U.S. Customs and Border Protection

TTO Trade Transformation Office

NAFTA/CAFTA Proof of Concept Overview & Results

Pub # (OPA) 0912-0619

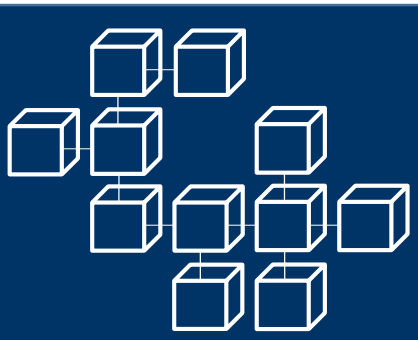
The North American Free Trade Agreement/Central America Free Trade Agreement (NAFTA/CAFTA) proof of concept (POC) tested the application of Blockchain technology for the entry summary submission process for NAFTA/CAFTA entries. A joint effort was spearheaded by Customs and Border Protection (CBP), Department of Homeland Security (DHS) and private sector organizations. The POC specifically tested the feasibility of the technology for receiving certificate of origin (CO) data and conducting free trade agreement (FTA) origin verifications. Via the test, CBP could request information through the Blockchain to substantiate a claim in lieu of CBP Forms 28 and 29. As a result, **the POC achieved almost instantaneous communications between CBP and trade, improved documentation of receipt, and expedited processing for CBP.** Other results of the POC include:

10
separate system integrations established with the CBP Blockchain

100%
success rate for live testing

3
different Blockchain softwares communicated seamlessly/interoperability

Recommendation to Proceed



The Business Transformation and Innovation Division (BTID) has reviewed the comments submitted by the private sector and government entities that participated with the NAFTA/CAFTA Free Trade Agreement Blockchain POC. The project received very high marks with the exception of one area outlined below. We are very proud of the work accomplished by all involved.

In stating the above several issues may prevent rapid adoption of this technology. 1) Free Trade Agreements have not been fully negotiated. 2) Few in the private sector have adopted Blockchain technology. 3) Designated application should be considered for potential Customs Trade Partnership Against Terrorism/Authorized Economic Operator (CTPAT/AEO) benefit but should run within a dedicated National Customs Automation Program (NCAP) test first.

Thank you,

Vincent Annunziato - Director, BTID

"…[the POC] was a wonderful experience and I believe that CBP is laying a solid foundation for the future of trade transactions."

– Nancy Luttrell, Director of Special Projects, F.H. Kaysing Company LLC

U.S. Customs and Border Protection

TTO Trade Transformation Office

POC Evaluation Highlights

The Blockchain POC was developed using a "fail fast" approach, which entailed running short, low-cost tests of Blockchain technologies. Participants in the POC included CBP auditors, import and entry specialists, CBP legal and policy personnel, importers, technology companies, and suppliers. Overall, the POC was a success. It achieved the goals identified at the beginning of the project, garnered more participation than anticipated, attracted more press than expected, and provided a number of lessons learned for future CBP Blockchain POCs in the space. Highlights of participant feedback, based on operational, technical, policy and legal considerations, are included in the quad chart below.

Operations

- ✓ Improved facilitation of CBP's audit process
- ✓ Increased speed and assurance of communication between CBP and trade
- ✓ Preliminary analysis and risk assessments enhanced by having the NAFTA/CAFTA statement embedded in initial filing
- ✓ Creates the potential for import specialists to focus more time on determinations and less time documenting results

Policy

- ✓ Supportive of leveraging Blockchain technology to enhance CBP's enforcement posture
- ✓ Recommend a working group be established with representatives across the Office of Trade (OT), Immigration and Customs Enforcement (ICE), and U.S. Trade Representative (USTR) to resolve questions on compliance issues and to develop standard operation procedures in applying blockchain to the FTA verification process.

Technical

- ✓ The digital signatures supported by Blockchain provide far more security than physical signature typically required for NAFTA/CAFTA processing
- ✓ Future Blockchain POCs should make running a Blockchain node a mandatory requirement of participation

Legal

- ✓ Found no legal prohibitions against electronic submission and CBP verification of the data elements comprising a NAFTA certificate of origin and a CAFTA-DR certification
- ✓ Recommend piloting the system under NCAP and specifically approving the use of the Blockchain technology to electronically sign and transmit an electronic equivalent of a NAFTA certificate of origin and CAFTA-DR certification

U.S. Customs and Border Protection

TTO Trade Transformation Office

Would you like to expand on this project to adopt it into ACE?

75% said yes (without conditions)

25% said yes (with conditions)

"I think this would be a great addition to bring into ACE"

Does Blockchain technology relieve the need for a physical signature?

75% said yes

How satisfied are you with the level of involvement you had on the POC?

93% said satisfied

"I felt honored and privileged to be part of this POC… I love Blockchain!"

What was your overall experience and satisfaction with this POC?

100% said satisfied

"I very much enjoyed the experience and was very satisfied with this POC."

Would you recommend investing more time and effort into Blockchain technology?

100% said yes

"Yes, it would be a useful tool to improve time spent on communications between CBP and Trade."

Is the long term Return on Investment (ROI) effective to the upfront cost?

Inconclusive

Do you feel that this technology is a worthwhile investment for the future?

100% said yes

NAFTA/CAFTA Proof of Concept Assessment

Version 2.0
November 28, 2018

Pub # (OPA) 0912-0619

Table of Contents

1. Executive Summary

1.1. Abstract

This Proof of Concept (POC) provides the results associated with the test conducted with North American Free Trade Agreement/Central America Free Trade Agreement (NAFTA/CAFTA). The goal of the NAFTA/CAFTA POC was to evaluate the application of Blockchain technology to the Entry Summary submission process. Overall, the POC was a success. It achieved the goals identified at the beginning of the project, garnered more participation than anticipated, attracted more press than expected, and provided a number of lessons learned for future CBP Blockchain POCs in the space.

