University of British Columbia
Records in the Chain Project

Title and code:		**Real Estate Transaction Recording on the Blockchain in British Columbia (RCPCA-02) – Case Study 1**
Document type:		Case Study
Status:		Pre-press
Version:		0.15
Research domain:		N/A
Date submitted:		March 18, 2018
Last reviewed:		July 7, 2018
Author:		Records in the Chain Project
Writers:		Alysha Joo, University of British Columbia Victoria Lemieux, University of British Columbia Darra Hofman, University of British Columbia
Test bed participants:		Land Title and Survey Authority of British Columbia (LTSA)
Research team:		**University of British Columbia** Alysha Joo, University of British Columbia Crystal Song, University of British Columbia Sean Burke, University of British Columbia Victoria Lemieux, University of British Columbia **Digital Identity and Authentication Council of Canada** Joni Brennan, President Tom Wolf, Director of Operations Heather Flanagan, Program Coordinator **LTSA** Connie Fair, President & Chief Executive Officer Al-Karim Kara, Vice President, Business Innovation & Chief

		Information Officer **LandSure Systems (subsidiary of LTSA)** Jonathan Oliver, Software Application Engineer Henry Lio, Customer Support Specialist **IdentityNORTH** Aran Hamilton, Co-Founder & Chair of IdentityNORTH and President & Co-Founder at Vantage Lauren Skipper, Event & Marketing Lead/Executive Partner at IdentityNORTH & Vantage Krista Pawley, Principal, Culture & Reputation Architect at Imperative Impact - Reputation by Design

Document Control

Version history			
Version	Date	By	Version notes
0.1	February 17, 2018	Alysha Joo Victoria Lemieux	First draft in English
0.2	March 6, 2018	Alysha Joo	Edits and additions to the February 17 draft in English
0.3	March 7, 2018	Darra Hoffman	Edits to the February 17 draft in English
0.4	March 18, 2018	Victoria Lemieux	Edits and additions to the March 6 draft in English
0.5	March 29, 2018	Victoria Lemieux	Edits and additions to the March 18 draft in English
0.6	June 13, 2018	Victoria Lemieux	Edits and additions to the March 29 draft in English
0.7	June 21, 2018	Alysha Joo	Edits and additions to the June 13 draft in English
0.8	June 26, 2018	Alysha Joo	Edits and additions to the June 21 draft

		Al-Karim Kara Joni Brennan	in English
0.9	June 27, 2018	Alysha Joo	Edits and additions to the June 26 draft in English
0.10	June 28, 2018	Alysha Joo	Edits and additions to the June 27 draft in English
0.11	June 29, 2018	Alysha Joo	Edits and additions to the June 28 draft in English
0.12	June 30, 2018	Alysha Joo	Edits and additions to the June 29 draft in English
0.13	July 7, 2018	Alysha Joo	Edits to the June 30 draft in English
0.14	July 8, 2018	Victoria Lemieux	Review of July 7 draft and minor edits
0.15	August 1, 2018	Al-Karim Kara Alysha Joo Victoria Lemieux	Final review and minor edits.

Table of Contents

Abstract

This document reports on a design challenge competition proposed by the Digital ID & Authentication Council of Canada (DIACC) and the Land Title and Survey Authority of British Columbia to offer students and professionals the chance to contribute ideas for a real world, industry application of digital identification in the context of land title transfers within the Canadian province of British Columbia. The design challenge was a collaboration between DIACC, the Land Title and Survey Authority of British Columbia, IdentityNORTH, and the University of British Columbia.

A. Overview

This case study reports on a Digital Identity Design Challenge competition that ran from August to November 2017.

What is a Digital ID Design Challenge (DIDC)?

A Digital Identity Design Challenge (DIDC) is a competition proposed by the Digital ID & Authentication Council of Canada (DIACC) to offer students and professionals the chance to contribute ideas for a real world, industry application of digital identification.

Created as a result of the federal government's Task Force for the Payments System Review, the DIACC is a non-profit coalition of public and private sector leaders committed to developing a Canadian digital identification and authentication framework to enable Canada's participation in the global digital economy**.**

The DIACC's objective is to unlock societal and economic opportunities for Canadians by providing the framework to develop a robust, secure, scalable and privacy enhancing digital identification and authentication ecosystem that will decrease costs for governments, consumers, and businesses while improving service delivery and driving GDP growth.

