Blockchain Task Force

USE CASE ASSESSMENT

Protective Orders

Jim Kita
Solution Architect,
Analysts International

Tom Messerges
Chief Technology Office,
Motorola Solutions, Inc.

Anil Sharma
Software Client Architect, IBM

Anne Thompson
Thompson | Finn LLC

Steven White
Missouri State Highway Patrol

IJIS Institute

Acknowledgments

This document is a product of the IJIS Institute, 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 Cardiellos
IJIS Institute

Paul Embley
National Center for State Courts

Akbar Farook
Global Justice Solutions

Tim Grapes
IJIS Institute

Di Graski
National Center for State Courts

Josh Jackson
Emory University

Jim Kita
Analysts

Tom Messerges
Motorola Solutions

Greg Park
City of Livermore

Anil Sharma
IBM

Andrew Owen
Search

Anne Thompson
Thompson | Finn LLC

Eric Tumperi
CorrectTech

Steven White
Missouri State Highway Patrol

Additional Contributors

The following individuals provided invaluable review and feedback.

Ashwini Jarral
IJIS Institute

Bob Kaelin
MTG Management Consultants

Susan Keilitz
National Center for State Courts

Shelley Spacek
National Center for State Courts

Iveta Topalova
Microsoft Corporation

Comments and Questions

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

Table of Contents

Table of Figures

1 | Executive Summary

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

Specifically, it investigates the protective order use case for Missouri and how blockchain technologies can address security, authority and validity, and auditability challenges.

Introduction

The IJIS Blockchain Task Force set out to:

- Evaluate whether distributed ledger technologies (i.e., blockchain technologies) can assist participants in the protective order process to more efficiently and effectively issue and disseminate protection orders, as well as address challenges related to security, authority, validity, and auditability
- Provide a generic use case evaluation framework to help practitioners in roles related to records management and information sharing determine whether blockchain should be considered when evaluating proposed changes to current processes and systems.

The protective order was selected based on task force membership and associated subject-matter expertise, while supporting a realistic scope within justice information management and sharing.

The Task Force used the following definition for blockchain from Hackernoon[1]:

> *"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 protective orders, which ensures that a protective order is:

- Authoritative (pertaining to a judge's signature, jurisdiction of law enforcement, services available to petitioner)
- Authentic (valid and current)
- Auditable (accurate record and timeline of document interaction)

Previous work completed by various organizations, such as Search and the National Center for State Courts (NCSC), establishes a basis for awareness and usage standards related to data exchange regardless of the technology used.

[1] Jordan Odinsky. "Blockchain Dictionary." Hackernoon.

The Protective Order Process and Problem

The Task Force analyzed the current protective order process for Missouri, concluding that many factors contribute to the challenges faced for accurate and timely protective order distribution and management.

These include:

- Highly manual, paper-based process
- Organizational factors (e.g., structure, hierarchy)
- Funding and procurement (e.g., different funding sources, priorities, and budget cycles)
- Data (e.g., governance, interchange standards, and quality)
- Technology (e.g., proprietary systems, interoperability, architecture, and maturity)

Assuming that courts, prosecutors, and law enforcement implement electronic data exchange protocols for information sharing, a private, permissioned blockchain model[2] has the potential to provide additional benefits beyond other shared database models.

The following table describes characteristics common to public and private blockchains. The Task Force is preparing an accompanying Technical Framework document that will discuss these in more detail.

BLOCKCHAIN CHARACTERISTIC	DESCRIPTION	BENEFIT
Trust between untrusted parties	Ensure that only one record exists when shared with general public and third-parties (as appropriate)	*Example:* Petitioner and respondent ensure that any record made public is always accurate.
Data integrity (Immutability)	Confidence that no one has altered information on the protective order	*Example:* Law enforcement can rely on the protective order and remain confident that it accurately reflects what the court determined.
Provenance	Confidence that the protective order being viewed is authentic and valid	*Example:* Agencies providing services can do so more efficiently.
Relative timestamp	Ability to see transaction timeline for protective order and everyone who interacted with the document (e.g., search, view, update, etc.)	*Example:* It provides law enforcement with certainty as to the authority and validity of a protective order (i.e., granted by court, entered in NCIC, served, updated, revoked, etc.).

[2] A private blockchain differs from a public blockchain in that it is only shared amongst trusted participants and permissions are governed by these participants.

Assessment Frameworks

The document includes two sample frameworks:

- The Worldwide Economic Forum (WEF) "Blockchain Applicability Decision Tree"[3]
- Department of Homeland Security (DHS) Science and Technology Directory's Flow Chart as provided in the NISTIR 8202 Blockchain Technology Overview[4]

The Task Force developed a third framework, "Blockchain Applicability Requirements Matrix," to help address the ongoing question of how a blockchain-based solution—based on a private, permissioned network—differed from a distributed database model with centralized permissions.

Two frameworks were applied to the Missouri Protective Order use case:

- Blockchain Applicability Decision Tree (WEF)
- Blockchain Applicability Requirements Matrix (developed by the Task Force)

Regardless of the framework used, essential questions aside from cost (which will be discussed in the subsequent companion document being prepared by the Task Force, "Technical Framework—Justice and Public Safety") when assessing whether blockchain or distributed ledger technologies are appropriate for justice and public sector use cases include:

- **Trust:** Are you certain of the authority of those conducting transactions? For example, do you need certainty regarding the authority behind a signature?
- **Data Integrity:** How important is it to know that no one changed or modified a transaction?
- **Provenance / Ownership:** Do you need the ability to see who has done what and / or who is participating in the life of a document?
- **Auditability / Relative Timestamp:** Is it important to know when something occurred during the transaction?

Additional Benefits

While not unique to blockchain, this technology provides flexibility for different organizations using various records management systems and workflows to share information, as well as trigger workflow events more efficiently.

For example, a petitioner granted a protective order and seeking services based on its authority would no longer have to present a physical record, and the service provider would be ensured the request is valid. The end-to-end auditability through multiple agencies also has the potential to provide more accurate reporting and capture a trusted account of the life-cycle of a participant's interaction with the justice system. Participants in the network "do not have to rely on a central entity to manage the system and mediate transactions."[5]

In addition, the nature of how changes to the data are agreed upon through consensus protocols provides an additional layer of security.

[3] Catherine Mulligan, Jennifer Zhu Scott, Sheila Warren, JP Rangaswami. "Blockchain Beyond the Hype: A Practical Framework for Business Leaders" World Economic Forum. April 23, 2018.
[4] Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. "Blockchain Technology Overview." October, 2018.
[5] ConsenSys, "11 Ways Ethereum Can Benefit Enterprise." October 18, 2018.

Evaluation and Proof-of-Concept Checklists

Assuming that the evaluation framework supports the use case, the Task Force developed a short checklist to help stakeholders determine next steps, including a proof-of-concept to enable further evaluation.

Open Questions

Blockchain technology continues to mature and various questions remain open, particularly regarding jurisdictional differences (i.e., state and federal levels); for example, how expungement is defined and what this means for an "immutable" record.

Conclusion

There is an increasing demand to share information among agencies at the local, state, and federal levels and a concurrent 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 efforts and investigations by bringing stakeholders together to discuss the development of a limited scope proof-of-concept.

Along with experimenting with technical feasibility, a proof-of-concept would help explore optimum funding and procurement, data governance, and organizational models among participating local, state, and federal agencies and solution providers.

2 | Related Documents

TITLE	AUTHORS	LOCATION
Technical Framework—Justice and Public Safety	Akbar Farook, Jim Kita, Anil Sharma, Anne Thompson, Steven White	IJIS Institute In progress: email info@ijis.org

3 | Audience

This document was developed for public sector executives and managers who manage and share information related to protective orders. They include judicial officers, court administrators and technologists, local, state and federal law enforcement, corrections and advocacy officials, and victim support agencies.

4 | Purpose

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

Specifically, the document investigates the protective order use case for Missouri and how blockchain technologies can be used to address security, authority or validity, and auditability challenges.

5 | Introduction

5.1. Task Force

The IJIS Blockchain Task Force was established in July 2018 following the 2018 IJIS Symposium. At the symposium, we elicited ten potential use cases (see "IJIS Symposium Use Cases"- Appendix 16.1) that could benefit from the unique characteristics provided by distributed ledger technology: security, transparency, immutability, auditability, shared administration, and governance.

The Task Force has two goals:

- Provide an assessment regarding the technology suitability for one of the use cases identified by the IJIS community and an evaluation framework for other use cases
- 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 is on the first goal: use case evaluation. *It is not intended to provide detail or recommendations regarding a technical framework.* The Task Force is working on a companion document to address technical aspects.

5.2. Protective Orders Use Case

The Task Force focused on Protective Orders and, more specifically, on issuing and disseminating a protection order for four reasons:

1. Expertise of task force participants
    1.1. Ability to follow up with a technical proof-of-concept (POC)
    1.2. Potential for seeking additional grant funding from relevant agencies
    1.3. The narrower scope of the use case (compared to the complexity of criminal history records)

5.3. Working Blockchain Definition

There are many definitions for blockchain. For clarification, we chose the following from Hackernoon[6]:

> *"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."*

5.4. Working Hypothesis for Blockchain and Protective Orders

Blockchain technology offers the potential to meet stakeholders' needs who manage and share information related to protective orders to ensure a protective order is:

- Authoritative (pertaining to a judge's signature, jurisdiction of law enforcement, services available to petitioner)
- Authentic (valid and current)
- Auditable (accurate record and timeline of document interaction)

5.5. Standards

Search

As part of Search Group's Justice Information Exchange Model (JIEM)[7] project, which began in the early 2000s and is supported by the U.S. Bureau of Justice Assistance, protective orders were selected (under recommendation by the Joint Technology Committee[8]) as one of the most commonly used court forms involving daily data exchange. Missouri was one of the states that provided input for the data elements for protective orders.

This led to the development of national standards to exchange protective order information while integrating it with the National Information Exchange Model (NIEM) and the Global Reference Architecture (GRA). Information Exchange Package Documentation (IEPD) that defines "reference" information exchanges was developed for protective orders. The IEPD "package" includes artifacts (e.g., documents, schemas, diagrams, and sample xml) that describe technical and functional requirements for data exchange.[9]

National Center for State Courts

The National Center for State Courts (NCSC) continues to work at state and cross-jurisdictional levels on projects supported by grant funding made available to the courts through the Violence Against Women Act (VAWA).

[6] Jordan Odinsky. "Blockchain Dictionary." Hackernoon.
[7] Justice Information Exchange Model (JIEM). Search.
[8] Protection Order Definition – 4.2 Process. NCSC.
[9] Patrick Brooks. "Making Good on the Promise of NIEM: Building an IEPD from the Ground Up." NCSC

The Office on Violence Against Women (OVW) was created in 1995 and is administered by the U.S. Department of Justice to provide financial and technical assistance through formula-based and discretionary funding.

Under VAWA's Services, Training, Officers, Prosecutors (STOP) Formula Grant Program, "Each state and territory must allocate 25 percent for law enforcement, 25 percent for prosecutors, 30 percent for victim services (of which at least 10 percent must be distributed to culturally specific community-based organizations), 5 percent to state and local courts, and 15 percent for discretionary distribution."[10]

The VAWA Courts Assistance project is a collaboration between the NCSC and the Conference of State Court Administrators (COSCA), with funding from OVW. The project encourages innovative use of STOP Project funds for courts. Any future efforts to investigate blockchain applicability for the protective order process should build upon previous efforts of these key stakeholder organizations.

