Intellectual Property Rights Blockchain Proof of Concept: Overview & Results

U.S. Customs and Border Protection (CBP) has taken a valuable step forward with its newest blockchain proof of concept (POC) – a program to evaluate the viability of a new technology – by enhancing the ability for CBP and the trade community to rapidly and cost-effectively enforce Intellectual Property Rights (IPR) rules. Aiming to enhance the process of exchanging data with IPR holders and other trade partners during the IPR examination and seizure process, the POC successfully:

- Demonstrated increased efficiency in the evaluation of imported products based on licensed Intellectual Property (IP)
- Showcased emerging global standards in blockchain technology, identity verification, and entity relationship security
- Facilitated real-time messaging between CBP and trade participants
- Enabled users to perform blockchain to blockchain communications without the use of standard Application Program Interfaces (API), an entirely new blockchain capability.

Additional benefits from the POC include:

- Data-level interoperability across multiple blockchains
- Cross blockchain interoperability by the use of blockchain links
- Standards-based method for trade participants to register product features

“Having completed two blockchain proofs of concept, CBP and DHS S&T have made great strides in understanding the technical and business value of blockchain. It has been a great experience working with the trade and engineering new ways to make processes more efficient. Leading the way both domestically and abroad, CBP will continue to work with DHS to bring value to our customer base in ways that will increase safety and facilitation.

Overall the POC went extraordinarily well, as the agency increased complexity for this burgeoning technology. Having the added benefits of new data elements, running a consumer test through mobile technology informing them of the legitimacy of a registered project and expediting imports for the trade, CBP found success and value. The Business Transformation and Innovation Division (BTID) recommends moving forward with maturing these tests as we take on the mission of re-engineering the supply chain in a 21st century world.”

Vincent Annunziato - Director, Business Transformation and Innovation Division, CBP
POC Evaluation Highlights

The IPR POC live fire test included participants from both CBP and the trade community. Upon completion of the test, each participant provided an evaluation of the POC. These evaluations produced beneficial information, including both the quotations displayed below and the quantitative summary presented on the following page.

Operational

**Strengths**
- “Storage of all documentation and information in one place, which improves efficiency in reviewing the information.”
- “Decreased time needed to review possible IPR violations.”
- “Reduced time required to access and analyze all relevant information.”

**Concerns**
- “Implementation and documentation synchronization.”
- “Broadly defined operational boundaries of the entities involved in POC.”

Legal

**Strengths**
- “Blockchain technology use to enhance CBP’s enforcement posture.”
- “The sharing of Personally Identifying Information (PII) through ACE in the public blockchain.”

**Concerns**
- “Unclear time requirement to initiate new rules and regulations.”
- “Indemnification of blockchain application users from liability caused by security breaches.”

Trade

**Strengths**
- “Reduced cost related to holds, detentions and seizures.”
- “Reduced paperwork and labor.”

**Concerns**
- “Unclear time requirement to initiate new rules and regulations.”
- “Broadly defined operational boundaries of the entities involved in POC.”
Viability of adopting IPR POC into business processes: 4.1/5

Strategic alignment of adopting IPR POC into business processes: 4.0/5

Overall experience and satisfaction with this POC: 4.5/5

Likelihood to recommend CBP invest more into blockchain: 4.9/5

User experience of the portal used in this POC: 4.2/5

Extent to which POC improved available data elements: 4.2/5

Likelihood of legal team allowing blockchain use for external data transfer: 4.1/5

Blockchain technology's potential to relieve need for a physical signature: 4.1/5

Ease of integrating blockchain into existing architecture: 4.1/5

Blockchain technology as a worthwhile future investment: 4.5/5
Customs and Border Protection

Intellectual Property Rights Blockchain

Final Report

Using Blockchain technology to enhance U.S. Customs and Border Protection processes related to intellectual property licensing.
1. **Digital Bazaar - Executive Summary**

1.1. **Objectives**

The Intellectual Property Rights Blockchain Proof of Concept (PoC) sought to enhance the process of registering and verifying intellectual property assertions related to products being imported into the United States of America. These registrations include product information such as the licensor and licensees, physical features, and information related to who is authorized to manufacture and import the product. The ultimate objective was to increase the ability for CBP Officers, retailers, and end consumers to rapidly and cost effectively determine whether or not a particular product is being legally imported to the country.

A second major objective of PoC was to demonstrate the value of using global open standards and other emerging standards to strongly identify different organizations such as licensees and licensors, record relationships between organizations in the supply chain, broadcast trusted and discoverable public data onto a shared distributed ledger, and provide fine grained access to tamper-evident private data stored on trade partner's servers.