IdentityNORTH sponsored the event and shared in the cost of funding prizes for the Challenge in order to support its mandate of driving engagement on the topic of digital ID.

Digital ID Design Challenge (DIDC): Electronic State of Title Certificates (eSTC)

The DIDC: eSTC, was a virtual competition hosted by DIACC, in collaboration with the Land Title and Survey Authority of British Columbia (LTSA), IdentityNORTH (IDN) and the University of British Columbia's Blockchain Research and Education Cluster (Blockchain@UBC). Broadly, the purpose of the DIDC was to explore the following research questions:

1. Was blockchain technology a suitable technology to be used to innovate the business processes of the LTSA?
2. What might be the social, legal and business implications of applying blockchain technology to innovate the business processes of the LTSA?

The collaboration between LTSA, DIACC and IdentityNORTH recognized that the one critical piece missing for Blockchain to be used for legitimate business purposes is identity authentication. Blockchain transactions use public key cryptography, relying on the use of a private key to digitally sign transactions (i.e., authorize them). However, private keys are not linked to "real-world" identities, making blockchain transactions pseudonymous. For some applications of blockchain technology, this is an attractive feature (i.e., cryptocurrency applications). In the context of recording land transactions, on the other hand, it is critical to connect the private key used to authorize a transaction with a real-world identity.

In order to explore the above research questions, Blockchain@UBC worked with the LTSA, DIACC and IDN to develop and deliver a virtual competition; the design challenge, which focused on generating well-designed ideas relating to the application of identity management and blockchain technology. The design challenge was expected to generate knowledge for LTSA regarding possible applications, future designs, and the social, legal and business implications of blockchain technology for the LTSA's operations and the registration of land titles in BC.

Between the months of August and November 2017, the planning, organization, and execution of the DIDC occurred. During this time, weekly conference calls were held between the organizing team of the DIDC to plan and organize this virtual design challenge. The timelines for the project were approximately:

- September 15: Website launched
- September 24: Use case for the DIDC announced
- September 30: Judges committee was formed
- October 24: Submissions were due from participants
- October 31: Judges selected 2 groups to present at IDN and 2 honorable mentions
- November 7: The 2 groups presented their solutions at IDN.
- November 8: IDN attendees voted on the grand prize winner, with this vote being added to the judges score.

For the DIDC, participants were asked to research and develop solutions to the problem of how digital identification can improve and simplify the process of accessing and distributing electronically delivered state of title certificates (eSTC). Participants were challenged to remove the friction of digital identification within this specific use case, while identifying options of extending to other real estate use cases and exploring the potential of blockchain technology related to the proposed challenge.

A total of 15 teams from around the world registered for the DIDC, and nine teams submitted solutions for the proposed challenge. Two finalists were selected and invited to present their solutions at the IdentityNORTH Western Forum on November 7th, 2017. The solutions were judged by three industry experts: Joni Brennan (DIACC), Aran Hamilton (IdentityNORTH), and Al-Karim Kara (LTSA), and in addition, the audience of the IdentityNORTH Western Forum contributed votes in order to select a winner on November 8th. Each of the judges had 25% of the vote for a combined judging power of 75%, while the audience functioned as a fourth judge with 25% of the vote. Noah Bouma, Founder of OnePair, was selected as the winner, and Alphabeta; a team comprised of Matthew Gaiser, a Computer Engineering student from Queen's University and Mike Brown, Director of Innovation at ATB Financial, were selected as the runners up.