6 | The Protective Order (PO) Process

6.1. Missouri

The protective order process involves the public, attorneys, the courts, law enforcement, and service providers. The process for Missouri is described below, noting that it may differ depending upon jurisdiction.

Current Process

Missouri's Protection Order (PO) system is paper-based. After the judge issues the protection order at the court, it is either faxed, delivered by hand, or emailed as a PDF to the sheriff's office. There are 115 sheriff's offices in Missouri that have Originating Agency Identification Numbers (ORIs). This includes 114 counties that have a sheriff and the City of St. Louis. However, not all sheriff's offices handle POs. For example, the sheriff of St. Louis doesn't enter or handle POs. In addition, some sheriff officers delegate 911 center staff to manage this process. A PO may be issued by a federal court; however, this is rare. A records clerk at the sheriff's office manually enters the protection order into the Missouri Uniform Law Enforcement System (MULES). The protection order is then automatically sent by MULES to the FBI's National Criminal Information Center (NCIC).

Any changes or updates to the order are made to the PO in the state's system and passed to NCIC. There is no indication of what was updated, only that the record was updated. The NCIC database only shows the most recent record.[11] In order for law enforcement to see the protective order's history, they must submit a request to view the audit log to NCIC staff. NCIC staff completes the request and compiles the relevant log files, which contain raw data recording all captured transactions. This request occurs several times a year, either as a result of litigation or internal quality assurance. In these instances, it is manual, lengthy, and time-consuming.

Either a shared database or blockchain technologies could make the auditing process easier, enabling participants to execute queries independently of other participants (assuming this has been agreed upon). However, only blockchain provides certainty that the record has not been changed due to its immutability characteristics and the way transactions are validated.

There is also a greater level of flexibility allowing different agencies to maintain policies and procedures independently, while still ensuring the integrity of a record exchange.

Prioritization and Notification

Since Missouri's protective order process is manual, there are no specific time measurements. Each sheriff sets the

[10] OVW Grants and Programs – Formula Grant Programs. US Department of Justice
[11] NCIC staff can conduct an audit; however, law enforcement officers are only able to access the most recent record.

priority and process for entering the protection orders, although this usually occurs within 24 hours. The sheriff also determines how and when the protection order is served.

The protection order is enforced upon being served. Once the protection order is served, there is a manual process for the sheriff's office to notify the court. The sheriff's office also updates the served status of the protective order in MULES—also within 24 hours—and the change in status is pushed to the NCIC.

Service

Due to the current manual process, turnaround time for recording services can be delayed. The victim has to opt in to receive email notifications at the court. The sheriff's office has 24 hours following service to update the record by notifying the court and updating MULES, which updates NCIC.

Again, a shared database and blockchain technologies could provide a solution to enable real-time access to status of the PO. Blockchain technologies would enable greater certainty regarding the authority and validity of the record's status.

Real-time access is important so that:

- the victim is notified as soon as possible that the protection order has been served
- law enforcement agencies know about the existence of a protection order, whether it has been served, and remain confident of its authority and validity.

Responsibilities

The court is the authority for issuing the PO, and the sheriff's office is responsible for entering the POs into MULES. MULES includes other records, such as criminal history records and warrants, and comprises proprietary and homegrown technologies. Law enforcement is responsible for service and enforcement.

Records Management

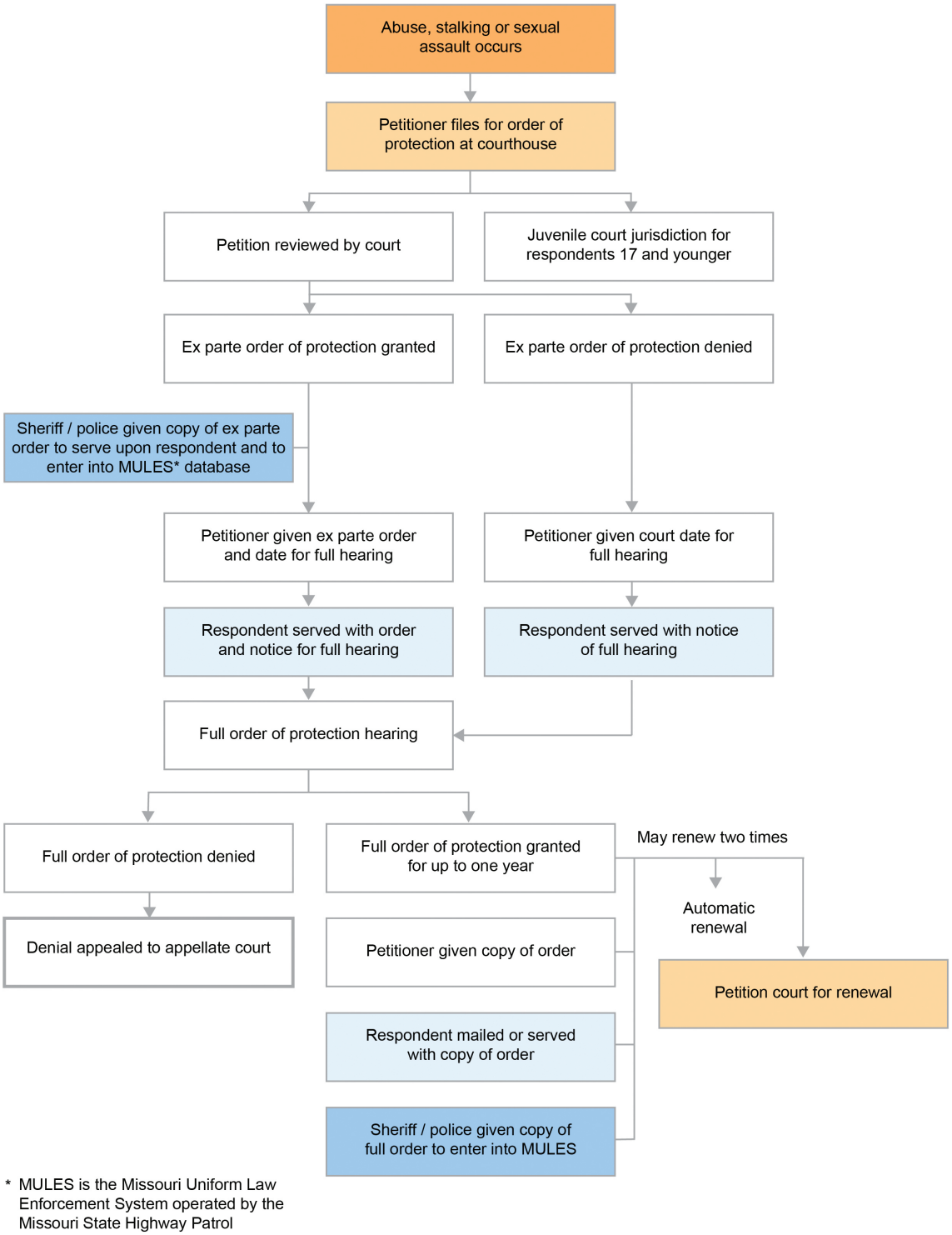
As this is a paper process, the sheriff's office maintains a fax of the court issued protective order (traditional filing systems). Missouri is digitizing its records; however, trust between agencies remains an issue regarding accuracy. This is due to current business processes for information exchange with the sheriff's office, which may affect how a PO's authority and validity is determined.

Data Quality

Communicating between the court and the sheriff's office resulted in past errors and inconsistent or lacking data elements. If law enforcement determine that they received incorrect information from the court, they may resolve this by entering partial data (e.g., name and birth date). An email may be sent in the interim for expediency; however, this may be inconsistent with the faxed, paper, or PDF copy received. As a result, the sheriff currently requires a physical copy, whether fax, paper, or PDF, of the protection order signed by the judge, before their office will process it. This may be more of an issue for states with decentralized or ununified systems where courts and law enforcement establish their own policies and procedures.

Blockchain will not resolve issues with data quality or address human error; however, it will mitigate the potential for error by maintaining one record of authority, assuming that all agencies participate.

Figure 1. Procedure for Obtaining an Order of Protection[12]



[12] "Domestic Violence and the Law: A Practical Guide for Survivors" Missouri Coalition Against Domestic and Sexual Violence (MCADSV).

Expiration and Revocation of PO

Once issued, a PO is generally valid for sometime after its expiration. During this time, a PO may also be invalidated by a subsequent court order addressing the PO.

A paper-based system delays the process. A protection order may have also been revoked by the court. The time to process and remove a revoked PO from the law enforcement system and from NCIC could lead to the respondent's unlawful detainment. To mitigate this issue, the police officer on scene will check with dispatch, who may need to check with the court to determine if the protection order was revoked. There is a possibility that the petitioner and respondent will have more recent paper copies of a protection order than law enforcement due to the existing manual process to update, enter, or remove protection orders from the law enforcement system.

6.2. Jurisdictions Differ

A baseline for jurisdictions considering blockchain technology implementation is whether they are currently able to digitally exchange information with justice partners.

The key differentiators that blockchain technology can enable are authoritative source (i.e., verified signature), validity (i.e., sole record, up-to-date), and immutability (i.e., tamper-resistant and auditable).

In addition, efficiencies implemented by a centralized database or cloud-based records management system, such as simultaneous access by multiple agencies, could be considered as part of a blockchain-enabled solution.

6.3. Key Roles in the Process

The key roles in the protective order process include:

ROLE	RESPONSIBILITY
Issuing Judge	Adjudicate
Court Clerk	Enter information into court case management system
Petitioner(s)	Filing the claim
Respondent(s)	Named in the claim
Attorneys for the Petitioner(s)	Represent the petitioner
Attorneys for the Respondent(s)	Represent the respondent
Law Enforcement Agency[13]	Enforce the PO Enter PO into state repository and FBI's NCIC database
State Law Enforcement	Enforce the PO
Federal Law Enforcement	Enforce the PO FBI maintains an NCIC record as submitted by the Law Enforcement Agency
Victim Assistance: Formal secure, trusted, and confidential organizations	Provide victim assistance
General Public	The information within a protective order is highly sensitive and access protected by law. It is only viewable by those who have authority to do so.

[13] While uncommon, federal courts can issue a PO. It is unclear who enters the information into NCIC in this case.

7 | The Protective Order (PO) Problem

7.1. Why is This a Hard Problem?

Any process involving interagency records management that includes multiple stakeholders, technologies, and methods of data exchange, and when the data exchanged is highly sensitive, makes proposed changes to existing processes and systems challenging.

Contributing factors include:

Organizational
Is the organization structured for change? Complex organizations with hierarchical, formal structures create additional challenges for achieving stakeholder buy-in and decision-making.

Funding and 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 in an organization? Are there alternative funding sources?

Data
The data contained within protective orders (POs) is highly sensitive in nature and may be subject to regulatory and legislative requirements regarding dissemination (e.g., time standards), access, availability, management and governance (e.g., controls and audit), and privacy.

Federal versus state requirements need to be considered and reconciled with respect to available victim data online and requirements related to sealed records and expungement. This is non-trivial and is an area where IJIS could assist with and inform on the regulatory, legislative, and policy changes that benefit all stakeholders.