1.1.1. **Specific Goals**

There were a number of specific goals that were identified as central to the PoC:

1. Track product licensing and other intellectual property information, including supporting documents and other related data in a digital, tamperproof, and auditable manner.
2. Enable CBP and the Trade Community to store trade sensitive data and supporting documentation on their own systems while providing auditable proof of existence and limited access to CBP and relevant Trade Partners.
3. Provide a system predicated upon blockchain principles to test the veracity of digitizing and tracking licensing information in the supply chain.
4. Ensure accuracy of licensing data by clearly identifying and authorizing licensors, manufacturers, and importers.
5. Enable CBP and authorized Trade Partners to determine if an organization has a license, or sublicense, to manufacture a particular product and if an Importer is authorized to import said product.
6. Enable CBP Officers to view a digital file that specifies the proper construction, logos, stitching, or other relevant markings to determine if the product is a legitimate good.
7. Enable retailers and end consumers to determine if a product that they are planning to purchase has been properly licensed for manufacture and legally imported.
8. To the greatest extent feasible, use existing open standards or pre-standards technologies and specifications to develop the Proof of Concept.
9. Reduce operational costs and targeting efficiency by achieving the goals above.
1.2. **Benefits**

1.2.1. **Global Open Standards**

The use of emerging standards in Blockchain, Verifiable Credentials, Authorization Capabilities, Encrypted Data Vaults, Decentralized Identifiers, and other emerging global standards ensures the resulting architecture is resistant to vendor lock-in, enabling any organization to access and use the eventual system without undue fees, royalties, or other licensing requirements.

1.2.2. **Strong Identification**

Moving beyond usernames and passwords, the W3C Verifiable Credentials standard and the emerging Decentralized Identifier standard combine to form a non-proprietary mechanism that strongly identifies organizations and individuals. It uses cryptographic mechanisms to verify authorship and authenticity of identity attestations from known or knowable entities. Whether relying on the identity proofing performed by CBP or the independent authority of a license owner, the cryptographically anchored identification demonstrated in the PoC increases the level of assurance that organizations in the supply chain are who they say they are and that what they say is a legitimate statement by that organization. In other words, strong identification dramatically improves the reliability of licensing claims within the PoC.

1.2.3. **Entity Relationship Recordation**

By recording the relationships between supply chain participants in a manner that protects trade secrets and other proprietary corporate information, the PoC dramatically reduced the processing time required to appropriately vet products entering into the country, without compromising strategic details about company operations. The data available in the system allows CBP Officers to inspect the chain of licensing and authorizations for Intellectual Property Rights from the Importer all the way back to Rights Holder, without exposing that information to the public or companies uninvolved in the licensing or manufacturing of a given product. Further, because this data was recorded and maintained digitally, the PoC was able to analyse the recorded chain of authority, flagging likely issues for greater attention by CBP officers. This enabled heightened scrutiny by trained officers without the false negatives that might slow down the processing of imports because of incorrect or incomplete data.

1.2.4. **Trusted and Discoverable Blockchain Data**

Blockchain Data, for use by CBP and all trusted Trade Partners, is easily accessible through a fit-for-purpose blockchain. The blockchain allows guarantees that the data recorded on the ledger was added by a trusted participant, and was done so in a verifiable way. The nature of the ledger also allows different organizations to independently build solutions to solve problems using the same high fidelity data.
1.2.5. Fine-Grained Access on Tamper-Evident Private Data

Private Data, stored by the source and only accessible to authorized parties, allows organizations to selectively publish sensitive trade secrets or private information on a record-by-record basis. Combined with verifiable links from Public Data, recipients of the private data can independently verify that the data retrieved hasn’t changed since the link was recorded. This approach avoids the need for a single data store to which all parties submit sensitive information, accumulating details of billions or trillions of US dollars of imported goods in a centralized honey pot. It does so without compromise of fidelity and accountability. It is possible to verify both the integrity of the data and the date it was published.

1.3. Use Cases

We structured the PoC to address the most relevant use cases for the import of goods using licensed intellectual property. The initial focal use cases centered on the primary flow from a rights holder through manufacturing, import, and entry, including sublicensing and a stretch goal of authorizing another party to make a filing on behalf of a legitimate importer.

1.3.1. Focal Use Cases

Consider two scenarios. Note: All trademarked and corporate names are used as examples and do not represent participation in or approval of the PoC by the rights holding organization.

- Two-party scenario: Fitnaid licenses the right to use Happy Hare on a t-shirt to a self-filing importer named Fanciful Tees. In this scenario, Fitnaid is the rights holder (and acts as the licensor). Fanciful Tees is the licensee, who is also the importer and filer.

- Multi-party scenario: Fitnaid licenses the rights to PedalBikes China to manufacture Happy Hare bicycles, which are then sold to BigRetailer and shipped via FastShipper which is acting as BigRetailer’s customs broker. In this scenario, Fitnaid is the rightsholder and licensor. PedalBikes China is the licensee. BigRetailer is the importer. And FastShipper is the Filer.
1.3.2. Participant and Public Use Cases
The PoC also began with an administrative use case that all participants would need, provisioning a profile within the system, and two use cases available to the general public: the ability to verify an importer as legitimately licensed source for a particular good and the ability for an end-consumer to verify if a good they are about to purchase is, in fact, legitimate.

As the PoC progressed, the Verify Importer feature was dropped due to a lack of demand by Trade, a lack of consensus about the desired inputs and outputs of such a service, and concerns over inappropriate exposure of proprietary corporate information.