Organizing Team Members of the DIDC: eSTC

The organizing team of the DIDC: eSTC was composed of members from the DIACC, the LTSA, LandSure Systems Ltd. (a subsidiary of LTSA), IdentityNORTH, and Blockchain@UBC. The participants and stakeholders who assisted in the organization and planning of the virtual design challenge were:

DIACC

- Joni Brennan, *President*
- Tom Wolf, *Director of Operations*
- Heather Flanagan, *Program Coordinator*

LTSA

- Connie Fair, *President & Chief Executive Officer*
- Al-Karim Kara, *Vice President, Business Innovation & Chief Information Officer*

LandSure Systems (subsidiary of LTSA)

- Jonathan Oliver, *Software Application Engineer*
- Henry Lio, *Customer Support Specialist*

IdentityNORTH

- Aran Hamilton, *Co-Founder & Chair of IdentityNORTH and President & Co-Founder at Vantage*
- Lauren Skipper, *Event & Marketing Lead/Executive Partner at IdentityNORTH & Vantage*
- Krista Pawley, *Principal, Culture & Reputation Architect at Imperative Impact - Reputation by Design*

Blockchain@UBC

- Victoria Lemieux, *Cluster Lead*
- Sean Burke, *Director of Research Facilitation & Operations*
- Alysha Joo, *Graduate Research Assistant*
- Crystal Song, *Undergraduate Research Assistant*

Case Study Goals

The DIDC also functioned as an opportunity to reflect upon the broad research questions and objectives of the University of British Columbia’s “Records in the Chain” project, led by. Dr. Victoria Lemieux. This report, therefore, forms part of a series of case studies under the auspices of that project which aims to describe:

- How the Blockchain solutions were proposed to be used
- What Blockchain platform the solutions used
- How the Blockchain solutions proposed to use the LTSA records and information
- How the Blockchain solutions were designed to operate
- How the Blockchain solutions were designed to work under the law
- How the Blockchain solutions could affect the citizens of British Columbia
- How the Blockchain solutions could affect the trustworthiness and long-term preservation of records

As the DIDC was a design challenge, this report is only able to discuss aspects of the designs and their proposed operation/implementations which were presented.

B. Statement of Methodology

The research was carried out under the overall direction of Dr. Victoria Lemieux of the University of British Columbia. The analysis was carried out by Alysha Joo, a UBC Master of Archival Studies and Master of Library and Information Studies student, supported by input from Darra Hofman, doctoral student in Archival Studies, Sean Burke, Director of Research Facilitation and Operations at Blockchain@UBC, and Victoria Lemieux. Development of this report entailed a review of documentation used to prepare for the DIDC as well as documents submitted by competition participants.

C. Description of Context

1. Provenancial

Test-bed Name

- Land Title and Survey Authority of British Columbia (LTSA)

Location

- British Columbia, Canada

Origins of the Test Bed

The Land Title and Survey Authority of British Columbia (LTSA) maintains British Columbia's official legal record of private property ownership. The LTSA delivers secure titles through timely, efficient registration of land title interests and survey records. The services the LTSA provides are essential to BC's private property market and the civil justice system, as well as to BC's civic governance, taxation and Crown land management frameworks.[1]

2. Juridical-Administrative

LTSA is a publicly accountable, statutory corporation formed in 2005 and responsible for operating the land title and survey systems of British Columbia.[2] As adapted from the BC Government Website, the LTSA has three main service areas of responsibility:

- Land Titles: ensures the integrity of the Torrens-based land title system for registering land titles, and interests in titles such as mortgages and other charges
- Land Surveys (Surveyor General): maintains the quality of the Province's land survey structure
- Crown Grants: issues Crown grant documents that transfer Crown land into private ownership, to support government's Crown land allocation programs[3].

[1] See, https://ltsa.ca/about-ltsa/ltsa-mandate.
[2] Ibid.
[3] See, https://www2.gov.bc.ca/gov/content/industry/natural-resource-use/land-use/crown-land/legislation-agreements/land-titles-surveys.

3. Legal

The LTSA is subordinate to the provincial government of British Columbia. The province establishes the mandate, responsibilities and performance standards of the LTSA in the *Land Title and Survey Authority Act* and an *Operating Agreement* with the government.[4] It is crucial to understand that the LTSA is not an agent of the BC government, except in situations when executing a Crown grant under the *Land Act*, or within written agreement with the government.[5]Additionally, LandSure Systems Ltd. is a subsidiary of the LTSA, which develops and operates the technology of the LTSA to enable land-related transactions[6]. The Ministry of Forests, Lands and Natural Resource Operations, on behalf of the province of British Columbia, is responsible for the development and implementation of policy and legislation to govern the land titles and survey systems, which in addition, oversees the following legislation: *Land Title and Survey Authority Act*, *Land Title Act*, *Land Survey Act*, *Land Surveyors Act*, *Boundary Act*, *Land Title Inquiry Act*, *Land (Spouse Protection) Act*, and *Land Transfer Form Act*[7].