Technology and Standards
Is the proposed alternative technology mature? Are standards in place? Governance (controls / audit capabilities)?

The benefits of an improved process for issuing and disseminating protective orders must be measurable and consider the above factors in order to provide incentive for change.

> *The key differentiator in using blockchain technology is the potential it provides as a trusted, authoritative source simultaneously to multiple parties (i.e., court, law enforcement, petitioner, service providers).*

7.2. Jurisdictional Considerations

Some jurisdictions may be a better fit than others depending upon whether the state follows a decentralized or centralized model in terms of technology and funding models.

Decentralized
For decentralized states, various solutions and stakeholders can make implementation and interoperability more difficult. Funding challenges can also occur related to available revenue, procurement policies and procedures, and the need to negotiate between counties, etc.

Centralized
Funding cycles can depend on state-level administration and are subject to legislative requirements for budget approval.

Competing priorities may make it challenging to prioritize investment, especially when it involves emerging technologies.

7.3. Missouri

This section lists the problems from stakeholder perspectives.

Issuing Judge
The judge is the authoritative source (signatory) of the protective order. If there is any doubt in the judge's signature, then the judge's availability is a dependency. Note that if there is doubt about the data in the PO, blockchain could not solve this. The court clerk is able to correct data without requiring the judge to re-sign (e.g., if an address needs to be corrected). The court clerk's availability would be an issue for missing or incorrect data.

Court Clerk
The court clerk is responsible for ensuring that the data quality is correct, complete, and accurate.

Petitioner
The petitioner's safety depends on the service of the protection order. Law enforcement may not be aware of the signed order until 24 hours after it has been issued, and additional delays may occur due to paper processes and manual data entry. The petitioner may request notification of service, requiring law enforcement to submit this information to the court following service. In addition, eligibility for services may depend on the validity of the protection order.

Attorneys
An attorney may be selected to represent the petitioner and the defendant. The attorney needs to see the facts on file related to the protective order, from request to issuance, whether temporary via an interview with the judge, or permanent, following a formal hearing.

Law Enforcement (Local, State, and Federal)
Law enforcement needs to access an updated version of the document and ensure it is accurate and valid (enforceable). Due to current manual processes, there may be a change in either information and / or status of the protective order before law enforcement entered the original order into MULES to comply with the 24-hour time standard.

For example, in instances where a judge's subsequent order cancels, or in some way revokes the parameters of the protective order, law enforcement may not enter anything into MULES if the update is received within the 24-hour period of the original order (now cancelled).

More than simply automating the process for efficient order processing and updates, blockchain technology would improve confidence levels surrounding source authority, which is not currently possible through current shared database technologies.

There exists an additional potential benefit that other attributes relevant to the petitioner and respondent may be made available (as appropriate), providing a more complete picture for law enforcement engagement.

Victim Assistance
This includes social workers or domestic violence shelters. Some domestic violence shelters do not have access to a system for viewing protection orders and have to rely on the client / petitioner for a valid paper copy of the protection order. Also, social workers and victim advocates would benefit from viewing the protection order process so they can assist victims. While access to a shared database could also accomplish this, blockchain technologies would provide a greater level of certainty about the authority, accuracy, and status of the protective order. Once governance over who has what kind of data access is established among participants, specific permissions for search and view access to

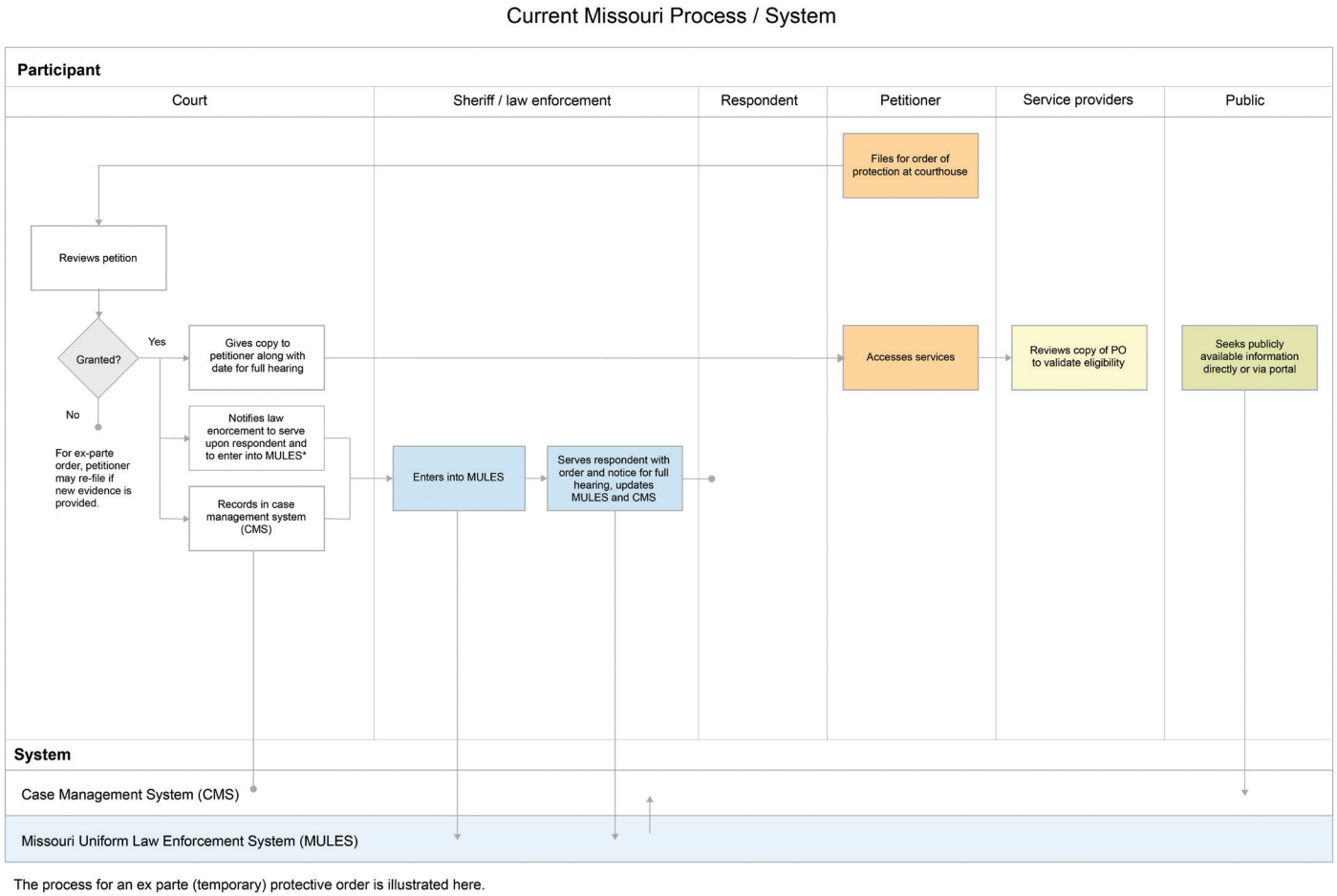
relevant parts of the record may be granted, which protects sensitive data.

General Public

For any third party with permission to see a protective order, it is imperative that the information they receive is accurate and updated. Blockchain technology ensures that the protective order is authoritative and valid.

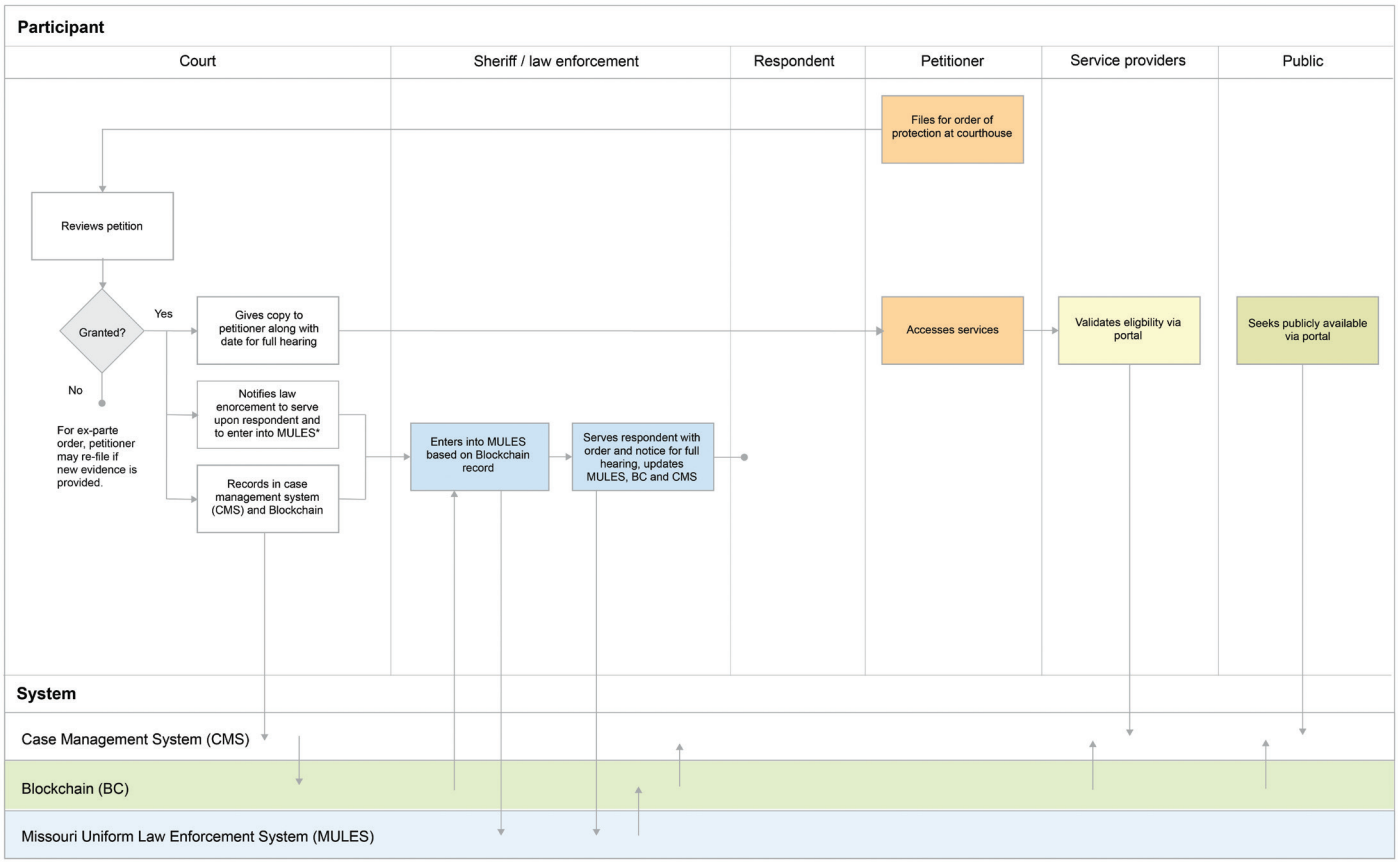
Figure 2. Blockchain Provides Certainty (Authority and Validity)

A high-level diagram showing how the process works in Missouri and how it compares with a solution using blockchain technologies.



The process for an ex parte (temporary) protective order is illustrated here.

Future Missouri Process / System



The process for an ex parte (temporary) protective order is illustrated here.