The POC evaluated whether employing Blockchain technology would provide compelling operational benefits and cost savings. Based on feedback provided by the POC participants, all respondents agreed that the POC should be adopted into ACE. Responses were mixed regarding the perceived long-term return on investment on Blockchain technology, however respondents universally supported continued investment of time and effort into Blockchain.

Participants in the live fire test also appreciated the new functionalities provided by the POC, including increased speed and assurance of correspondence between CBP users and the trade, the elimination of paper documents, and improved facilitation of the auditing process. The group most critical of the POC was the trade, which expressed that the POC did not increase the efficiency of their work.

2. Introduction

2.1. General

A Proof of Concept (POC) is a short assessment used to demonstrate the feasibility of a specific concept or theory. The POC furthers the concept development by establishing viability, identifying technical and operational issues, providing recommendations for investment in a framework for future program development and budgeting of the activity, and the various resources required to execute the concept of operations.

This POC provides the results associated with the test conducted with North American Free Trade Agreement/Central America Free Trade Agreement (NAFTA/CAFTA). It applies the principles and best practices of IT project management to a POC or demonstration pilot for custom built, alternative business solutions, and innovative technologies whose purpose is to assess whether the solution or technology should be integrated into our existing business and/or technology operations, or deployed agency-wide.

A proof of concept effort always terminates in an evaluation that documents the results of the effort and compares the results to the original, planned objectives and goals and explores new ideas arising from the proof of concept. Results of the proof of concept assessments may be fed back into requirements specifications, designs, or technology investigations. When employed for these purposes, a proof of concept is a useful tool in systems development.

2.2. Background

The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate conducted an invitation-only Blockchain Workshop on October 11-13, 2017, with day two designated as “Trade Day.” The session was well attended, with approximately 80 participants at the level-setting “Blockchain 101” session on day one, and approximately 30 participants at Trade Day. Participants collaborated in the development of criteria for proposed use cases, identified 12 ideas, and then prioritized the top 3-4 candidates for further investigation.

Subsequent to the Blockchain workshop, the U.S. Customs and Border Protection (CBP) held deep-dive requirements sessions with members of the trade community on January 18-19, 2018 to further refine requirements for use of Blockchain. Participants in the follow up-discussions were asked to provide the following information related to each use case:

- Current state of operations, forms, and workflow
- To-be state of operations, focused on how Blockchain would alter the current state
- Metrics to demonstrate success of a particular use case
- Benefits expected

Based on scoring at the following discussions, NAFTA/CAFTA was identified as the best candidate for a Blockchain pilot.

Blockchain is one of the first technologies the Commercial Customs Operations Advisory Committee (COAC) Emerging Technologies Working Group is focusing on to determine how it can be used to benefit the Trade mission. There appears to be opportunity among the trade community to leverage Blockchain either to track/validate goods in the supply chain to support due diligence, or potentially to support verifiable claims to CBP for audit/compliance purposes.

2.3. NAFTA/CAFTA Proof of Concept

The CBP NAFTA/CAFTA proof of concept evaluated whether employing Blockchain technology would provide compelling operational benefits and cost savings. The aim of utilizing Blockchain technology was to improve the processing of trade-related documents by hosting information about trade transactions on a decentralized, tamper-proof distributed ledger system, which can be authenticated and accessed by various stakeholders. The goal was to prove that a standards-based, fully digital system could be created to replace the existing paper-based system. The system would enable better auditability, expedite the evaluation of free trade agreement eligibility, and increase NAFTA/CAFTA transparency, and more clearly identify suppliers and manufacturers. It would also allow the trade community to implement and administer their own evidence systems, sharing certain required documentation with CBP only.

Therefore, the assessment and evaluation is perhaps the most important part of the proof of concept. An initial baseline analysis allows CBP to understand the concerns of the participants involved and provides an opportunity to address them before proceeding with full deployment and/or expanding the model to additional programs. Interim assessments can evaluate the effectiveness of particular aspects of the proof of concept (e.g. business and technical requirements) and gauge changes in usage of the system and user satisfaction.

2.4. Goals and Objectives

The overall objective of the proof of concept is to determine the feasibility of using Blockchain technology. The following considerations as to what the proof of concept should accomplish are outlined below:

- Verify the functionality, interoperability, and systems design
- Validate the usefulness, efficiencies, productivity, and effectiveness of the systems or technology
- Obtain end user insights and feedback regarding impacts to day-to-day operations, processes, and procedures
- Test interfaces with related business functions and information systems
- Verify that the system is both operationally and technically viable and stable
- Validate initial outcomes and cost/benefit projections

2.5. Why Blockchain

The primary purpose of the project is to prove the viability of using a decentralized ledger or “Blockchain” to achieve the above goals. Decentralized ledger technology provides:

- Cryptographically provable and tamperproof history; auditability
- Distributed access, consensus, and independent administration of a shared database
- No single point of failure or central clearing house; resilience
- Hyperlinks or “anchors” to information with cryptographically verifiable content integrity and proof of existence

- An operational architecture that shares and reduces costs

2.6. Stakeholders

Table 1.

	Stakeholder	Now	Future
Supplier	**Manufacturer** Adds value to the raw materials into other consumables and finally the end product	- Has limited ability to control and verify the flows coming from its suppliers	- Benefits from an integrated and distributed ledger that enables them to control the inputs and keep track of production
	Exporter Responsible for the information related to the entry/clearance of goods into the United States (U.S.)	- Limited certification ability and complex tracking	- Shared information system - Distributed and certified system - Ensure goods are transported in the right conditions
Trade	**Importer** Responsible for the purchase of goods entering the U.S.	- Limited certification ability and complex tracking	- Shared information system - Assurance that goods will arrive in due course
	Broker Responsible for facilitating transactions between Exporter and Importer	- Difficult to certify the origin and path of goods brought and sold	- Full end to end visibility - Verifiable authenticity and immutability of digital documents
Government	**PGA** Liaison between the stakeholders	- Difficult to certify the origin and path of the goods brought and sold	- Can easily check the origin of the goods and their transformation path on the Blockchain - Check and prove its authenticity
	CBP Audit/compliance	- Difficult to certify the compliance, origin, and composition of the goods to be brought	- Have full view of the goods brought directly on the Blockchain