1.3.3. Discovered Use Cases
During the course of the PoC, Digital Bazaar worked with Trade participants to understand how best to address the use cases outside the simple scenarios described in 1.3.1. The discussion led to a stretch goal for a generalized Authorization framework that would enable CBP to trace the provenance of any given import through the supply chain back to the original license. This traceability applied to both formal sublicensees as well as parties authorized by licensees or sublicensees to perform a step in the process. This stretch goal is described in more details in 1.3.4.2

1.3.4. Stretch Goals
There were four discovered use cases that later became stretch goals for the PoC. The stretch goals are listed in priority order based on Trade partner consensus. All stretch goals were implemented except for the stretch goal, Retailer Portal (1.3.4.4), due to lack of support from the group.
1.3.4.1. Blockchain-to-Blockchain Linking
Currently, the blockchain space is filled with a variety of non-standardized technologies. This stretch goal provides interoperability via the use of blockchain links between different types of blockchains. Ultimately, one would be able to refer to data on two completely separate blockchain networks and access that data. This blockchain link, also known as a "blink", is similar to an HTTP URL in that it allows one to use an identifier to refer to and retrieve a specific set of data. This goal was completed by adding a blink to Entry Data placed on the CBP IPR Blockchain built on top of Veres Delta that referenced bill of lading information on an Ethereum blockchain network.

1.3.4.2. Authorization
During the course of the PoC, a use case surfaced where parties who are authorized to act on behalf of a licensee were not identified in the license. For example, GreatMugs, LLC, a fictional licensee of XYZ Industries’ PhotonCup brand would be able to authorize MugMakers, Inc., a fictional manufacturer located in Mexico, to manufacture the mugs and deliver them to GreatMugs’ facility in El Paso. This authorization does not sublicense GreatMug’s license, it merely authorizes them to fulfill the order on Great Mugs’ behalf. This authorization does not require XYZ Industries’ permission or approval, as GreatMugs already has a license to have the mugs manufactured with the PhotonCup trademark. In addition, MugMakers desires to authorize Customs Brokering--an import logistics specialist--to handle the logistics of actually delivering the mugs to the facility, including shipping, warehousing, and import (making entry into the US). This stretch goal enabled trackable, flexible authorization throughout the PoC’s workflow, enabling any licensee to authorize other parties to help them fulfill their contractual obligations without transferring or sublicensing the license from the original Rights Holder.

Although MugMakers is not a licensee, they can authorize Customs Brokering such that when the products come into CBP for a determination, CBP can trace the authorization back to the original license and confirm that this particular shipment is based on a legitimate license from a Rights Holder who has recorded their trademark for protection by CBP. The end result is that CBP can avoid unnecessarily delay that occurs when importers are required to gather further documentation, like Purchase Orders, for evaluation by CBP to complete determination.

1.3.4.3. Consumer Portal
This stretch goal provided a public-facing web page where a consumer, at the point of making a purchase, can scan in a product code and get information about whether or not that specific product is a legitimate, licensed good. A serialized Global Trade Identification Number (GTIN) was used to uniquely identify individual products with an automated legitimate goods checking service. Consumers would scan a QR code and either receive positive confirmation (along with information like a product image and country of origin) or an indeterminate result stating that no record is found.
One complication is that CBP, as a federal agency, should not be making a statement related to the legitimacy of the good but rather forwarding what the company that produced the good is stating about the provided serialized GTIN. Nevertheless, the ability to enable consumers to verify legitimate goods--whether at a department store or at a flea market--would go a long way to support law enforcement goals.

1.3.4.4. Retailer Portal

This stretch goal would have provided retailers with a web page where they can lookup valid importers for a product or check if a given importer has authorization for a given product. This stretch goal was not implemented due to fundamental concerns regarding the protection of trade secret information related to corporate supply chains.

In one version, the portal operated like an Authorized Goods Yellow Pages (search based on product rather than business name). This would be a useful resource--especially for smaller businesses--who want the assurance that they are receiving legitimate products from their suppliers. The identified challenge was that the portal would also expose licensing information that Trade may prefer to keep confidential.

In another version, the website would look like an Authorized Goods Business White Pages (search based on business name rather than product). This could streamline the checks that a retailer already makes to verify legitimate sources for product. Discussions with Trade revealed that often, during sourcing, the conversation starts before the supplier or manufacturer has a particular license to the desired product. The negotiations proceed while the source secures the proper license. Once terms are decided and a legitimate right to produce the good is demonstrated, a Purchase Order given. In this scenario, the source would not appear in the directory because the license is obtained after negotiations begin, which would significantly limit the value of the service.

Due to these complexities, and based on only modest interest from Trade, Digital Bazaar proposed to drop this stretch goal.

1.4. Illustrative Use Case

Throughout the test plan for the PoC, we used an illustrative example using actual products and participants from the Proof of Concept. The names and participants have been replaced with fictional names to ensure that this report can be released to the general public.