8 | Assessment Frameworks

There are different evaluation frameworks being developed to help determine whether blockchain technology will apply.

- Blockchain Applicability Decision Tree – provided in the World Economic Forum (WEF) 'Blockchain, Beyond The Hype' document.[14]
- DHS Science & Technology Directorate Flow Chart – provided in the NISTIR 8202 Blockchain Technology Overview [15]

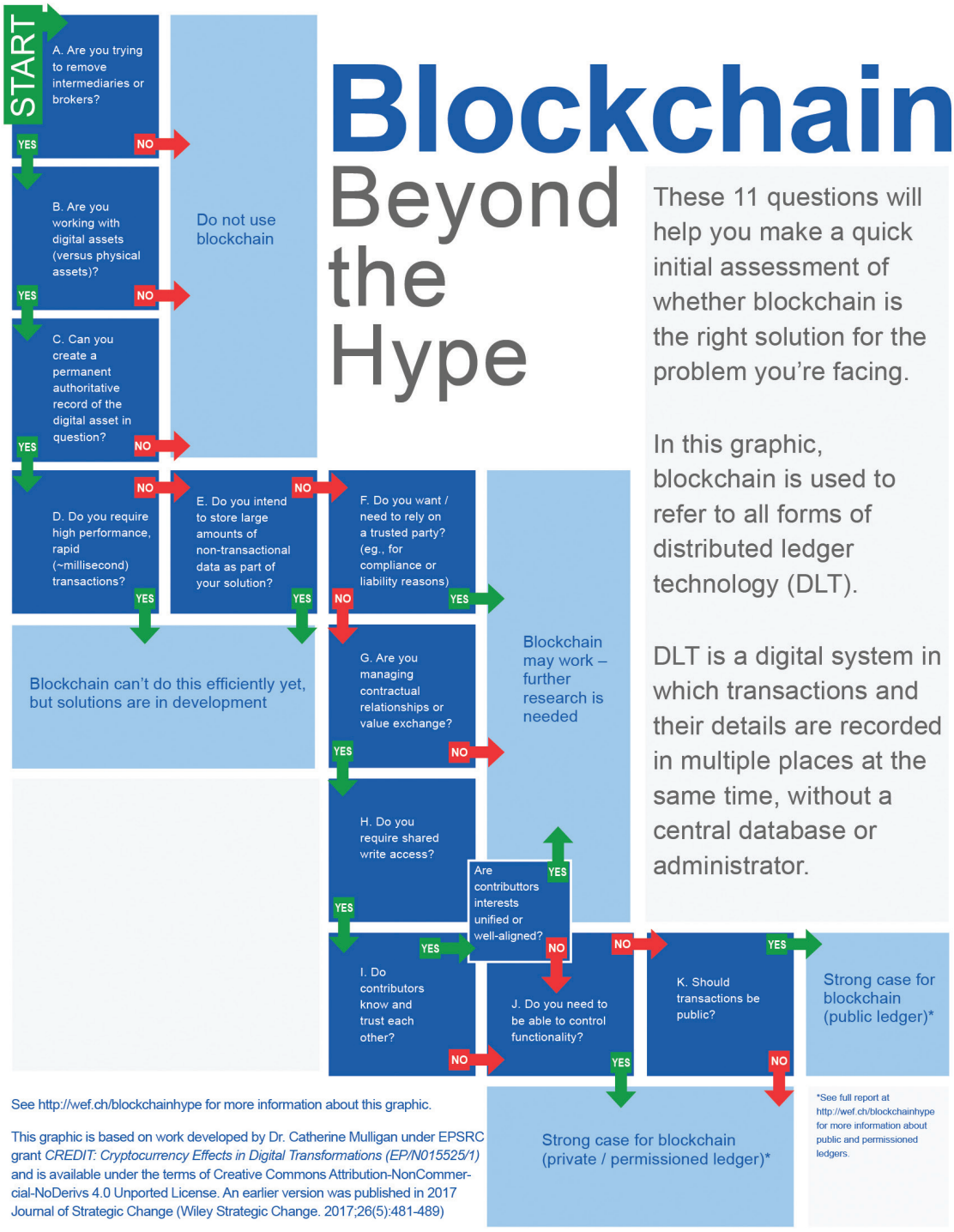
Decision trees are helpful to quickly assess whether or not blockchain technologies may apply to a use case; however, the technology is rapidly evolving so these mechanisms must be considered in that light. For example, the trustless focus of public networks is not as relevant for the justice and public safety communities and for the protective order use case (as this would use a permissioned model), though traceability, auditability, and reporting capabilities are critical. Blockchain technology enables multiple agencies to remain confident in the protective order's authority (in its source and verification of signatory) and its validity. In addition, it provides capabilities that enable more efficient and effective access by multiple independent agencies.

[14] Catherine Mulligan, Jennifer Zhu Scott, Sheila Warren, JP Rangaswami. "Blockchain Beyond the Hype: A Practical Framework for Business Leaders" World Economic Forum.
[15] Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. "Blockchain Technology Overview." October, 2018.

8.1. Blockchain Applicability Decision Tree

Figure 3. Blockchain Applicability Decision Tree[16]

This framework is applied to the Protective Order Use Case in Section 9.



[16] Catherine Mulligan, Jennifer Zhu Scott, Sheila Warren, JP Rangaswami. "Blockchain Beyond the Hype: A Practical Framework for Business Leaders" World Economic Forum. April 23, 2018.

8.2. DHS Science and Technology Directorate Flow Chart

Figure 4. DHS Science and Technology Directorate Flowchart—NISTIR 8202[17]

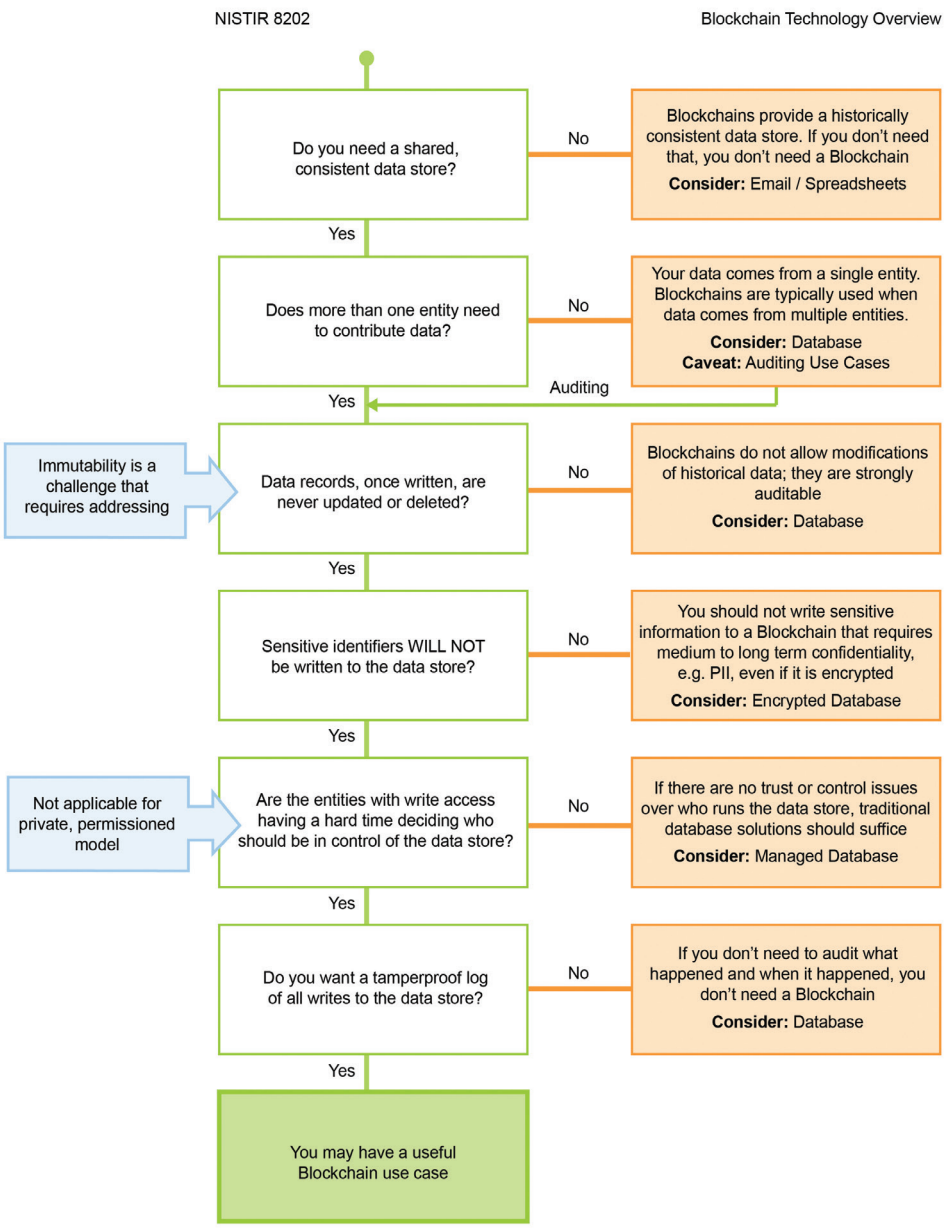


Figure 6 – DHS Science & Technology Directorate Flowchart

[17] Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. "Blockchain Technology Overview." October, 2018.

9 | Applying Frameworks to Protective Orders

The following section assesses the Missouri Protective Order use case using two frameworks:

- Blockchain Applicability Decision Tree
- Blockchain Applicability Requirements Matrix (developed by the Task Force)

It is worth noting that many of the pain points in the Missouri Protective Order use case are due to paper and / or manual processes.

The Task Force developed the Blockchain Applicability Requirements Matrix to help address the question of how a blockchain-based solution—based on a private, permissioned network—differs from a distributed database model with centralized permissions.

9.1. Blockchain Applicability Decision Tree

The Blockchain Applicability Decision Tree uses 11 questions to evaluate a use case, which are answered below for the Missouri Protective Order use case.

A. Remove Intermediaries or Brokers?

The blockchain implementation enables direct and rapid access to protective orders (POs). The following headings represent those used in Figure 3 - "Blockchain Applicability Decision Tree."