2.7. Future Adoption Assumptions

The following assumptions reflect the future vision for adoption of the POC:

- All participants in the Blockchain will be instituted on the Blockchain
- Trade partners will build and maintain their own Blockchain nodes
- Data elements on forms will be sent instead of the form itself. No “digital paper.”
- Trade secrets and personally identifiable information (PII) will be managed securely
- Enable trade secrets and PII to be maintained by the trade locally, off of the Blockchain
- All current data required for Entry Summaries will remain the same
- Entry summaries would be sent to a separate system
- Importers, exporters and CBP would be part of the Blockchain
- Should allow country of origin tracking

3. Assessment

3.1. General

The feasibility of using Blockchain technology to conduct NAFTA/CAFTA verifications is assessed based on tasks, conditions, and standards established by the Working Group.

3.2. Establishing Criteria for Evaluation and Succes

3.3. Evaluation Considerations

The questions identified in Table 2 were meant to serve as a guideline and source for valuable feedback. The questions could have been modified by POC participants, provided they still validated business and technical requirements and performance expectations. The responses to the evaluation considerations can be found beginning with Appendix A.

Table 2.

#	Please describe any advantages/disadvantages of:
1.	Having the NAFTA/CAFTA statement embedded in the initial entry summary filing
2.	Utilizing Blockchain technology in lieu of the traditional CBP Form 28/29 process
3.	Request notification for additional data
	Business/Operational
4.	How did this proof of concept improve your efficiency?
	a. Please describe which metrics were used.
5.	Please describe the advantages/disadvantages associated with the efficiency of this proof of concept.
6.	How could we improve the user experience to make this more efficient?
7.	How did this proof of concept reduce operational costs, if any?
	a. Please describe which metrics were used.
8.	Based on the data you received, would you like to have seen more/less data? Something different?
9.	Was the data accessible – was there ease of collection and use?
	Technology
9.	Please describe the complexity of your initial architecture and setting up the Nodes and/or Trade Evidence System for your institution?
10.	How will you transition from the current data structure to the Blockchain structure?
11.	Is the manpower associated with Blockchain enhanced or worsened compared to current systems and procedures?
12.	Is the long term Return on Investment (ROI) effective to the upfront cost?
13.	Do you feel that this technology is a worthwhile investment for the future? Why/Why not?
14.	Is it scalable to the volume of data being dealt with in the future?
	Legal (CBP Only)

15.	Does Blockchain technology relieve the need for a physical signature?
16.	Which rules and regulations need to be updated with Blockchain technology?
	a. Which statutes – if any?
	b. Since all entities are on the Blockchain, what would it take for CBP to be able to remove the CBP Form 28/29 process?
17.	Based on the answers to the questions above, how much time would it take to implement new rules and regulation packages?
18.	Are there any other legal implications that should be considered?
	Please describe your thoughts on the business aspects of the Blockchain Proof of Concept for NAFTA/CAFTA
19.	How satisfied are you with the level of involvement you had on the proof of concept?
20.	What was your overall experience and satisfaction with this proof of concept?
	What went well? What did not go well?
	a. Business vs. technology and vice versa
21.	What would you suggest could be done differently to improve future projects?
22.	Would you like to expand on this project to adopt into ACE?
23.	Would you recommend investing more time and effort into Blockchain technology? Why/Why not?
24.	Any other comments?

3.3.1. Success Criteria

Key Performance Indicators (KPIs) are crucial to evaluating the success of this proof of concept. The metrics identified in Table 3 are meant to serve as a guideline and source for valuable feedback. The metrics may be modified as needed but should validate business and technical requirements and performance expectations.

Table 3.

Key Performance Indicators	Metrics	Method
Increased adoption		
Training effectiveness		
Reduced operating costs		
Increased productivity		
Improved collaboration		

4. Findings

4.1. General

From September 11 to October 2, 2018, 30 participants from CBP HQ, CBP operations, technology and development, and trade communities participated in the CBP NAFTA/CAFTA proof of concept (POC). Following the POC, each participant completed an evaluation to provide their feedback (see *3. Assessment* for evaluation questions and criteria). BTID received 23 assessments, which were used to discern various outcomes and recommendations from the POC participants' perspective.

The POC participants provided both affirmative and critical feedback of the POC, with comments typically aligning according to participant group (e.g. CBP, trade, etc.). Members of the trade, for example, reported that the POC created certain redundancies, and CBP participants reported issues with data consistency. Many respondents praised the live test, and all assessment respondents indicated that they were satisfied with the POC experience and that they would "recommend investing more time and effort into Blockchain technology."

4.2. Key Outcomes

4.2.1. Results: What Worked Well

POC live test participants indicated various benefits of the POC, including that it standardized the process for filers, facilitated CBP's compliance evaluation process, eliminated the use of paper, allowed for the digital submission of certificates of origin, and overall expedites the filing process. The POC also successfully embedded statements in the initial entry summary and streamlined requests for information which would normally require CBP personnel to complete CBP Form 28 and notify the importer of the outcome of an action using CBP Form 29, which CBP participants reported as an advantage of the POC. Although the idea was not universal among respondents, POC participants suggested that Blockchain technology eliminated the need for CBP Form 28. Various CBP respondents also noted the benefit of being able to request notification for additional data, which they indicated would greatly assist with the auditing process, and the ability to verify claim receipts. Notably, members of the trade did not identify any advantages regarding embedded statements, CBP forms 28 and 29 or notification requests for additional data.

With regards to operational benefits to POC users, participants in the live test identified that the POC has the potential to significantly assist the auditing process by providing faster, digital communication between CBP officials and the trade. Live test participants from CBP also reported that the POC has the potential to reduce operational costs by reducing travel costs for auditors, reducing inquiry response wait time, and reducing the need to print paper copies of requests. Members of the trade and CBP operations did not indicate that the POC possessed any cost reduction opportunities.