A land title refers to the ownership of land, which is documented by registration through the LTSA. Once registered, the LTSA issues a Certificate of Title, which represents legal title to land for the named owner.[8] A registered title is conclusive evidence of the ownership of that land. This type of land title registration system is known as a Torrens system.[9] Additionally, land titles show legal interests or encumbrances which much be formally registered against a title by the LTSA. Common charge types include: mortgages, statutory rights of way, easements, covenants, judgements, leases and Claims of Builders Liens[10].

A title that is indefeasible cannot be defeated, revoked or made void[11], because the evidence of the right to land ownership is established by a registered indefeasible title in the land register, which includes the name of the owner and the names of others who have interests in the

[4] See, https://ltsa.ca/about-ltsa/ltsa-mandate.

[5] See section 2(5) of the *Land Title and Survey Authority Act*, http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_04066_01.

[6] See, http://www.landsure.ca/who-we-are.

[7] See, https://www2.gov.bc.ca/gov/content/industry/natural-resource-use/land-use/crown-land/legislation-agreements/land-titles-surveys.

[8] See, https://ltsa.ca/help/what-does-it-mean-have-title-land-british-columbia.

[9] Greg Taylor (2008). *The Law of the Land: The Advent of the Torrens System in Canada*. Toronto: University of Toronto Press for the Osgoode Society for Canadian Legal History. pp. 31 seq., 221. The land title system of British Columbia is based on the Torrens registry system and is considered one of the best in the world[9]. The Torrens registry system was first adopted in the Colony of Vancouver Island in 1861, which the Colony of British Columbia adopted shortly after. During that time, the Colony of Vancouver Island was the second jurisdiction in the world to adopt a Torrens land title registration system. Presently, many countries around the world as well as provinces in Canada are using the system or are in the process of moving towards a land registration system based upon Torrens principles [See, https://ltsa.ca/about-ltsa/history-bcs-land-title-system.].

[10] See, https://ltsa.ca/property-information/what-information-title.

[11] See, https://ltsa.ca/practice-information/title-security-bc.

property. In order to establish an indefeasible title, documents which transfer legal ownership or create an interest in land must be filed and registered at the Land Title Office. Even though registration is not mandatory in British Columbia, failure to register means that ownership or interests claimed cannot be enforced by a third party (i.e., LTSA).[12] There are a limited number of exceptions to the principle of indefeasibility, as outlined in section 23 of the *Land Title Act.*[13]

With the abolition of the "doctrine of notice" in the Torrens system, a person is entitled to rely on the land register for proof of ownership and interests instead of having to pursue an inquiry into the validity of a title or interest.[14] However, there are exceptions as described in section 29 of the *Land Title Act.*[15] Furthermore, because the land title registration system is said to be conclusive, since the government or its agent guarantees an indefeasible title (i.e., LTSA), a land title is to be "assured".[16] This means that in the unlikely event that property owners are affected by a title registration error or they become the victim of land title fraud, there is an Assurance Fund which compensates their losses.[17]

The legal basis of a state of title certificate is found under s. 378(1)(a) of the *Land Title Act*. Ultimately, it is codified in law that the Director of Land Titles, as appointed by the CEO of the LTSA, has the authority to "approve the form of an instrument, document or notice that is to be registered, deposited, filed or given under this Act"[18], which also includes recognizing the designation of electronic form for instruments, documents or notices (e.g., State of Title Certificate). Ultimately, an eSTC is considered authentic in terms of evidentiary matters pursuant to s. 379 of the *Land Title Act*.

Funding

All LTSA operations are funded from revenues earned from land title and survey services provided to customers. Service fees are established in compliance with the *Operating Agreement* with the provincial government of British Columbia. The terms of the *Operating Agreement* dictate a revenue sharing arrangement with the Province of British Columbia. Additionally, net earnings are ultimately re-invested in order to achieve land title and survey public policy objectives.[19]

[12] See pg. 24-25, http://www.ltsa.ca/docs/Why-BC-Property-Owners-Sleep-Soundly-at-Night.pdf.