ROLE	PAPER-BASED / MANUAL PROCESS PAIN POINTS	BLOCKCHAIN BENEFITS
Issuing Judge		
Court Clerk	Single data entry point; may have to validate orders and information as requested (within court operating hours).	Provides one source for authoritative document and ability to track provenance (does not address data quality or process inefficiencies)
Petitioner(s)	Must retain order copy provided by court. Unless he or she explicitly requests notification at the court, he or she may be unsure whether the order was served. Also, a petitioner may need the order to access services.	Provides service providers with certainty as to authority and validity of order (provenance)
Respondent(s)	Must retain order copy provided by court (if full protective order from hearing). Freedom / access dependent on accurate status of petition.	Provides law enforcement with certainty as to authority and validity of order (provenance)
Attorneys for the Petitioner(s)	Need to go to court to verify process transactions and potentially add new relevant information.	Authoritative source and verifiable audit trail of transactions (updates)

ROLE	PAPER-BASED / MANUAL PROCESS PAIN POINTS	BLOCKCHAIN BENEFITS
Attorneys for the Respondent(s)	Must go to court to verify process transactions and potentially add new relevant information	Authoritative source and verifiable audit trail of transactions (updates)
Sheriff / Local Law Enforcement	Ensuring accurate and timely information from court; must return servicing information to court; constrained by court hours / access to judge	Authoritative source and verifiable audit trail of transactions (updates)
State Law Enforcement	PO might not have yet moved up and back through the system.	Authoritative source and verifiable audit trail of transactions (updates)
Federal Law Enforcement	PO might not have yet moved up and back through the system.	Authoritative source and verifiable audit trail of transactions (updates)
Victim Assistance	May have to contact several agencies to determine status of PO; constrained by court hours / access to staff	Quicker response to victims; ability to verify claims and provide services
General Public	Determining if a PO exists; determing the timing and if all PO events occurred	Single location to determine PO and events associated with PO; ability to remove / deauthorize access from documents distributed to third-parties

B. Working with Digital Assets Versus Physical Assets

The order can be a scanned PDF. The actual PDF would be not be stored on the blockchain but could be accessed via a secure reference. The blockchain computes and stores transaction records related to the PO. In Missouri, there is currently a trust factor where law enforcement want to see the actual image of the protection order to ensure its accuracy and validity. The digital assets include data and an image of the protection order referenced in the blockchain and are accessible via the reference from the appropriate repository. In addition, there are times when delivery of the document is required to gain access to other resources (e.g., housing, medical, income, etc.). If other agencies have view access to the authoritative source on the blockchain, this is another opportunity to expedite service delivery.

C. Permanent Authoritative Record of the Digital Asset

The scanned PDF is considered authoritative (full text of the protective order signed by the judge). Blockchain could assert the authority of the PO without law enforcement needing to view the digital image or, as described above, could also provide a reference to the PO, which is stored in a shared repository. Public Key Infrastructure (PKI) would need to be implemented, and training would be needed at all levels. Blockchain could be a barrier for implementation if the technology requirements are too high.

D. High Performance Requirement

No high-performance requirement exists. Protective orders can take a few minutes or even hours to access. There is typically a required timeframe for entry and for validation requests.

E. Store Large Amount of Non-transactional Data

We propose storing only some data elements on the blockchain along with a uniform resource indicator (URI) / pointer to the PDF and related documents. For example, at time of entry, a digital signature or hash of the original documents would be created and added to the block. Using this method (a unique hash representing the PO) is a way to ensure that the stored record has not been tampered with. A similar approach could be used for other off-chain documents. For example, a picture or mug shot could be also referenced in this way to assist with accurate identification. All items on the blockchain would be signed with several encrypted items. For more information on how public and private keys asserting identity could be managed, this will be addressed in the related document, "Technical Framework—Justice and Public Safety."

The blockchain becomes a repository and the authoritative source for data elements, but it does not become the repository for all information. Due to the computational resources required for distributed ledger technology (DLT), storing minimal information on the blockchain is desirable, and the document repository could contain large documents, images, and other information with the protection order and the protection order process. This removes the computational overhead to store this information on the blockchain.

F. Rely on a Trusted Party

Other than administering the Public Key Infrastructure (PKI) and cloud infrastructure, no third-party is needed. Once the court records the protective order on the blockchain, all participants can validate on demand.

G. Contractual Relationship or Value Exchange

From the network participants point of view, the contractual relationship determines who should have access to what data from participating agencies and who can create the PO, modify it, view it, etc. The value exchange may not be relevant for participating agencies, although a use case may exist for external parties requiring data access to the PO.

The contractual relationship can also be understood as the relationship between the petitioner, the respondent, and the court. The blockchain acts as a ledger that shows the sequence of events (e.g., issuance, expiration, renewal, revocation, etc.). Digital signatures would only authenticate a document. The protection order process transactions could also be included on the blockchain, including time and date for when the respondent was served, when the PO was entered into the NCIC database, etc. This informs all parties with access that the respondent (or respondents) was served and demonstrates the validity of the contract (PO).

H. Require Shared Write Access

This requires further examination as the courts require write access. Depending on what specific functions are implemented, law enforcement may require write access for certain transactions. Victim services could be included to provide eligible services more efficiently.

In a distributed ledger technology (DLT) environment, multiple access levels exist. In the protection order process, write access to the blockchain could be shared by multiple entities. Depending on the specific functions used, the figure on page 24 is one potential access chart.

ROLE	RESPONSIBILITY	ACCESS
Issuing Judge	Adjudicate	Read / write
Court Clerk	Enter information into court case management system	Read / write
Petitioner(s)	Filing the claim	View only
Respondent(s)	Named in the claim	View only
Attorneys for the Petitioner(s)	Represent the petitioner	View only
Attorneys for the Respondent(s)	Represent the respondent	View only
Sheriff	Enter PO into state repository and FBI's NCIC database; serve respondent; enforce the PO	Read / write
Local Law Enforcement	Enforce the PO	View only
State Law Enforcement	Enforce the PO	View only
Federal Law Enforcement	Enforce the PO	View only
Victim Assistance: Formal Secure, Trusted, and Confidential Organizations	Provide victim assistance	View only [relevant data about transaction on blockchain]
General Public	Media; third-party publishers; citizens	View only [permissible data]

I. Trust of Contributors

All criminal justice agencies are concerned about liability when conducting law enforcement activities. An agency could be held liable for damages if the wrong person is arrested or detained, if a person is improperly served, or if the information is outdated. Further, if action is not taken, individuals can be harmed, causing the public to lose trust in the process. While contributors generally do trust one another, their responsibility as agencies of public trust is held to a high standard. Currently, there is a lack of trust among agencies related to transferring information electronically. Law enforcement "trusts" a physical order (paper) with a judge's signature. It provides protection from liability. If the information is wrong, law enforcement can show the paper copy to reduce their liability by demonstrating without doubt that they acted on information provided by the court. In a digital-only electronic system, it may be difficult to provide an audit trail that proves the accuracy and authority of information acted upon. Blockchain technology enables them to confidently rely on the accuracy and validity of information provided electronically by efficiently tracking the process steps during the PO enforcement phase.

Blockchain technology provides liability coverage for criminal justice agencies. While it might take some time to reach the comfort level of using a paper copy, the blockchain provides a proven authoritative source for information, and it provides the chronological order of transactions. While a system log could provide transaction records, it would need to demonstrate validity if challenged. The technology needs to be proven in the court system as trustworthy by withstanding potential litigation; however, the technology increases trust levels throughout the process.

J. Control of Functionality

We recommend controlling access to functionality by using a private, permissioned blockchain, or a cloud implementation, managed by a trusted government or governmental entities.

The blockchain implementation decision depends largely on transparency with the public and the requirement for authoritative auditing and reconstruction. If the public must review or use the information, then a hybrid approach could be used (e.g., Ethereum offers a way to allow "data storage across the blockchain and private cloud with customizable privacy and scalability."[18]). The data is public, but the transactions are sanctioned by chosen or approved individuals. In this scenario, data can also be protected from public view, but more control exists over who can put transactions on the blockchain.

If the blockchain is only intended for users in the criminal justice community, a private, permissioned model can be used, where data is not publicly available. Even though the data is not available to the public in this model, there is a single distributed ledger that records the transactions, which are available to multiple criminal justice agencies with blockchain access. Additionally, those who validate the transactions would be selected and authorized; transactions would not be sanctioned by the public or even all participating blockchain members.

A permission-less blockchain would not be appropriate, as anyone could validate the transactions. This would not be acceptable in a criminal justice environment where defined roles exist regarding who can release information. Even if the information is public, a third-party cannot access or see all the data before it is made public.

K. Public Access to Transactions

For certain types of POs and jurisdictions, public access may be needed or even required by law. Access is view-only and may have different levels. For example, some of the petitioner's information may need to be hidden from the general public but not from victim assistance organizations.

Federal versus state requirements need to be considered and reconciled regarding online victim data and requirements for sealed records and expungement. This is non-trivial and an area where IJIS could provide guidance on the regulatory, legislative, and policy changes that benefit stakeholders.

[18] "5 Reasons Why Enterprise Ethereum Is so Much More Than a Distributed Ledger Technology." ConsenSys

9.2. Blockchain Applicability Requirements Matrix

The Task Force developed the table below to help guide decisions about blockchain applicability from a requirements perspective. It addresses requirements specifically focusing on authority, validity, security and access, immutability, and auditability. Blockchain is only of value when the solution requires:

- Trust among untrusted parties
- Provenance / ownership (auditability)
- Data integrity / immutability (tamper-proof)

The parties include those with a role in the process; this excludes technology and other system support roles. The relevant parties include the Issuing Judge, Court Clerk, Petitioner, Respondent, Attorney, Law Enforcement (Local, State, Federal), Victim Assistance, and the general public. The Task Force used the requirements-based comparative table to help address the how a blockchain-based solution, which is based on a private, permissioned network, differs from an on-premise or cloud-based multi-agency repository for records management data. For example, agencies could use an existing shared database model to manage the exchange of protective orders and data, using agreed standards while still maintaining separate independent repositories.

Blockchain technology does not need to be a monolithic solution. Assuming that the value proposition of authoritative, auditable, immutable, and secure records management is true, and the cost / benefit is shown to be favorable, then an incremental approach to address data interchange using blockchain technology compatible with current cloud implementations is feasible. The Technical Framework—Justice and Public Safety document[19] will cover the cost / benefit analysis and technical considerations in more detail.

User Based

REQUIREMENT	RELEVANT TO	MISSOURI CURRENT STATE	MULTI-AGENCY REPOSITORY FOR RMS DATA (CLOUD / HOSTED)	BLOCKCHAIN-ENABLED RECORDS MANAGEMENT SYSTEM (PRIVATE / PERMISSIONED)
Gain access to record	All	Authoritative source and verifiable audit trail of transactions (updates)	Application specific credentials grant access to authorized data records.	Blockchain applications (smart contracts) enforce rules for data access.
Enter record within time standards	Law enforcement	Manual process, currently policy is a 24-hour turnaround	Multiple systems exchange the electronic record using agreed upon standards.	Multiple systems interact with a common blockchain network to record relevant events related to the document. This limits the individual system-to-system data exchanges. The blockchain acts as the system of record for protective orders across record management systems.

[19] The Technical Framework—Justice and Public Safety companion document, is being developed by the IJIS Blockchain Task Force

User Based

REQUIREMENT	RELEVANT TO	MISSOURI CURRENT STATE	MULTI-AGENCY REPOSITORY FOR RMS DATA (CLOUD / HOSTED)	BLOCKCHAIN-ENABLED RECORDS MANAGEMENT SYSTEM (PRIVATE / PERMISSIONED)
Validate authority of record (signed by judge).	Law enforcement	Manual process. Sight physical document	Identity management is typically application specific or managed by third party identity providers.	For permissioned blockchains, identity management is integral to the transaction process. Public / Private Key Infrastructure (PKI) is provided by a central identity authority within the blockchain network.
Ensure validity / data integrity of record (without tampering)	All	Trust physical document with Judge's signature	Transaction and change tracking are application specific. Databases do not provide native tamper detection or prevention.	All changes to data are visible in global transactions. This provides data integrity and tamper detection.
Ensure currency of record (up-to-date)	All	Issue, although this can be due to data quality or multiple communication channels (e.g., email, paper, etc.).	Maybe Multiple records management systems may contain different document versions, and while it is possible to address via a centralized, distributed model, different organizational structures, solutions, and procedures and policies may prohibit this.	Yes The blockchain contains a single instance of transaction-level changes to the document at the current point in time and offers potential for greater accommodation of individual agencies systems, policies and procedures.
View that the record is current.	All	Based on seeing judge's signature on faxed, paper or emailed PDF copy of PO. (Updates can be communicated via email.)	Based on seeing judge's signature on copy accessed through records management system.	Seeing the judge's digital signature on the blockchain record, along with tamper prevention, ensures visibility of current record.