Respondents universally indicated that Blockchain technology is a "worthwhile investment for the future." Regarding the scalability of the POC for larger data sets, respondents stated that they believed the POC ought to be scalable, depending on the size of the data sets used in the future.

In the legal realm, live fire participants noted that the POC ought to be able to relieve the need for a physical signature and eliminate the need for CBP Form 28, given regulatory approval.

When asked about their satisfaction with their level of involvement in the POC and the overall experience with the POC, all respondents indicated that they were satisfied on both accords. Many live test participants stated that the POC was conducted smoothly and that, from the user's perspective, everything was straightforward. The preparatory work for the live test also helped facilitate the experience. All respondents supported expanding the POC project to adopt it into ACE and investing more time and effort into Blockchain technology going forward.

4.2.2. Results: Areas for Improvement

Members of the trade mentioned that the POC does not save them work and does not improve efficiency because it creates redundancies within the filing process. Respondents also mentioned that the POC required them to input data they were not previously required to input for NAFTA/CAFTA evidence. Various technology and development participants also expressed concern over how the novelty and newness of Blockchain could prove an obstacle when pitching the technology to potential new users.

When asked about the operational aspects of the POC, technology and development respondents noted that the POC creates more work for the filer by requiring that they have the Certificate of Origin ready in advance. Respondents also requested that PDF files be removed from the POC and that the system have a purely data-driven process. One respondent noted the additional work created by having to sign into an additional system. Multiple POC participants also experienced issues with data inconsistencies when filling out Certificated of Origin in different time zones. One CBP respondent indicated that future versions of Blockchain should ensure compatibility for the system and software programs utilized by both sides. Members of the trade indicated that the POC suffered from the exclusion of exporters; they recommended including exporters in future POCs.

Regarding technology-related issues of the POC, respondents noted that the POC would benefit from the removal of free-form text entry. One member of the trade also indicated that the data requested by the POC creates duplicate work for importers, as the data was previously entered by exporters. Many respondents also indicated that they felt unable to estimate the scalability of the POC or its long term return on investment. One CBP user expressed the need to include a comment section for both trade and CBP users to allow users to explain why a submission was rejected.

There were no clear areas of improvement regarding the legal aspects of the POC, however some respondents did question the ability to eliminate CBP Form 28 for legal reasons and the ability to view previous versions of the Certificate of Origin while using Blockchain, which users are currently able to do. There was also an expressed interested in including "the appropriate policy offices" in the process so as to have the upgrade to Blockchain not be derailed by internal regulations. One member of the trade also noted that while the POC relieves the need for a physical signature, it does not eliminate the need for an electronic acknowledgement of receipt.

4.3. Conclusion

All POC participants conveyed satisfaction with the preparatory work prior to the POC and the execution of the POC itself. All assessment respondents similarly expressed a desire to continue investing resources in Blockchain technologies and to expand the POC to adopt it in ACE. Members of the CBP community appeared to express the most praise for the POC, chiefly due to the POC's ability to facilitate the auditing process. Other recurring praise for the POC included its ability to expedite communication and eliminate the use of paper documents, physical signatures, and potentially CBP Form 28.

The POC live test produced critical feedback as well, coming most evidently from the trade community. Unlike other respondents, those from the trade indicated that the POC did not increase the efficiency of their workflow. Various technical malfunctions also arose during the POC, such as Certificate of Origin data consistency, as well as certain user interface components, including the use of PDFS, the absence of comment boxes, and the use of free-form text entry.

5. Recommendations

5.1. Lessons Learned

The POC produced both commendations and critiques from participants in the live fire test. POC live test participants unanimously reported satisfaction with their preparation for and participation in the POC live test. Users felt well-informed before participating in the test, and also reported that the POC was straightforward and user-friendly during the live test. Given POC users' widespread praise for how they felt informed and included throughout the POC process, the POC live test could be used as a replicable model for future innovative deployments.

All assessment respondents also agreed that the POC should be adopted into ACE. Responses were mixed regarding the ROI on Blockchain technology, however respondents universally supported investing more time and effort into Blockchain technology.

As for the functionalities of the POC, users appreciated the increased speed and assurance of correspondence between CBP and the trade, the elimination of paper documents and physical signatures, and the bettered facilitation of the auditing process. The group most critical of the POC was the trade, which expressed that the POC did not increase the efficiency of their work. This was a result of redundant data entry and difficult access to certain forms due to the POC's exclusion of exporters. Multiple trade members indicated that adding exporters to the POC would have decreased their workload during the live test.

5.2. Next Steps

NAFTA/CAFTA POC

- Involve exporters in the NAFTA/CAFTA POC
- Resolve Certificate of Origin time and date inconsistencies
- Remove the use of PDF files in order to run a purely data driven process
- Ensure compatibility for the systems and software program utilized by both sides and enhance the messaging capabilities for better communication
- Ensure that all users meet software requirements prior to POC

Future POCs

- Continue investing in Blockchain technology
- Run a live fire POC in ACE

General

- Create strategy to facilitate new user integration into Blockchain to facilitate adoption
- Replicate the NAFTA/CAFTA POC preparation plan in future live fire tests

Appendix A – Test Parameters

- Acceptance of “digital paper,” PDF forms in addition to data elements
- Trade secrets and PII not held on the Blockchain. Trade maintained locally
- At minimum, trade participants were required to implement Trade Evidence Server, to store interoperable data
- Participants also had option to develop local Blockchain node
- Entry Summaries were truncated for the purposes of this test
- Data did not remain on DHS system; system taken down completely at end of test
- Importers and CBP participated in this test
- All submissions were tested by operational staff for accuracy and ease of use
- Test created translation layer for exchange across systems levering existing industry standard, HTTP API protocols
- Data for exchange developed according to DHS S&T standards

Appendix B – Evaluation Responses

Please indicate your entity/role on the project :		
☐ CBP Operations	☐ CBP	☐ Supplier
☐ Technology/Development Team	☐ Trade	