For the primary work flow, XYZ Industries is a Rights Holder, owner of the PhotonCup trademark. These mugs are licensed for import by Customs Brokering, who will file the Entries on behalf of XYZ Industries.

For the stretch goal with authorizations, XYZ Industries is a Rights Holder, owner of the PhotonCup trademark. These mugs are licensed to MugMakers, Inc. (a fictional company) for manufacture in Mexico and imported by XYZ Industries for sale in the United States. XYZ Industries works with Customs Brokering, who will file the Entries on behalf of XYZ Industries.
Note that while a pilot system would enable Customs Brokering to act more broadly on behalf of XYZ Industries, in the Proof of Concept, only the filing of the entry is delegated as part of the authorization stretch goal. While creating any trademarks, products, and licenses, Customs Brokering will be acting directly as if they were XYZ Industries, simulating their role in the system. When filing an entry, Customs Brokering will act as itself, authorized to file an entry on behalf of XYZ Industries. All of this work will be done on the Customs Brokering instance of the Trade Partner Website.

1.4.1. Step 1 Profiles
Create profiles for XYZ Industries as a Rights Holder, Customs Brokering as a Filer, and MugMaker as Licensee.

1.4.2. Step 2 Trademarks
Using the XYZ Industries profile, create the PhotonCup trademark, USPTO# 8493728 for “Coffee cups, tea cups and mugs”.

1.4.3. Step 3 Products
Create a single product based on the PhotonCup trademark. We created LMGSET1 - 8 oz Square Ceramic PhotonCup Blank Sample Set.

1.4.4. Step 4 Licenses
Create a license authorizing MugMakers, Inc. to produce 500 units of the LMGSET1 - 8 oz Square Ceramic PhotonCup Blank Sample product.

1.4.5. Step 5 Entry
Customs Brokering files an entry, specifying XYZ Industries as the importer of record, for a batch of 100 units of the LMGSET1 - 8 oz Square Ceramic PhotonCup Blank Sample product.

2. Digital Bazaar - Findings

2.1. General
The PoC successfully demonstrated increased efficiency and efficacy in the evaluation of imported products based on licensed intellectual property. In addition, it demonstrated the value of emerging standards in Blockchain, Verifiable Credentials, Authorization Capabilities, Encrypted Data Vaults, Decentralized Identifiers and other emerging global open standards. The PoC also helped improve the specifications of those standards through a better understanding of potential tradeoffs and choices made during the project.
2.2. **Goal Fulfilment**

During the PoC, the goals (1.1.1) were fulfilled in the following ways:

1. Public, non-trade sensitive, licensing data and hyperlinks to supporting documents that reside on an external storage server can be written to the blockchain. (addresses goals 1, 2, 3, 5)
2. Hyperlinks in the blockchain can be dereferenced by CBP or authorized Trade Partners, via a common protocol, to retrieve supporting documents from an external storage server. (addresses goal 1, 2)
3. The existence and integrity of supporting documents retrieved from an external evidence system can be verified against blockchain records with a positive or negative result. (addresses goal 1, 2, 3, 4, 5, 6, 7)
4. Multiple parties in the supply chain, including licensors, manufacturers, and importers, are clearly identified in the information anchored to the blockchain. Unauthorized parties are not able to write to the blockchain. (addresses goals 1, 4)
5. A separately administered blockchain node can join the blockchain, read all of its data, and write new data to it. (addresses goals 1, 3, 4)
6. A CBP Officer can use a software application to perform a side-by-side comparison of a product being analyzed and it’s expected markings to determine whether or not it is a legitimate import. (address goal 6)
7. A retailer or end consumer can use a software application to look up whether or not a product has been legitimately licensed, manufactured, and imported. (address goal 7)
8. As much as reasonably feasible, open specifications covering non-market vertical specific data formats and protocols are available under a license that is patent-free, royalty-free, non-discriminatory, and available to all worldwide. (addresses goal 8 and 9)

The group was able to achieve 7 separate software system integrations, 10 hours of live testing, and a 100% live testing success rate for both required goals and stretch goals.

2.3. **Key Phases and Outcomes**

We break the key outcomes into two sections focused on Development and Testing.
2.3.1. Development

Development started in April 2019 with the creation of an Engineering Plan. The majority of software development proceeded from May through mid-July 2019. Trade Partner integration proceeded from mid-July to the end of August 2019, ending with Testing in September 2019. A visual summary of the timeline is shown below:

<table>
<thead>
<tr>
<th>Design</th>
<th>Development</th>
<th>Integration</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2019</td>
<td>May - July 2019</td>
<td>August 2019</td>
<td>September 2019</td>
</tr>
</tbody>
</table>

2.3.2. Testing Summary

The testing process was organized into two phases. Both phases tested the illustrative use case in 1.4. The first phase was the Dry Run tests that occurred during the last two weeks of August 2019. The second phase was live fire testing that occurred over the month of September 2019. Overall, just over 10 hours of live testing was performed over the course of five weeks with 7 organizations. Three organizations created custom interfaces for submitting information to their Trade Server. One organization used Ethereum and another used Hyperledger Fabric as a part of their integrations. Every Trade Partner used the Trade Server software provided by Digital Bazaar to interact with other PoC Blockchain Nodes. There was a 100% success rate for all live tests including both the required goals and stretch goals. The following table summarizes the outcomes during testing.