User Based

REQUIREMENT	RELEVANT TO	MISSOURI CURRENT STATE	MULTI-AGENCY REPOSITORY FOR RMS DATA (CLOUD / HOSTED)	BLOCKCHAIN-ENABLED RECORDS MANAGEMENT SYSTEM (PRIVATE / PERMISSIONED)
View historical record	Judge, petitioner, respondent, attorney, law enforcement	Requires manual request to NCIC staff for transaction log	Functionality specific to the records management system	All changes to the record are tracked through transactions, and viewing historical versions can be provided.
Notify participants	Judge, court clerk, petitioner	Currently, petitioner has to opt in at the court to be notified.	Functionality specific to the records management system	External transaction monitors can trigger notifications to relevant parties with respect to document of concern (alerts).
Provide services based on record	Victim assistance, petitioner	Requires petitioner to present physical order granted by court	Eliminate manual process; reduce time period by verifying qualifying status; enable evidence-based measures reinvestment and outcomes	Eliminate manual process, reduce time period by verifying qualifying status, enable evidence-based measures reinvestment and outcomes.
Update record (modify, revoke, etc.).	Judge, court clerk	Manual process; Current policy is a 24-hour turnaround.	Records updated through records management system version control functionality	Changes to documents are managed by viewing all prior transactions to the record on the blockchain. Because all document versions are visible, redaction and revocation may pose a challenge.
Audit record	Judge, court clerk, attorney, law enforcement	Requires manual request to NCIC staff for transaction log; MULES provides audit tracking capabilities.	Audit log on top of the National Data Exchange Program (N-DEx) / other cloud based records management systems (RMS)	Blockchain could track the data exchange between different systems and users (whether on premise, private cloud, third-party, N-DEx). The audit log can be external to the document transaction log or integrated with the document transaction log. In each case, access control rules in the blockchain application (via smart contracts) can enforce visibility.

System / Technical

REQUIREMENT	RELEVANT TO	MISSOURI CURRENT STATE	MULTI-AGENCY REPOSITORY FOR RMS DATA (CLOUD / HOSTED)	BLOCKCHAIN-ENABLED RECORDS MANAGEMENT SYSTEM (PRIVATE / PERMISSIONED)
Data interchange standards	IT, Policy	Policy driven, independent systems and processes; the National Information Exchange Model (NIEM) is the accepted standard. NCIC uses a minimum set based on NIEM, which agencies must negotiate. Each agency must establish Interchange Exchange Package Documentation (IEPD) to establish data exchange using NIEM. Dependency on other agencies, including courts to implement automated data exchange (e.g., Missouri implemented a new warrant system in 2018 based on an eight-year old plan and related standards. Maintaining alignment in data standards is a difficult and lengthy process with many stakeholders.	Multiple Record Management Systems support role specific interchange standards. For example, N-DEx and NCIC have inconsistent standards despite similar roles.	As a Protection Order information sharing hub, blockchain drives a greater degree of data interchange standardization.

System / Technical

REQUIREMENT	RELEVANT TO	MISSOURI CURRENT STATE	MULTI-AGENCY REPOSITORY FOR RMS DATA (CLOUD / HOSTED)	BLOCKCHAIN-ENABLED RECORDS MANAGEMENT SYSTEM (PRIVATE / PERMISSIONED)
Access Control: View, Read / Write, Share, Delete	IT, Policy		Access can be controlled by records management system permissions. Identity across multiple records management systems are rarely standardized. Federation and single sign-on mitigate this issue, which is difficult to set up and maintain.	Access can be controlled by permissions through the centralized identity provider.
Managing functional changes: application, infrastructure, network	IT		Change in application functionality is managed by a records management system vendor. Vendors have different upgrade processes and backwards compatibility.	Changes to blockchain code (smart contracts[20]) is managed through transactions. Backward compatibility is available by default as the document, and the business rules for the document are immutable. New code and rules apply to new document.
Maintaining legacy systems (integration, migration)	IT, Operations		Legacy systems are maintained (as is or with a modern veneers) or sun-set completely but not often integrated.	Existing records management systems can be integrated to a blockchain solution via a properly designed API layer.

[20] Adil Haris. "Smart Contracts—A Simple yet Comprehensive Explanation in Pictures." Hackernoon.

System / Technical

REQUIREMENT	RELEVANT TO	MISSOURI CURRENT STATE	MULTI-AGENCY REPOSITORY FOR RMS DATA (CLOUD / HOSTED)	BLOCKCHAIN-ENABLED RECORDS MANAGEMENT SYSTEM (PRIVATE / PERMISSIONED)
Establishing and managing data security (access, storage, transfer protocols)	IT		Data security protocols are established by the proprietary records management system functionality and cloud-based hosting.	Established by the blockchain code (smart contract) and immutable nature of the blockchain network
Establishing and managing performance / scale requirements	IT, Policy		Established by the records management system cloud-based hosting	Yes, can be addressed through type of consensus / network
Establishing and managing availability, reliability, and stability, including backup and disaster recovery	IT, Policy		Established by the records management system cloud-based hosting	Established by the architecture of the blockchain network
Establishing and managing storage for non-transactional data (physical and digital)	IT	Paper-based	Established by the records management system cloud-based hosting	Transactional data on blockchain; different off-chain records managed collectively or independently

10 | Governance

For the protective order use case, a private, permissioned blockchain is assumed. Governance questions for a distributed ledger technology environment, where information (and how it is exchanged and managed) is shared across multiple agencies, include[21]:

- Who owns the data?
  - Court
  - Sheriff's Office
  - Other
- Who ensures the data remains untampered?
- Who has the authority to access, change, distribute, or delete the data?
- Who creates, runs, and funds the application layer/s that validate transactions and interact with the data (e.g., smart contracts)?

Governance for Missouri

QUESTIONS	MISSOURI
Who owns the data?	The originator / issuer of the data (whether a full document or metadata) In law enforcement, they "own" any data they generate (e.g., the service data for a PO). *For example, if the DMV changes something about a driver's license, they "own" the record at that level.*
How is governance established and maintained? (includes policies and procedures around data ownership, compliance [who audits], access [create, view, update, distribute, delete], operationalization [network participants, integrators, application layers, maintenance])	Each agency manages its own data "record" and may add additional elements as needed.

The governance model must address the above questions. As the table on page 33 describes in detail, the implementation type determines the governance approach, due to technology and participants. It is important to ask what type of governance logic is in place to ensure after questions such as ownership, data integrity, access, disaster recovery, interoperability (monitoring), and auditability and reporting are addressed.[22]

For a private, permissioned blockchain, it must be determined how the organization (or technology provider) establishes and implements adequate controls.

[21] "5 Reasons Why Enterprise Ethereum Is so Much More Than a Distributed Ledger Technology." ConsensSys.
[22] "Governance in the Age of Blockchain Distributed Ledger Technology." PwC.

IMPLEMENTATION TYPE	GOVERNANCE / CONTROL RESPONSIBILITY	CONSIDERATIONS / QUESTIONS
Permission-less	Community	Who determines the controls? How are the controls implemented?
Federated	Shared among various parties	How does the consortium determine the controls? How are the controls implemented?
Private	Centralized party	How are the controls implemented?

11 | Evaluation Checklist

Assuming that your use case is suitable, ensure the following steps are addressed by the appropriate stakeholders:

1. Identify the business stakeholders
2. Identify the ideal process
3. Identify and prioritize current pain points
4. Identify solutions (technology and process) to eliminate or reduce the pain points
5. Evaluate solutions based upon
   5.1. Functionality
   5.2. Cost
   5.3. Ease of implementation
   5.4. Completeness of the solution
   5.5. Maintainability
6. Compare the cost / benefit for a blockchain solution with other solutions
7. Determine if stakeholders trust the solution and will participate
8. Determine the feasibility of implementing a blockchain solution
   8.1. Include known barriers and options to address
   8.2. Determine whether a POC is an optional first / next step
9. Determine the governance model
10. Determine funding sources and procurement options

The journey map process included in the Appendix serves as a companion to steps 1-4 above and and can serve as a useful method for achieving consensus among diverse stakeholders with competing priorities.

12 | Proof-of-Concept (POC)

Developing a POC would contribute to a generic assessment framework and reveal additional questions that must be addressed. The components for a successful POC for the PO use case include:

1. Identify and contact business stakeholders
2. Identify the protection order process and prioritize pain points with all stakeholders
3. Compare process against policy / statutory requirements (Security, FBI, State, Local)
4. Set the POC goals and evaluation criteria (how long, what is success, what is failure)
5. Obtain stakeholder buy-in and funding
6. Determine the technical solution based upon consensus from business stakeholders
7. Determine who will implement a technical solution and how technical solution will be implemented (COTS, homegrown, who builds and maintains, etc.)
8. Determine POC governance model
9. Build and implement POC
10. Evaluate and re-assess

13 | Open Issues / Questions

The following list is not comprehensive, and responses are merely suggestions. Questions unique to protective orders are indicated.

All Use Cases

1. Different legal entities / jurisdictions have vastly different rules.

    1.1. Response: This is not necessarily prohibitive; however, it requires identification and engagement of stakeholders from the justice community, and possibly, legislatures.

2. What does “expungement” mean? What is required from a “system” perspective? If all expunged records must be deleted from all storage locations, then blockchain cannot be used. Smart contracts? – Data no longer available to be viewed?

    2.1. Response: Expungement is defined differently, depending on the jurisdiction. Opportunity for a follow-up white paper on this topic from domain experts within the justice and public safety communities.

3. Each entity needs to define what happens when an order expires or another court order revokes or amends the status of the protective order before expiration.

    3.1. Response: Changes of state and triggered processes must be accommodated and future-proofed.

4. An individual may have multiple roles for specific protective orders (POs). For example, a law enforcement officer can also be a named petitioner or respondent.

    4.1. Response: Permission model needs to be flexible and accommodate changes in access at a PO-level, if necessary.

5. How should organizations proceed when there are so many unknowns (e.g., scale, speed, performance)?

    5.1. Response: Align with the overall organizational strategy. Undertake pilot projects that can be evaluated before scaling.

14 | Conclusion

An increasing demand to share information exists among agencies at the local, state, and federal levels, as does a need to comply with data privacy and security requirements in each jurisdiction.

The Task Force reviewed the current process for protective orders in Missouri and particpants' challenges. We assessed the protective order process using the Blockchain Applicability Decision Tree and the Blockchain Applicability Requirements Matrix. The Task Force also considered governance, open issues, and questions.

The Task Force concluded that the benefits of ensuring an authoritative source, an updated and valid document, and a document history audit to see who interacted with it warrant additional efforts and investigations to bring stakeholder groups together to discuss opportunities for developing a limited scope POC.