Please describe any advantages/disadvantages of:		Comments
1.	Having the NAFTA/CAFTA statement embedded in the initial entry summary filing	
2.	Having Blockchain technology in lieu of CF 28/29 process	
3.	Request notification for additional data	
Business/Operational		**Comments**
4.	How does this proof of concept improve your efficiency?	
	a. Please describe what metrics were used.	
5.	Please describe the advantages/disadvantages associated with the efficiency of this proof of concept.	
6.	How could we improve the user experience to make this more efficient?	
7.	How does this proof of concept reduce operational costs, if any?	
	a. Please describe what metrics were used.	
8.	Based on the data you're receiving, would you like to have seen more/less data? Something different?	
9.	Is the data accessible – is there ease of collection and use?	
Technology		**Comments**
9.	Can you describe the complexity of your initial architecture and setting up Blockchain for your institution?	
10.	How will you transition from the current data structure to the Blockchain structure?	
11.	Is the manpower associated with Blockchain enhance or worsen in terms of the Blockchain technology?	
12.	Is the long term Return on Investment (ROI) effective to the upfront cost?	
13.	Do you feel that this technology is a worthwhile investment for the future?	
14.	Is it scalable to the volume of data being dealt with in the future?	

Legal		Comments
15.	Does Blockchain technology relieve the need for a physical signature?	
16.	What rules and regulations need to be updated with Blockchain technology?	
	a. What statutes – if any?	
	b. Since all entities are on the Blockchain, what would it take for CBP to be able to remove the CF 28/29 process?	
17.	Based on the answers to the questions above, how much time would it take to initiate new rules and regulation packets?	
18.	Are there any other legal implications that should be considered?	
Please describe your thoughts on the business aspects of the Blockchain Proof of concept for NAFTA/CAFTA		**Comments**
19.	How satisfied are you with the level of involvement you had on the proof of concept?	
20.	What was your overall experience and satisfaction with this proof of concept?	
	What went well? What didn't go well?	
	a. Business vs. technology and vice versa	
21.	What would you suggest could be done differently to improve future projects?	
22.	Would you like to expand on this project to adopt it into ACE?	
23.	Would you recommend investing more time and effort into Blockchain technology?	
24.	Any other comments?	

Appendix C – Digital Bazaar: NAFTA/CAFTA POC Findings

1.1. General

The goal of the NAFTA/CAFTA POC was to evaluate the application of Blockchain technology to the Entry Summary submission process with a specific focus on submitting the Certificate of Origin and enabling content integrity verification before it is requested by a CBP Import Specialist.

One metric of success was to get a single trade partner system to integrate with the CBP Blockchain system. The group was able to achieve 10 separate software system integrations, 22 hours of testing, and a 100 percent live testing success rate.

There were a number of goals that were identified as central to the NAFTA/CAFTA Proof of Concept:

1. Track NAFTA/CAFTA Entry Summary header status, supporting documents, and other related data in a digital, tamperproof, and auditable manner.
2. Enable the trade community to store Entry Summary data and supporting documentation on their own systems while providing auditable proof of existence and limited access to CBP.
3. Provide a system predicated upon Blockchain principles to test the veracity of digitizing NAFTA/CAFTA data further back in the supply chain.
4. Reduce/remove laborious practices by supplying NAFTA/CAFTA data earlier in the process and providing direct links to supporting documentation.
5. Ensure accuracy of origin data by clearly identifying suppliers/manufacturers
6. Increase transparency of NAFTA/CAFTA eligibility to all entities by supplying communal information that informs the status of the shipment.
7. Provide a mechanism for each participant to be responsible for generating their own notifications of Entry Summary status activity.
8. Reduce operational costs by achieving the goals above (increase rate of processing, reduce shipping preparation and printing costs, enable further automation).

During the NAFTA/CAFTA POC, the goals were fulfilled in the following ways:

- Entry Summary NAFTA/CAFTA status information and hyperlinks to supporting documents that reside on an external evidence system were written to the Blockchain (addressed goals 1, 2, 3, 4, 6, 7, 8).
- Hyperlinks in the Blockchain were dereferenced by CBP (via Object Capabilities and Resource Integrity Proofs) to produce supporting documents from an external evidence system (addressed goal 2).
- The existence and integrity of supporting documents retrieved from an external evidence system were verified against Blockchain records with a positive or negative result (addressed goals 1, 2, 3).
- Multiple parties in the supply chain, including suppliers/manufacturers, were clearly identified in the information anchored to the Blockchain (addressed goals 3, 5).

- A separately administered Blockchain node joined the Blockchain network and read all of its data. Writing data was supported, but no trade partner attempted to do so via their own Blockchain node during the POC. (addressed goals 6, 7, 8).

Based on the goals and requirements identified by the group in the Engineering Plan, the Proof of Concept was a success. The following sections detail key outcomes, lessons learned, and suggestions for future Blockchain POCs and pilots.

1.2. Key Outcomes

We break the key outcomes into two phases focused on Development and Testing. Each section identifies good outcomes and bad outcomes. Lessons learned and suggestions for future pilots and Productionization of this technology, if it progresses to the next phase, are provided in following sections.

1.2.1 Development

The development process started in April 2018 with the creation and refinement of an Engineering Plan. The majority of software development proceeded from May through mid-July 2018. Trade Partner integration proceeded from mid-July to the end of August 2018, ending with Testing in September 2018. A visual summary of the timeline is shown below:

Design April 2018	Development May - July 2018	Integration August 2018	Testing September 2018

The process of developing the Engineering Plan went smoothly. The initial in-person meeting between CBP and the Trade Partners was helpful in establishing group rapport. Clear goals provided by CBP and Trade helped with group cohesion and understanding what the Proof of Concept was and was not attempting to achieve. Weekly meetings during the development phase helped ensure that all participants stayed in sync on the Engineering Plan. Overall the project was well scoped and managed. There were little to no disagreements on technical approach, although the tight timeframe probably helped keep any disagreements to a minimum.