<table>
<thead>
<tr>
<th>Dry Run Test</th>
<th>Trade Partner 1</th>
<th>Trade Partner 2</th>
<th>Trade Partner 3</th>
<th>Trade Partner 4</th>
<th>Trade Partner 5</th>
<th>Trade Partner 6</th>
<th>Trade Partner 7</th>
<th>Test Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-08-01 (Dry Run Test)</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
</tr>
<tr>
<td>Live Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019-08-29 (Live Test 1)</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
</tr>
</tbody>
</table>

There were a few usability issues uncovered during the Proof of Concept. Trade partners integrating with the API would have liked to see the ability to make batch requests for a more optimized interaction. A number of CBP Personnel expressed interest in a more powerful search feature to find Entries during test. The same group had high praise for the unified Entry display that provided a single place to work on processing Entries. The development of a dropdown as a mechanism to drilldown for more information was successful overall but could be improved on. Participants raised the issue that on first use it was not intuitive to figure out where to click.
2.3.3. Use of Standards During Testing

One of the primary goals of the PoC was testing whether the use of global standards or pre-standards specifications resulted in interoperability between disparate systems running across a variety of independent organizations. This section outlines the specifications that were used, their current status, and what each specification was used to accomplish during the PoC.

It is important to highlight that these specifications are currently going through various standardization processes and are being shaped by some of the participants in the PoC. Direct funding for these standards and organizations remains anaemic, slowing their progress, and endangering the completion of the work on a reasonable time frame. DHS/S&T, DHS/SVIP, and DHS/CBP have been the primary agencies driving funding toward these efforts. Other government agencies and private industry are urged to make investments in order to ensure that systems such as the one described in this report are capable of being built using open standards in a way that enables a competitive vendor landscape.

2.3.3.1. Decentralized Identifiers (aka: DIDs)


A DID is like a driver's license number or social security number. It is an identifier. Unlike more traditional identifiers, like SSNs or DUNS Numbers, an organization can perform cryptographic authentication using DIDs. That is, the organization can mathematically prove that the number is theirs via digital signatures.

DIDs were used during the PoC to:
- Express public keys used to digitally sign Trademarks, Products, Licenses, Authorizations, and Entries so that CBP knew who submitted the data element and that the data element had not been tampered with after submission.
- Express public keys used to digitally sign Entry Statuses, so that Trade Partners knew that the Entry Status was coming from authorized CBP Personnel and had not been tampered with in transit.
- The did:key method was used as a simple DID Method when accessing the WebKMS systems employed during the PoC.

2.3.3.2. Verifiable Credentials (aka: VCs)

A Verifiable Credential is like a driver’s license or social security card (credentials one carries around in their wallet). They are typically issued by an authority such as the DMV or Social Security Administration. Unlike more traditional credentials, Verifiable Credentials are digitally signed and are thus highly resistant to forgery, even when sent over the Internet. The expectation is that eventually CBP or the state corporation commission will issue Verifiable Credentials to businesses which can then be used in digital supply chain ecosystems such as the PoC.

Verifiable Credentials were used during the PoC to:

- Identify the Rights Holder, Licensee, Filer, Importer, Manufacturer, Retailer, and CBP. We captured company name, logo, phone, address, LEI Code, GLN, and Entry Filer Code for the PoC.

2.3.3.3. Authorization Capabilities (aka: ZCAPs)

Standardization Status: Experimental pre-standards specification, currently incubating in W3C Credentials Community Group.

An Authorization Capability is like a key to a Post Office box. The owner of the post office box can hand the key to an individual or corporation to access the post office box at their leisure. The holder of the key may also delegate opening and closing the post office box to someone else they trust.

Authorization Capabilities were used during the PoC to:

- Enable Trade Partners to manage access to Encrypted Data Vaults on their corporate systems where they stored trade secret information such as Product Guides and supporting evidence for Entries.
- Provide keys to their Encrypted Data Vaults to CBP so that only CBP could access trade sensitive information.

This security model enables Rights Holders, Importers, Entry Filers and other participants in the supply chain to provide keys to CBP with respect to IPR Data without sharing that information with anyone else. It could also allow a specific trade partners to provide access to another specific trade partner on an as-needed basis using standard data models and protocols.

There were a few other standards and pre-standards specifications in use, like Web Ledger, JSON-LD, RDF Dataset Canonicalization, Linked Data Proofs, and Linked Data Signatures.

2.3.3.4. Encrypted Data Vaults

Standardization Status: Experimental pre-standards specification, expected to become adopted by W3C Credentials Community Group as a work item.
An Encrypted Data Vault is a secure server that receives, stores, and transmits encrypted data. Access to an Encrypted Data Vault is managed via Authorization Capabilities. An Encrypted Data Vault is similar to a Post Office box with a few extra security features: every letter is encrypted, every letter can be encrypted for multiple recipients, and access to any of the encrypted letters in the Post Office box requires a cryptographic proof created by a recipient's secret key.