In addition to experimenting with technical feasibility, a POC would help explore optimal organizational, funding and procurement, and data governance models among participating local, state, and federal agencies.

15 | Appendix

15.1. IJIS Symposium Use Cases

Obtained from IJIS Symposium attendees in February 2018:

- Digital assets: validation of associated metadata and transactions
- Arrest warrants: issue to dissemination
- Protection orders: issue to dissemination
- Criminal history: disposition recording
- Criminal history: validation of data as part of dissemination
- Law enforcement: sharing of officer testing and certification
- Dispatch: resource sharing between agencies
- Information sharing: API for digital notarization of documents
- Law enforcement: interagency de-confliction

15.2. Key Data Elements in a Protective Order

Some key data elements of a protective order are shown below.

Note: For comprehensive data schema, this is available via the NIEM Movement Tool on the NIEM.gov site under the Justice Domain.

For the State of Missouri, the Office of the State Court Administrator is responsible for establishing and maintaining standards for data exchanges. These are typically documented in an Information Exchange Package Documentation (IEPD) and ideally include other justice partners.

For Missouri, key agencies involved in the exchange of protective order data include:

JIS: Justice Information System (Court CMS)
MULES: Missouri Uniform Law Enforcement System (LE CMS)

DATA ELEMENT	DESCRIPTION	NAME (PROPERTY TYPE) – PER NIEM
Issuing Judge	A judge or other judicial official that issued a court order	CourtOrderIssuingJudicialOfficial
Issuing Court	A court that issued a court order	CourtOrderIssuingCourt (j:CourtType) • CourtCategoryAbstract (abstract) … • CourtClerk (j:JudicialOfficialType) … • CourtDivision (TextType) • CourtFilingClerk (j:JudicialOfficialType) … • CourtName (TextType) • CourtReporter (j:JudicialOfficialType) … • CourtSupervisingAgency (nc:OrganizationType) …

DATA ELEMENT	DESCRIPTION	NAME (PROPERTY TYPE) – PER NIEM
Issuing Judge	A judge or other judicial official that issued a court order	CourtOrderIssuingJudicialOfficial
Issuing Court	A court that issued a court order	CourtOrderIssuingCourt (j:CourtType) • CourtCategoryAbstract (abstract) … • CourtClerk (j:JudicialOfficialType) … • CourtDivision (TextType) • CourtFilingClerk (j:JudicialOfficialType) … • CourtName (TextType) • CourtReporter (j:JudicialOfficialType) … • CourtSupervisingAgency (nc:OrganizationType) …
Order Time	Time that an order was issued by an authorized person	/nc:ProtectionOrder/j:ActivityResultTime
Order Date	Date that an order has been signed by an authorizing person	/nc:ProtectionOrder/j:ActivityResultDate
Issue Time	Time of day an order was issued	/nc:CourtOrderIssueTime
Issue Date	Date an order was issued	/nc:ProtectionOrder/j:CourtOrderIssuingDate
Case Number	The case number at the issuing court	CaseDocketID (niem-xs:string) CaseTrackingID (niem-xs:string) CaseNumberText (nc:TextType)
Date Issued	A date a court order was issued by a judicial official	CourtOrderIssuingDate (nc:DateType) … DocumentIssuanceDate (nc:DateType) … DocumentEffectiveDate (nc:DateType) … DocumentFiledDate (nc:DateType) …
Date Expired	The date and time the order will expire	DocumentExpirationDate (nc:DateType) …
Date Recalled	A date a court order was recalled or rescinded	CourtOrderRecallDate (nc:DateType) … CourtOrderRecallReasonText (nc:TextType) DocumentLastModifiedDate (nc:DateType) …
Order Type	A civil order, issued by a court, protecting one individual from another	ProtectionOrder (j:ProtectionOrderType) …

DATA ELEMENT	DESCRIPTION	NAME (PROPERTY TYPE) – PER NIEM
Status	While POs generally expire based on dates, they may also be rendered invalid via a subsequent court action. The Status field can be used to capture elements such as, "Active," Expired," "Revoked," "Expunged," etc.	CourtOrderStatus (nc:StatusType) • StatusAbstract (abstract) > StatusCommentText (TextType) • StatusDate (nc:DateType) > StatusDescriptionText (TextType) • StatusIssuerIdentification (nc:IdentificationType) > StatusIssuerText (TextType) DocumentStatus (nc:StatusType) … DocumentStatusDetails (nc:DocumentStatusDetailsType)
Petitioner(s)	The petitioner(s)	Petitioner (hs:PetitionerType) CaseInitiatingParty (nc:EntityType) PersonProtectionOrderPetitionerIndicator (niem-xs:boolean) True if the person is the plaintiff / petitioner / protected party of a protection order; false otherwise
Respondent(s)	The defendant(s) An entity in a court case that is required to answer a petition for a court order or writ requiring the respondent to take some action, halt an activity or obey a court's direction. In such matters the moving party (the one filing the petition) is usually called the petitioner. Thus, the respondent is equivalent to a defendant in a lawsuit. On an appeal, the party who must respond to an appeal by the losing party in the trial court (called appellant) in the appeals court. The accused in a domestic violence case or civil action; a person responding to a Request or Petition for protection filed by a petitioner.	CaseRespondentParty (nc:EntityType) PersonProtectionOrderRespondentIndicator (niem-xs:Boolean) True if the person is the subject / respondent of a protection order; false otherwise

DATA ELEMENT	DESCRIPTION	NAME (PROPERTY TYPE) – PER NIEM
Attorneys for the Petitioner(s)	The attorney for petitioner(s) and BAR number(s) An attorney in a court case representing the party who filed a petition for a court order or writ requiring the respondent to take some action, halt an activity or obey a court's direction. Representative of the party seeking action from the court	CaseInitiatingAttorney (j:CaseOfficialType) ...
Attorneys for the Respondent(s)	The attorney for respondent(s) and BAR number(s) An attorney in a court case representing the party that is required to answer a petition for a court order or writ requiring the respondent to take some action, halt an activity, or obey a court's direction.	CaseRespondentAttorney (j:CaseOfficialType)
Location of Source (Authoritative) PO	Link to signed, scanned PDF	DocumentIdentification (nc:IdentificationType) DocumentFileControlID (niem-xs:string) DocumentLocation (nc:LocationType) … DocumentLocationURI (anyURI)

15.3. A Stakeholder's Perspective

The following section includes a sample draft journey map which documents the protective order process from the petitioner's perspective. It demonstrates a useful method to achieve consensus among diverse stakeholders who have competing priorities and helps implement steps 1-4 of the Use Case Evaluation Checklist.

It enables participants to assess pain points in current processes from the perspective of all stakeholders, discover opportunities for improvements in current processes, and agree on priorities. For example, the diagrams in Figures 5a–5b show the stages a petitioner goes through when applying for a PO in Missouri[23].

The use case for blockchain applies once the order is issued by the judge (either for ex-parte or permanent protective order), and is shown in the diagram by the steps outlined in red. The petitioner relies on law enforcement to serve the protection order, although they may not have direct interaction with law enforcement.

Stages in the process (from the petitioner's perspective)

1. Relocate
    1.1. Ensure safety
2. Search / Retrieve
    2.1. Find and retrieve correct forms

[23] Jennifer Mueller. "How to Get a Restraining Order in Missouri." *wikiHow*

3. Consider
    3.1. Consider representation
4. Travel
    4.1. Arrange travel to court
5 Complete
    5.1. Complete necessary forms
6. File
    6.1. File forms with clerk
7. Appear (receive ex parte order)
    7.1. Appear before the judge and explain facts supporting petition
    7.2. Receive order
8. Confirm
    8.1. Confirm with clerk if notification of service is desired
    8.2. Confirm hearing date for permanent order
9. Prepare
    9.1. Prepare for hearing
10. Travel
    10.1. Arrange travel to court
11. Appear
    11.1. Receive permanent order

After Order is Granted

Once either the ex parte and / or permanent order is granted, it may take up to 24 hours before law enforcement enter it into the Missouri Uniform Law Enforcement System (MULES). The petitioner also has the right to be notified upon service; however, they must request this from the court. The ex parte order is a temporary order, and a full order of protection is dependent on the petitioner satisfying the requirements for evidence at a hearing.

Figure 5a: DRAFT Petitioner's Journey Steps 1–7.1

DRAFT JOURNEY MAP: Protective Order

Nelly Dean – Petitioner

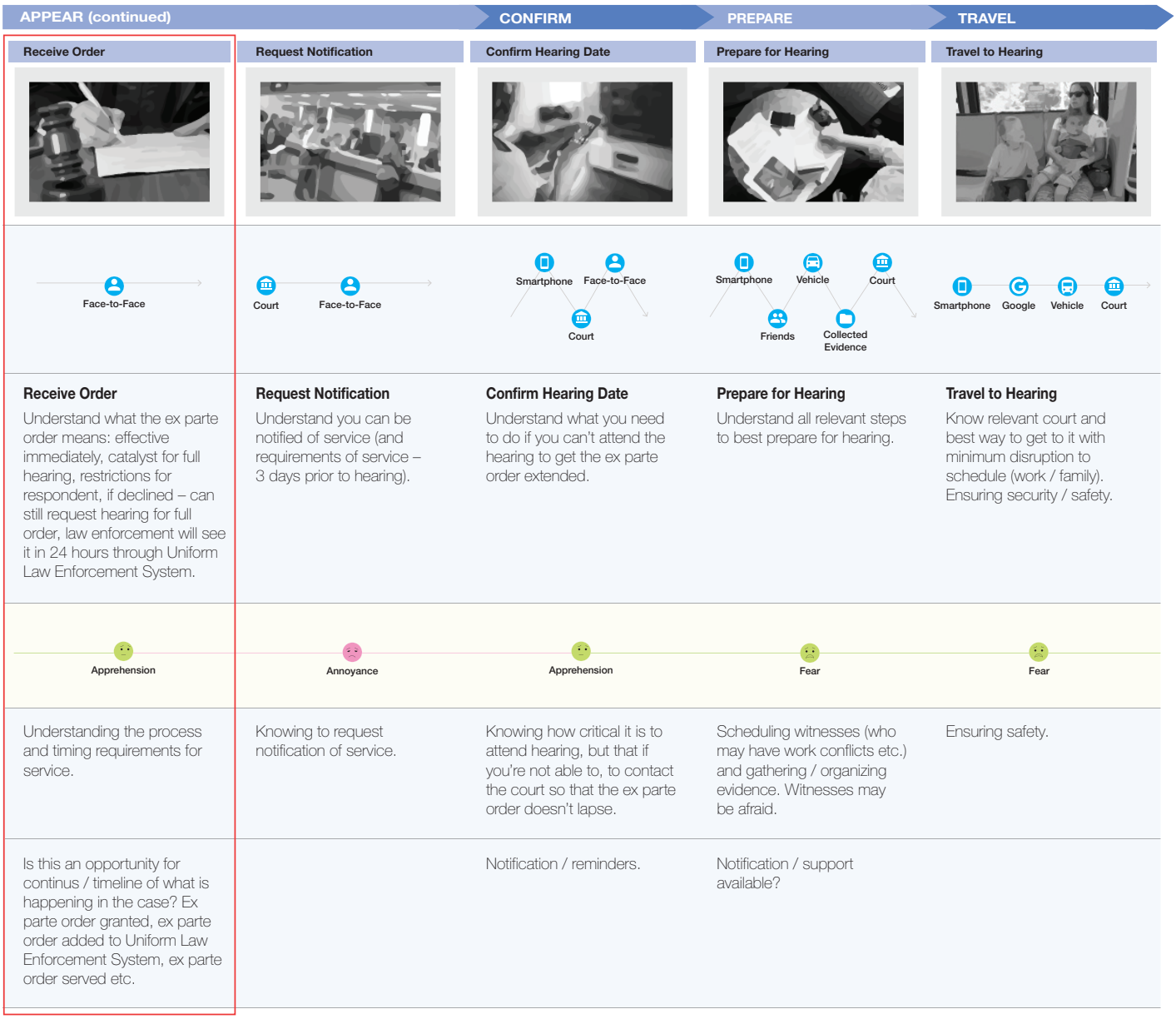
Nelly Dean is seeking an order of protection in the State of Missouri. She has four children ages three to eleven.