Focusing the Engineering Plan as the single source of truth for the project also helped ensure that all participants referred to it when developing their own systems instead of depending on tribal knowledge during the project. The result of this approach resulted in many more software integrations than we had counted on, which also created challenges as we will outline below. Overall, the development process was fairly smooth but intense due to the large amount of work and the short timeframe.

Furthermore, the technical team was able to achieve all of the development stretch goals we had set for the Proof of Concept. This includes integrating pre-standards technologies by using the Decentralized Identifiers, Verifiable Credentials, Object Capabilities, and Web Ledger specifications.

The challenges during this process were largely created by the short timeframe of the Proof of Concept. Digital Bazaar made a decision early on to provide all software necessary to integrate with the system. In hindsight, that was the right decision to make as many of the Trade Partners were unable to allocate significant internal development resources to participate in a meaningfully technical way. Providing software enabled those that did not have the budget or personnel to participate to still learn from the exercise. That said, a few Trade Partners did a significant amount of integration effort and having the Digital Bazaar software system to copy or use was beneficial. Almost every Trade Partner used the Trade Evidence Server software to interact with the CBP Blockchain Nodes.

Digital Bazaar providing all software necessary to integrate increased the number of organizations that could participate and resulted in far more support than we had anticipated for the POC. We had estimated 20 percent of the POC time budget for support and ended up with closer to 40 percent of the entire time budget supporting Trade Partners. In the end, the large number of successes reflected the support provided, but caused disruption among the core development teams.

While a comprehensive Engineering Plan was created and updated throughout the development process, the metrics for commercial success were not clear throughout the process. This made it difficult for the developers to prioritize features or areas of focus from a systems design and user interface perspective. It only became more clear during testing what the pain points were. It still remains to be seen what the direct economic impact will be if the system goes into production. Statements collected during the POC seemed to indicate a reduction in manual paperwork, waiting for forms to be sent back and forth, and fines levied on Trade Partners as a result of poor Trade Partner documentation. Losses to large Trade Partners seemed to be in the tens of millions of dollars per year, and if true, would provide a compelling business case for the Trade Partners.

1.2.2 Testing

The testing process was organized into two phases. The first phase consisted of a set of Dry Run testing that occurred during the last two weeks of August 2018. The second phase consisted of a month of testing during September 2018. Overall, 22 hours of testing was performed over the course of six weeks with 9 organizations and 25 different people operating various components of the system. There was a 100 percent success rate for all live tests. A number of minor, non-fatal errors were encountered during the tests, which were documented and supplied to CBP.

There were a number of good outcomes during testing. At least three Trade Partners integrated their own systems into the NAFTA/CAFTA POC system. The remaining seven systems utilized the Digital Bazaar provided Blockchain Node and Trade Evidence System. Dry run testing prepared all Trade Partners and CBP Personnel for the live tests and contributed to the success rate of the system.

The challenges during testing revolved around the myriad of different operational environments that the Trade Partners had deployed. Some ran the systems on Amazon Web Services, others in the IBM Cloud, others in custom Docker environments, and others in Open Stack environments. Some of the internal Trade Partner networks caused occasional connection failures while others blocked traffic sporadically. In the end, Digital Bazaar engineers were able to work through all of the issues during dry run testing, but had underestimated the degree of the heterogeneity of the full system.

The development timeline was aggressive, which resulted in Trade Partners attempting to ensure they could participate in the testing phase, which further resulted in a conservative set of priorities. For example, many did not run Blockchain nodes due to it being an optional system. Many focused on using the Digital Bazaar software provided instead of building their own. The two companies that did build their own systems utilized one to two developers, which demonstrated that it could be done with little effort but a perception of it being a monumental task most likely prevented others from attempting to engineer their own systems.

Decentralized systems, such as the one created for the NAFTA/CAFTA Proof of Concept, are far more resilient to system-wide failures but are still susceptible to point to point failures. For example, for an Entry Summary to be successfully processed in this Proof of Concept, at least four systems needed to be operational at the time of processing: The Veres One Decentralized Identifier Blockchain (highly fault tolerant), the CBP NAFTA/CAFTA Blockchain (highly fault tolerant), the CBP Evidence Server (single point of failure), the Trade Partner Evidence Server (single point of failure). While it is possible to make those single points of failure highly fault tolerant, it does take effort and was not done during the Proof of Concept. While this didn't result in permanent failures during testing, it did result in one or two events that required Web page refreshing to make progress. During testing, developers were instructed to not put corporate identifiers onto the Blockchain did so on multiple occasions. The only possible place to do this was in the domain name for the Trade Evidence Server, and several teams used human readable corporate identifiers in the domain name of their Trade Evidence Servers. The lesson learned here is that if it is possible to put sensitive data into a Blockchain, developers will find a way to do so even if it has been warned against on multiple occasions.

Testing also uncovered a number of usability issues with the Proof of Concept. All parties wanted to be able to state why an Entry Summary was rejected. It was not clear what the units of measure were in the system. Multiple CBP Personnel worked on the same entry summary at the same time and wanted a warning in the system if someone else was currently working on an Entry Summary. These desires should be taken into account if the system were to proceed to a pilot phase.

1.2.3 After Action Review

After the testing phase, both CBP and the Trade Partners gathered to discuss the things that went well, the things that did not go well, lessons learned, key outcomes, and potential next steps.

It became clear during the after action review that some of the Trade Partners and CBP wanted a slightly different data model. Specifically, they desired one that would allow them to dynamically link to a single Certificate of Origin from multiple line items. While the notion was raised during the planning phase for the project and the group decided to just focus on a single line item containing a single Certificate of Origin, Trade seemed to want the ability to link many line items to a single Certificate of Origin. It is unfortunate that the strength of that desire wasn't uncovered during the development process as it would have been fairly trivial to add that feature to the system.

