciencedirect.com/science/article/pii/S240595951930164X>