	RELOCATE	SEARCH / RETRIEVE	CONSIDER
Goals and expectations	**Ensure Safety** 	**Find and Retrieve Forms** 	**Consider Representation** 
Process and channels	Smartphone, Friends, Website	Smartphone, Library / Court, Printed Court Forms, Court Website, Web Form	Smartphone, Face-to-Face, Google
Actions	**Find Help** Missouri Coalition Against Domestic & Sexual Violence's service locator map: http://www.mocadsv.org/How-To-Get-Help/ National Domestic Violence Hotline: 1-800-799-7233 National Sexual Assault Hotline: 1-800-656-4673 Deaf Crisis Line Videophone: 321-800-3323 or text HAND to 839863	**Find Correct Forms** Understand eligibility: Domestic order of protection: related in some way or had a romantic relationship with the person you want the court to restrain Stalking order of protection: no familial or romantic relationship to the person you want restrained.	**Consider an Attorney** Easily know whether or not representation is needed AND, if so, how to find, afford, secure.
Emotional experience	Fear	Apprehension	Apprehension
Problems	Access and availability to resources to request an ex-parte order. Lack of knowledge about the process.	Ability to access technology to download and print forms. Knowing what forms you need (plain English).	Knowledge and understanding of the avenues for legal aid and assistance in representation.
Ideas / Opportunities	Understanding process (what constitutes cause. Information / evidence requirements for the whole lifecycle). Understanding at this time that these agencies may be able to offer legal services.	End-to-end understanding that this is about providing date / time / evidence. What information should be kept / stored. Easily accessible.	Opportunity at the beginning to obtain representation and understanding of how this works, what the costs are etc.

continued

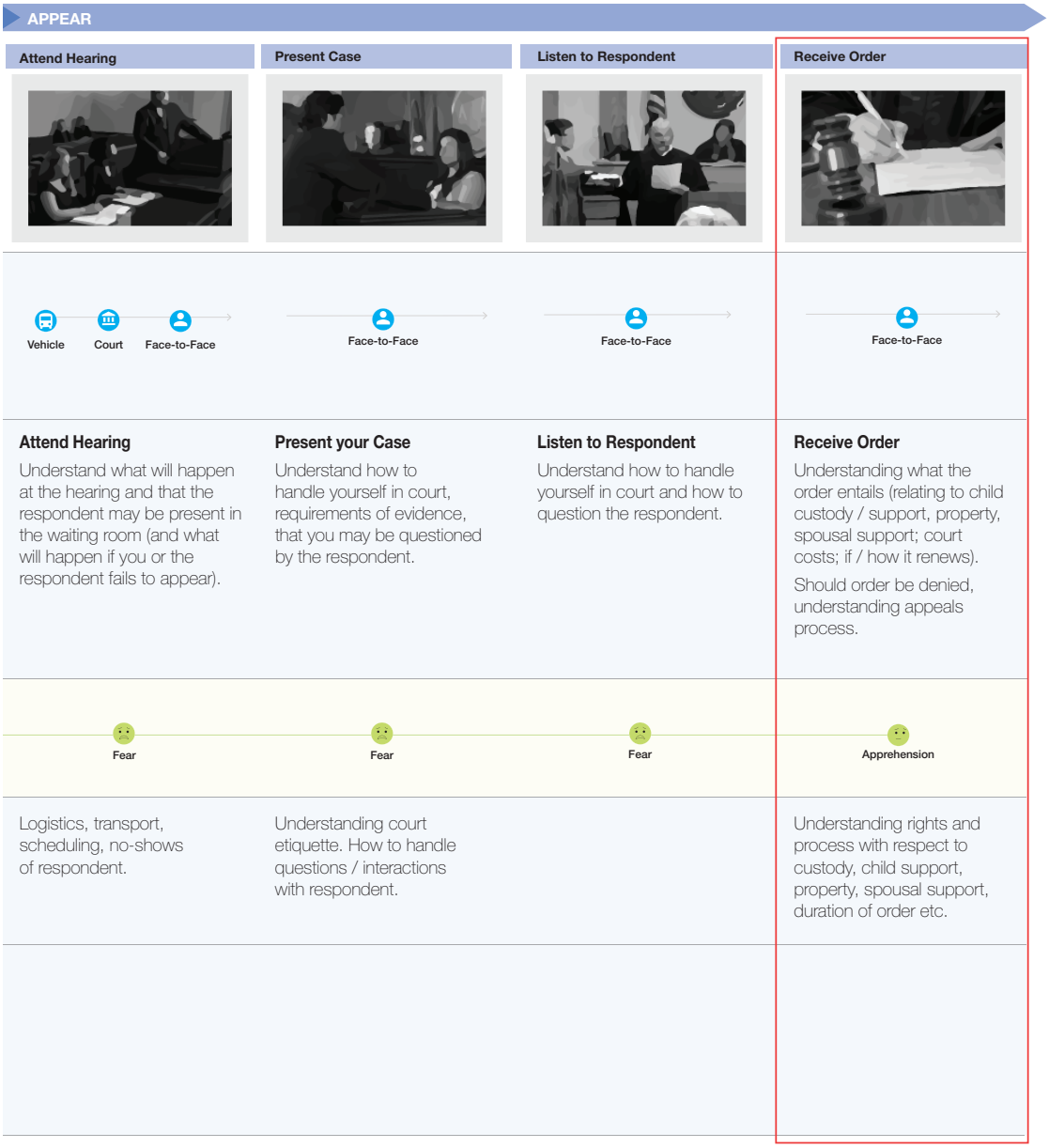
Figure 5a: DRAFT Petitioner's Journey Steps 1–7.1 (continued)

Figure 5b: DRAFT Petitioner's Journey Steps 7.2–11



continued

Figure 5b: DRAFT Petitioner's Journey Steps 7.2–11 (continued)



15.4. References

"11 Ways Ethereum Can Benefit Enterprise." ConsenSys. October 18, 2018. ConsenSys. Retrieved from: https://media.consensys.net/11-ways-ethereum-can-benefit-enterprise-aac6d798a9fb Web. April 26, 2019.

"5 Reasons Why Enterprise Ethereum Is so Much More Than a Distributed Ledger Technology." ConsensSys. December 12, 2018. Retrieved from: https://media.consensys.net/5-reasons-why-enterprise-ethereum-is-so-much-more-than-a-distributed-ledger-technology-c9a89db82cb5 Web. April 26, 2019.

"Blockchain Use Cases and Applications by Industry." ConsenSys. November 14, 2018. ConsenSys. Retrieved from: https://media.consensys.net/enterprise-ethereum-blockchain-use-cases-and-applications-by-industry-3914d1210049 Web. April 26, 2019.

"Busting the Myth of Private Blockchains." ConsenSys. January 3, 2019. Retrieved from: https://media.consensys.net/busting-the-myth-of-private-blockchains-9ae0ed058b0d Web. April 26, 2019.

"Justice Information Exchange Model (JIEM)". Search. Retrieved from: https://www.search.org/solutions/information-sharing-standards-and-models/jiem/ Web. July 5, 2019.

Brooks, Patrick. "Making Good on the Promise of NIEM: Building an IEPD from the Ground Up." NCSC. Retrieved from: https://ncsc.contentdm.oclc.org/digital/ Web. July 5, 2019.

Curran, Chris, Galindo, George, Smith, A. Michael, Khan, Emad, Latch, Charlie. "Governance in the Age of Blockchain Distributed Ledger Technology." 2018. PwC. Retrieved from: https://www.pwc.com/us/en/about-us/new-ventures/assets/pwc-governance-in-the-age-of-blockchain-distributed-ledger-technology.pdf Web. April 27, 2019.

del Castillo, Michael. "Blockchain Goes To Work". April 16, 2019. Forbes. Retrieved from: https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-goes-to-work/#796773e92a40 Web. April 16, 2019

Greenspan, Gideon. "Four genuine blockchain use cases." May 10, 2016. MultiChain. Retrieved from: https://www.multichain.com/blog/2016/05/four-genuine-blockchain-use-cases/ Web. April 26, 2019.

Haris, Adil. "Smart Contracts—A Simple yet Comprehensive Explanation in Pictures." March 22, 2019. Hackernoon. Retrieved from: https://hackernoon.com/smart-contracts-a-simple-yet-comprehensive-explanation-in-pictures-bc-21c7ab89b6 Web. Oct 20, 2019.

Mulligan, Catherine, Zhu Scott, Jennifer, Warren, Sheila, Rangaswami, JP. "Blockchain Beyond the Hype: A Practical Framework for Business Leaders." World Economic Forum. April, 2018. Retrieved from: http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf Web. July 16, 2019.

Mueller, Jennifer. "How to Get a Restraining Order in Missouri." March 29, 2019. Retrieved from: https://www.wikihow.com/Get-a-Restraining-Order-in-Missouri Web. April 28, 2019.

Mulligan, C, Rangaswami, J.P, Warren, S, and Scott, J. Z. "Blockchain Beyond the Hype." World Economic Forum. April 23, 2018. Retrieved from: https://www.weforum.org/whitepapers/blockchain-beyond-the-hype. Web. September 5, 2018.

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

"OVW Grants and Programs; Formula Grant Programs." US Department of Justice. Retrieved from: https://www.justice.gov/ovw/grant-programs Web. July 5, 2019.

"Protection Order Artifacts". National Center for State Courts. Retrieved from: https://www.ncsc.org/Services-and-Experts/Technology-tools/National-standards/IEPDs.aspx#PO Web. July 5, 2019.

Protection Order Information Exchange Package Document (IEPD). Missouri Office of the State Court Administrator. Retrieved from: http://www.courts.mo.gov/exchanges/download/attachments/3866814/Protection+Order+Master+Document.doc Web. July 11, 2019.

"Procedure for Obtaining an Order of Protection", p 46, Domestic Violence and the Law: A Practical Guide for Survivors, 2019. Missouri Coalition Against Domestic and Sexual Violence. Retrieved from: https://www.mocadsv.org/resources/ Web. Feb 4, 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.

Stinchombe, Kai. "Blockchain is not only crappy technology but a bad vision for the future." April 5, 2018. Medium. Retrieved from: https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-c1ca122efdec Web. April 28, 2019.

Yaga, Dylan, Mell, Peter, Roby, Nik, Scarfone, Karen. "Blockchain Technology Overview." October, 2018. National Institute of Standards and Technology. Retrieved from: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf Web. July 16, 2019.