It also became clear that a number of the Trade Partners did not understand the full capabilities of the system (as they requested features that already existed in the system), nor why we used some of the pre-standards technology subsystems that we did. For the sake of completeness, each key pre-standards technology is outlined below along with why we used it in the Proof of Concept.

1. Decentralized Identifiers (analog: driver's license number)
2. Verifiable Credentials (analog: driver's license)
3. Object Capabilities (analog: key to a post office box)

1.2.3.1 Decentralized Identifiers (aka: DIDs)

Standardization Status: Pre-standard specification, expected Working Group in early 2019 at World Wide Web Consortium

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 do cryptographic authentication using DIDs. That is, the organization can mathematically prove that the number is theirs via digital signatures.

DIDs were used in the NAFTA/CAFTA Proof of Concept to:

- Digitally sign Entry Summaries so that CBP knew who submitted the Entry Summary and that the Entry Summary had not been tampered with after submission.
- Digitally sign Requests for Information, so that Trade Partners knew that the request was coming from authorized CBP Personnel and had not been tampered with in transit.
- Digitally sign Information Responses, so that CBP knew that the data was coming from a specific trade partner and evidence had not been tampered with after submission.

1.2.3.2 Verifiable Credentials (aka: VCs)

Standardization Status: International Standards-track specification, expected ratification of standard mid to late 2019.

A Verifiable Credential is like a driver's license or social security card (the things one may carry around in their wallet). They are typically issued by an authority such as the DMV or the 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 NAFTA/CAFTA POC.

Verifiable Credentials were used in the NAFTA/CAFTA POC to:

Identify the Entry Filers, Importers, Brokers, Producers, and Exporters. While we just focused on company name and logo for the POC, it would be trivial to add mailing address, phone, email, and a variety of other corporate identity related information such as GS1 issued Legal Entity Identifiers or Global Location Numbers.

1.2.3.3 Object Capabilities (aka: OCAPs)

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

An Object 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.

Object Capabilities were used in the NAFTA/CAFTA POC to:

- Enable Trade Partners to create corporate post office boxes on their corporate systems where they stored trade secret information, like the Entry Summary details, Certificates of Origin, and supporting evidence.
- Provide keys to their corporate post office boxes to CBP so that only CBP could access trade sensitive information.

This security model enables Manufacturers, Importers, Producers and other participants in the supply chain to provide keys to CBP with respect to Entry Summary line item details without sharing that information with anyone else. It also allows 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 pre-standards in play, like Web Ledger, JSON-LD, RDF Dataset Canonicalization, Linked Data Proofs, and Linked Data Signatures, but the top three are the key enabling standards and pre-standards for the NAFTA/CAFTA Proof of Concept.

1.2.3.4 Mental Model Misconceptions

Since a number of the Trade Partners did not fully grasp the data model, and the use of standards was not entirely clear, they may believe that some things are possible in the near term that are not or that some problems remain unsolved when there was a technical demonstration that the technical problem was solved during the POC.

There are four misconceptions that we identified during the After Action Review.

The first misconception was around the concept of there being a large number of heterogeneous Blockchains that Customs and Border Protection and the Trade Partners could just “reach into”. Doing so would require data model standards, which we did make quite a bit of progress on during the POC, and Blockchain interaction protocols, which were not a primary focus during the POC. The Proof of Concept relied on gateway systems, such as the Trade Evidence Server, to translate information between Blockchain systems. That will most likely be the primary approach taken until there is more standardization in Blockchain communication protocols.

In order for generalized software to be written that enables CBP or Trade Partners to “reach into” any Blockchain, a series of standards would need to be created. The most difficult problems to solve are creating a standard Blockchain data model, standard Blockchain consensus algorithm, and then a standard Blockchain access protocol. While DHS S&T and Digital Bazaar have performed these activities through the Web Ledger Data Model, Web Ledger Protocol, and Continuity Consensus algorithm work, large industry players have not been receptive to the work yet due to the current “gold rush” mentality around the Blockchain ecosystem.

Announcements such as the ones that DHS S&T and CBP have been making regarding the need for standards in the space are forcing technology providers to take standards more seriously. That said, it will be many years before those standards are ratified. In the meantime, organizations will deploy proprietary Blockchain solutions. The strategy, if history is any indicator, will be to standardize the data shared between the “Blockchain gateways”, which is what this particular Proof of Concept focused on.

The second misconception related to Identity Management and that it remained an unaddressed problem. The Verifiable Credentials technology used during the Proof of Concept was designed to strongly authenticate the participants in the Blockchain. For the sake of implementation speed for the Proof of Concept, organizations self-issued their own organizational credentials. In a pilot or Production setting, the issuing authority would be a state or federal government or a set of organizations authorized to do identity proofing for organizations. Unfortunately, it seemed as if many of the Trade Partners did not realize that much of the technology to do this was fielded during the Proof of Concept.

The third misconception had to do with the inability of CBP to issue statements on the Blockchain that noted that a particular supplier meets the requirements of a particular Free Trade Agreement. This was possible during the Proof of Concept, as it could have been modeled as just another Verifiable Credential. Thus it seemed as if many of the Trade Partners and CBP did not realize how flexible the technology stack was and what was enabled by the data model and technology that was proposed.

The fourth misconception had to do with who would operate the Blockchain network. Trade Partners seemed to assume CBP would and CBP seemed to assume that Trade would help run the network. It was also not clear who would pay for the operation of the network. Based on the desired interactions, we would suggest that a government-private industry partnership, perhaps operated as a non-profit consortium could run the NAFTA/CAFTA Blockchain network. Access to the network would be fee-per-transaction based and authorized by CBP. The per transaction fees would be used to compensate organizations running nodes on the network, pay for software licensing and development, and would maximize cost sharing when operating the network. This would most likely result in the lowest cost for CBP and Trade Partners in operating the network and enable the network to rapidly go into a production capacity.

1.3. Conclusion

In summary, we believe that the POC achieved the goals that were identified at the beginning of the project, garnered more participation than we had predicted, attracted more press than we expected, and provided a number of lessons that would benefit any future CBP Blockchain Proof of Concept in the space.