Encrypted Data Vaults were used during the PoC to:
- Enable Trade Partners to store encrypted trade secret information Product guides and supporting evidence off-chain.
- Enable CBP to retrieve and decrypt trade private data and evidence as authorized by trade.

2.3.5. Hashlinks and Blockchain Links

Standardization Status: Experimental pre-standards specification, expected to become adopted by W3C Credentials Community Group as a work item.

Hashlinks refer to the ability to express a cryptographic hash that is computed from the content that can be retrieved by dereferencing a hyperlink.

Hashlinks and Blockchain Links were used during the PoC to:
- Express hashes written to the blockchain to provide proof of existence and ensure the integrity of data retrieved from systems.
- Point to specific data objects in specific blocks on specific blockchain networks, enabling cross-blockchain linking.

2.3.6. WebKMS

Standardization Status: Experimental pre-standards specification, expected to become adopted by W3C Credentials Community Group as a work item.

A Key Management System (KMS) is a cryptographic system that provides functionality, such as generate key, sign, verify, wrap key, and unwrap key. Web KMS provides a common interface to allow Web applications to communicate with KMS systems and is typically used when interoperability with proprietary hardware-backed key management solutions are desired.

Web KMS was used during the PoC to:
- Create and use cryptographic keys for use in Web applications that are based on secret material in a KMS that has key recovery features and protections against cryptographic key exfiltration.
2.4. Conclusion

The funding and operation of the Intellectual Property Rights Blockchain Proof of Concept by DHS/S&T, DHS/CPB, and the Trade participants, as well as the previous NAFTA/CAFTA Blockchain Proof of Concept, have been vital in not only shaping the global standards being pursued at the W3C, a consortium of over 480 global organizations, and IETF but have also led to a new area of standards related to increasing trust and verifiability on the Internet. This is demonstrated by W3C Membership’s broad support for the creation of the Verifiable Credentials Working Group and the Decentralized Identifier Working Group citing DHS/S&T, DHS/CPB, and private industry involvement as a key motivator for the creation and investment in these global standards setting groups. There are plans that are being actively pursued for launching more global standards groups to take the remaining technologies identified in this PoC through the standardization process.

The Proof of Concept achieved the original goals and stretch goals that were identified during the project, garnered more participation than we had predicted, and provided a number of lessons that would benefit any future CBP blockchain Proof of Concept in the space.

3. Digital Bazaar - Recommendations

3.1. Lessons Learned

In general, the PoC demonstrated that it is viable to use Verifiable Credentials, Decentralized Identifiers, Authorization Capabilities, WebKMS, Hashlinks, Blockchain Links, and Encrypted Data Vaults for streamlining CBP entry evaluations. Trade participants were able to use these technologies to achieve the desired outcome and CBP officers were able to use the information provided for making entry determinations.

Direct licensing and sublicensing proved to be insufficient for covering the range of use cases required by Trade. Instead, we discovered that a generic mechanism that allows a licensee to authorize any party for further fulfilment was necessary. This allowed Trade partners the flexibility to manage their supply chain as needed, while giving CBP the visibility to verify that specific products have appropriate license provenance without secondary requests for additional documentation.

A series of training sessions on the standards-based technologies used during this Proof of Concept were provided before the bulk of the trade engineering and development occurred. This led to a more educated set of participants. Participants where this was their second blockchain PoC were notably more vocal, understood the technologies being used at more depth, and had an easier time with the proof of concept than participants that were new to blockchain proof of concepts.
Work on the international standards used in this PoC continues, but without the support of many of the participants in the PoC. There is a healthy group of companies participating in the standards work, but very few dedicating resources on a consistent basis to move the standards along at an acceptable pace. This results in many of the standards taking longer to be completed than necessary. Consistent funding specifically for standards development from government and private industry would make a significant impact in the advancement of these technologies which make robust competitive marketplaces possible. Not funding these initiatives results in a proliferation of proprietary solutions, which harms interoperability, reduces competition, and raises costs for all participants in the ecosystem.

The list below highlights additional lessons learned during the previous NAFTA/CAFTA Proof of Concept that were also applicable during the IPR Proof of Concept:

1. Ensuring that the Engineering Plan is the single source of truth helps drastically reduce miscommunication, particularly in a setting such as the CBP NAFTA/CAFTA Proof of Concept.
2. Providing basic software components to all participants enables broad participation at the risk of reducing the number of organizations that develop software to demonstrate interoperability.
3. Decentralized systems design (e.g., any Blockchain system) remains a fairly foreign concept to many Trade Partners’ technology teams participating for the first time. Creating HTTP API interfaces that interact with Blockchain systems help dramatically with demonstrating interoperability as most teams know how to work with HTTP APIs.
4. Technology teams require quite a bit of support with regards to Blockchain systems integration and future projects should consider how to scale Trade Partner support.
5. Not understanding the economics of the system (e.g. what financial losses are a result of the current system) makes it difficult for core designers and developers to prioritize features.
6. Previous PoCs contained participants that did not educate themselves about the technologies and standards in use, which led to misconceptions around what was and was not possible with the system. The training sessions run as a part of this PoC helped mitigate this problem.
7. If there is an opportunity to put Private Information on a Blockchain, developers will do it, even if repeatedly warned to not do so. This PoC did not suffer from this problem as much as the NAFTA/CAFTA PoC did as the design moved many of these potentially problematic fields to Encrypted Data Vaults.
8. Decentralized systems are far less susceptible to system-wide failure, but are more prone to serial system dependency failures.
9. Decentralized models of Identity Management, while common in day to day settings (e.g. driver’s licenses), strike many participants as difficult to achieve in computer systems due to decades of proliferating broken security models such as usernames and passwords as well as access control lists. It will take a significant amount of educating to overcome this, but luckily we can build safer technology systems without having to do this education up front.
10. Unless a specific focus is placed on how the economics and politics of running a Blockchain network will happen, the discussion will not occur. This is the second PoC where the discussion related to who would run the blockchain or how a consortium would be put together to operate the system did not happen. Governance is a vital part of blockchain systems. Many of the PoCs explore the technological capabilities, some legal capabilities, but leave the governance of these systems to a later stage. Not discussing governance in the early stages can result in a PoC not progressing because private industry expects government to figure it out and government expect private industry to figure it out, leading to a catch-22 situation.

3.2. 

Opportunities for Improvement in a Pilot System

The PoC was designed to prove the benefits of specific, limited capabilities. In a pilot deployment, there would necessarily be numerous improvements to handle operations at scale and to address the edge cases that fall outside the uses addressed in the PoC.

We list here several specific areas for improvement that were identified during the PoC.

3.2.1. On-Chain License Count

Public ledgers are particularly good at resolving the problem of the transfer of resources. A pilot system could leverage the blockchain not just to track the veracity of licenses, but to keep track of quantity-limited licenses in a robust manner. This would require integration with more players in the supply chain. Further research is needed to ensure that proprietary data about import volumes is not exposed to competitors and the public.

3.2.2. Recordation of Affixation

One key insight of the PoC was that the legal authority to restrict import depends on whether or not IP is legally affixed to a particular product. Although license holders may have restrictive contracts about the distribution of licensed goods, a violation of those contracts are not enforceable by CBP. For example, a product with IP legitimately licensed for sale in Mexico may be legally importable to the US even though it violates the licensing contract, precisely because at the time of affixation of the IP, it was legitimate. This is an example of a gray market product.

Therefore, what CBP needs to verify at import is not whether or not there is a license to “import” but rather whether or not the IP was legitimately licensed at the time the IP was affixed to the product. It would probably be useful to enable and encourage manufacturers to record the proper licensed affixation at the time of manufacturing. This would provide non-repudiable evidence, for a given product, that a license was in place at the time of manufacturing, giving CBP the ability to verify a particular good is legitimately produced, independent of other unenforceable contract terms.

3.2.3. Messaging

The PoC relied on the blockchain for all inter-party communications. A pilot system would benefit from a secure messaging channel that could be used between participants without posting messages to the public chain. This would allow, for example, licensors to inform licensees that a license has been
recorded or updated, potentially with unique pair-wise identifiers so that only the licensee knows the license is for them. Then, when the licensee wants to use that license to file entry with CBP, the on-chain-recordation of the license is verifiable and no outside party is capable of correlating the public transactions with the companies involved.

3.2.4. Gray Market Goods
There are a number of “edge cases” for gray market goods that are, in fact, quite important to participants in the PoC, but were not well served in the limited test. A pilot system would benefit from figuring out how to validate IP licenses for gray market products. This would include refurbished goods, sold by someone other than the original manufacturer, which are nevertheless originally legitimately licensed products, as well as goods licensed for one country, legitimately produced, then redirected for sale in the US. The best way to handle these use cases is an open question; one that should be answered in a pilot system.

3.2.5. Customer Portal First Sale integration
In the PoC, there was no mechanism to prevent bad actors from re-using valid serialized GTINs on invalid goods, leaving customers to believe they had a valid product when in fact it was a counterfeit. Integration with a supply chain could use deeper provenance to attempt to detect this, possibly by providing information about whether or not the GTIN in question has already been sold. If a customer is expecting a new product, this would be a red flag. This would require some sort of tracking by the manufacturer to the good’s point of sale, and is unlikely to ever reach 100% coverage without undue requirements on retailers. However, for a majority of sales, especially through major retailers who have the infrastructure to integrate with such a system, this could be a distinct competitive advantage.
# 4. Appendix – Digital Bazaar

## 4.1. IPR Proof of Concept Evaluation Responses

Please indicate your entity/role on the project:

<table>
<thead>
<tr>
<th>CBP</th>
<th>Operations</th>
<th>Legal</th>
<th>Technology</th>
<th>Policy</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TRADE</th>
<th>Technology/Development Team</th>
<th>Business Team</th>
<th>Broker</th>
<th>Supplier</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Company and/or Office: Digital Bazaar, Inc.