Digital Bazaar - Recommendations

2.1. Lessons Learned

The list below is a summary of the lessons learned during the POC and has been condensed from the previous sections regarding Key Outcomes.

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. 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. Many participants 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.
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.
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.

2.2. Next Steps

The following next steps are recommended:

1. Gather all assessment feedback and distribute to the participants and broader COAC.
2. Determine which pre-standards are critical to the future of this system and continue to publicly support and test those pre-standards.
3. Perform a legal and regulatory evaluation of the project and what would be needed to proceed from those standpoints.
4. Perform a technical evaluation of the project and determine what would be changed from the current POC software to transition into a pilot program.
5. Reconvene the group in 2-6 months to determine if a pilot program is warranted given the legal, regulatory, and technical evaluations.

2.3. Suggestions for Pilot Phase

While the POC identified a number of advantages when utilizing Blockchain technology for the purposes of information sharing among Trade Partners, it was simple in nature and a pilot program would need to address at least the following items that the POC did not address, namely:

1. Ensure that the Blockchain is capable of supporting two to three times the full yearly load of information that would be expected to be processed if adopted by industry.

2. Ensure that the data model is expanded to support more use cases, noting that cost efficiencies are gained as the Blockchain supports more use cases. Use cases not supported by the Blockchain will inevitably require a separate Blockchain to support the use cases.
3. Ensure that the interfaces to the Trade Evidence Server support any new use cases.
4. Ensure that the group of organizations that have consensus authority (e.g. US Government + a number of trade partners) on the Blockchain are well understood.
5. Ensure that the economics of operating the Blockchain are sound. Specifically, ensure that costs are shared equitably among those that utilize the Blockchain and do not result in excessive costs or burden to CBP or Trade Partners.

2.3.1 Blockchain Economics and Adoption Scenarios

It is important to note that direct Blockchain to Blockchain interoperability is still many years away. While Veres Delta, the Blockchain deployed for this POC, was built entirely on open standards or pre-standards specifications, many other Blockchain platforms in the space are not built in this manner. The development teams in charge of many Blockchain projects will take years to become convinced to adopt standards as there are market pressures, such as Initial Coin Offerings and proprietary lock in, that drive anti-standards behavior. This creates near-term adoption and economic concerns around Blockchain ecosystems.

2.3.1.1 The Blockchain "Gold Rush" Mentality

The systems design approach we have taken in the short term is to assume a "gold rush" mentality among software vendors. This mentality presumes that software vendors will only adopt standards as a last resort, after their attempts to lock customers in to proprietary technologies eventually start to fail. There are customers in the space, such as in the financial services industry, that view proprietary systems as a competitive advantage and are quick to become locked into software vendor ecosystems if the short term benefits are financially compelling. These cycles can take a decade or more to play out.

As such, the CBP POC was architected to be composed of a series of loosely coupled Blockchain systems. The loose coupling was provided by a data translation system, as implemented by the Trade Evidence System, which enables multiple different types of Blockchains to interact with each other without having to adopt the full stack of Blockchain standards necessary to do direct Blockchain-to-Blockchain interaction.

2.3.1.2 Loosely Coupled Blockchain Systems

This systems design approach is the same as the one that is used to connect multiple proprietary back-end corporate systems together today and has a 30+ year track record of enabling a path toward standardization without forcing organizations to move faster than they are capable of moving and thus delaying the benefits of the new technology to the ecosystem at large.

Fundamentally, an organization using an HTTP API to connect to a remote system doesn't care if the remote system uses an Oracle database, an IBM Blockchain, or a Veres Delta fit-for-purpose Blockchain. One of the most important things the organization accessing the remote system cares about is if the data comes back in a way that they can understand. The most important part of interoperability is a shared data model and lightweight protocols to exchange that core data model. This is the sort of interoperability that we achieved during this POC.

2.3.1.3 The Source of Truth and System Costs

The “NAFTA/CAFTA Blockchain” built during the POC established the source of truth for CBP and the Trade Partners that participated in the Blockchain. It was a point of coordination among all parties, only stored public data, and provided pointers to off-chain private data held in Trade Evidence Systems entirely owned and operated by each Trade Partner. This is a common design pattern in Blockchain systems and as such, the question of how that single source of truth operates and is funded is an important question to explore when discussing how the POC system progresses to a pilot.

With respect to who operates the source of truth, we suggest that a joint public-private partnership operates the ledger. This ensures that no one party shoulders the burden for the others, costs are controlled and shared through per-transaction fees that everyone pays, and consensus and high-availability are achieved by sharing the load among all parties that rely on the Blockchain.
With respect to who the technology provider is for the Blockchain, cross-Blockchain consensus remains an unstandardized aspect of Blockchains, which currently makes it impossible for two different technology providers to both offer Blockchain node software for the same Blockchain, such as the “NAFTA/CAFTA Blockchain”. The Veres Delta platform is the only Blockchain that we know of that has standards and pre-standards developed for every aspect of the Blockchain software, including the consensus algorithm. This provides a path toward having multiple technology providers eventually providing interoperable Blockchain-to-Blockchain software if they build towards the standards.

These realities provide a number of avenues forward for a near-term pilot program with respect to who builds and maintains the system:

1. CBP decides to build and operate, either from scratch or by licensing existing technology, the NAFTA/CAFTA Blockchain as a US Government system. All costs of building and running the software would be shouldered by CBP. Prices would be determined by CBP.
2. A software vendor builds and operates the NAFTA/CAFTA Blockchain as a private system. All costs of building and running the software would be shouldered by that organization, with costs passed on to all participants that depend on the Blockchain. Prices are determined by the software vendor.
3. CBP and Trade create a public-private partnership that refines the software developed during the Proof of Concept. All costs of building and running the software would be shared by all participants that depend on the Blockchain. Prices are determined by the public-private partnership.

Of these three approaches, we believe the third choice will result in the most cost effective system in the long term with a balanced and transparent governance structure.