Role: CEO

<table>
<thead>
<tr>
<th>Overall</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 1. Rate the viability of adopting this IPR proof of concept into your business process.

- Low: 1, 2, 3, 4, 5 High

### 2. Rate the strategic alignment of adopting this IPR proof of concept into your business process.

- Low: 1, 2, 3, 4, 5 High

### 3. How likely are you to recommend that CBP adopt the trademark and licensee data as part of filing?

- Low: 1, 2, 3, 4, 5 High

### 4. How likely are you to recommend that CBP incentivize the trademark and licensee data as part of filing?

- Low: 1, 2, 3, 4, 5 High

### Management Comments

#### 5. What was your overall experience and satisfaction with this proof of concept?

- Low: 1, 2, 3, 4, 5 High

#### 6. How likely are you to recommend that CBP invest more time and effort into blockchain technology?

- Low: 1, 2, 3, 4, 5 High

#### 7. How likely are you to recommend that your company invest independently in blockchain?

- Low: 1, 2, 3, 4, 5 High
<table>
<thead>
<tr>
<th>Question</th>
<th>Score/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. How likely are you to recommend that your company invest in blockchain in collaboration with supply chain partners?</td>
<td>Low [ ] 1 2 3 4 5 High</td>
</tr>
<tr>
<td><strong>Operational</strong></td>
<td></td>
</tr>
<tr>
<td>9. To what extent does this proof of concept improve your efficiency?</td>
<td>High [ ] Low 1 2 3 4 5</td>
</tr>
<tr>
<td>a. Please describe what metrics were used.</td>
<td></td>
</tr>
<tr>
<td>10. To what extent does this proof of concept reduce operational costs?</td>
<td>High [ ] Low 1 2 3 4 5</td>
</tr>
<tr>
<td>a. Please describe what metrics were used.</td>
<td>N/A - We do not have operational data.</td>
</tr>
<tr>
<td>11. Rate the user experience of the portal used in this proof of concept.</td>
<td>High [ ] Low 1 2 3 4 5</td>
</tr>
<tr>
<td>12. To what extent did the POC improve available data elements?</td>
<td>High [ ] Low 1 2 3 4 5</td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td></td>
</tr>
<tr>
<td>13. How easy is it to integrate blockchain to your existing architecture?</td>
<td>Very Easy [ ] Very Difficult 1 2 3 4 5</td>
</tr>
<tr>
<td>14. How likely is it that blockchain would allow you to reduce manpower?</td>
<td>Very Likely [ ] Very Unlikely 1 2 3 4 5</td>
</tr>
<tr>
<td>15. How would you rate the current return on investment (ROI) relative to the upfront cost?</td>
<td>High [ ] Low 1 2 3 4 5</td>
</tr>
</tbody>
</table>
### CBP Intellectual Property Rights Blockchain Proof of Concept
Digital Bazaar Final Report

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
<th>Rating</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.</td>
<td>How would you rate blockchain technology as a worthwhile investment for the future?</td>
<td>Low 4 High</td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>To what extent was blockchain shown to be scalable to the expected volume of future data?</td>
<td>Low 4 High</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Legal</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>How likely is your company’s legal team <em>currently</em> willing to allow use of blockchain for external data transfer?</td>
<td>Very Likely</td>
<td></td>
</tr>
<tr>
<td>19.</td>
<td>How would you rate blockchain technology’s potential to relieve the need for a physical signature?</td>
<td>Low 4 High</td>
<td></td>
</tr>
<tr>
<td>20.</td>
<td>To what extent would <em>rules and regulations</em> need updated to leverage blockchain technology?</td>
<td>Low 4 High</td>
<td></td>
</tr>
<tr>
<td>21.</td>
<td>To what extent would <em>statutes</em> need to be updated to leverage blockchain technology?</td>
<td>Don’t know</td>
<td></td>
</tr>
<tr>
<td>22.</td>
<td>Based on the answers to the questions above, how much time would it take to initiate new rules and regulation packets?</td>
<td>Don’t know</td>
<td></td>
</tr>
<tr>
<td>23.</td>
<td>Are there any other legal implications that should be considered?</td>
<td>Don’t know</td>
<td></td>
</tr>
<tr>
<td>24.</td>
<td>What would you suggest could be done differently to improve future projects?</td>
<td>Included in Final Report</td>
<td>Included in Final Report</td>
</tr>
<tr>
<td>25.</td>
<td>From those collected as part of this POC, what data fields would you add or remove?</td>
<td>Included in Final Report</td>
<td>Included in Final Report</td>
</tr>
<tr>
<td>26.</td>
<td>What went well that should be retained for future projects?</td>
<td>Included in Final Report</td>
<td>Included in Final Report</td>
</tr>
<tr>
<td>27.</td>
<td>Please provide any additional comments you may have.</td>
<td>Included in Final Report</td>
<td>Included in Final Report</td>
</tr>
</tbody>
</table>