[13] See section 23 of the *Land Title Act*, http://www.bclaws.ca/civix/document/id/complete/statreg/96250_03#section23.

[14] See pg. 24-25, http://www.ltsa.ca/docs/Why-BC-Property-Owners-Sleep-Soundly-at-Night.pdf.

[15] See section 29 of the *Land Title Act*, http://www.bclaws.ca/civix/document/id/complete/statreg/96250_03#section29.

[16] See, https://ltsa.ca/about-ltsa/history-bcs-land-title-system.

[17] See, https://ltsa.ca/practice-information/title-security-bc.

[18] See section 9(2) of the *Land Title Act*, http://www.bclaws.ca/civix/document/id/lc/statreg/96250_02#section9.

[19] See, https://ltsa.ca/help/how-ltsa-funded.

Resources (Physical)

With respect to its facilities, the LTSA has several offices across the Province, located in Victoria, New Westminster, Kamloops, and Vancouver. The head office is located in Victoria, BC.[20]

Human Resources

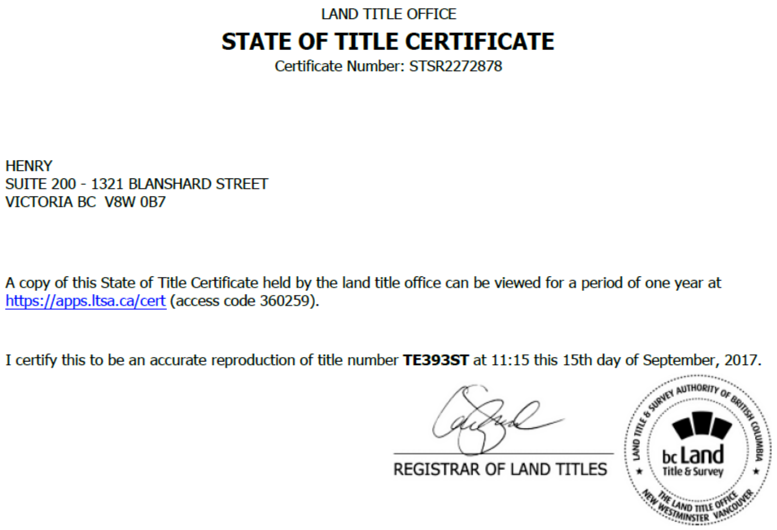
As of June 2017, the LTSA had 152 personnel in their employ.[21]

4. Procedural

A State of Title Certificate (STC) is a certified copy of a land title that is processed by the land title office (the LTSA)[22]. Customers can request State of Title Certificates (STCs) be delivered electronically, by regular mail or by picking it up at the land title office. A STC includes a unique nine-digit parcel identifier (PID), a legal description (a textual unique identifier for each parcel of land in the province that generally includes lot number, plan number, survey system identifiers (e.g., Section, Range, Township, District Lot, District, etc.), the registered owner(s) of title, registered owners of interests in land and various legal notations.

The following details the process of an electronically delivered State of Title Certificate, in other words, an Electronic State of Title Certificate (eSTC).

When a request for a certificate to be delivered electronically is processed, the customer is granted access to a secure PDF of the eSTC containing the Registrar's seal (**Figure 1**), with access valid for 7-days.



LAND TITLE OFFICE

STATE OF TITLE CERTIFICATE

Certificate Number: STSR2272878

HENRY
SUITE 200 - 1321 BLANSHARD STREET
VICTORIA BC V8W 0B7

A copy of this State of Title Certificate held by the land title office can be viewed for a period of one year at https://apps.ltsa.ca/cert (access code 360259).

I certify this to be an accurate reproduction of title number **TE393ST** at 11:15 this 15th day of September, 2017.

REGISTRAR OF LAND TITLES

LAND TITLE & SURVEY AUTHORITY OF BRITISH COLUMBIA
bc Land Title & Survey
THE LAND TITLE OFFICE NEW WESTMINSTER VANCOUVER

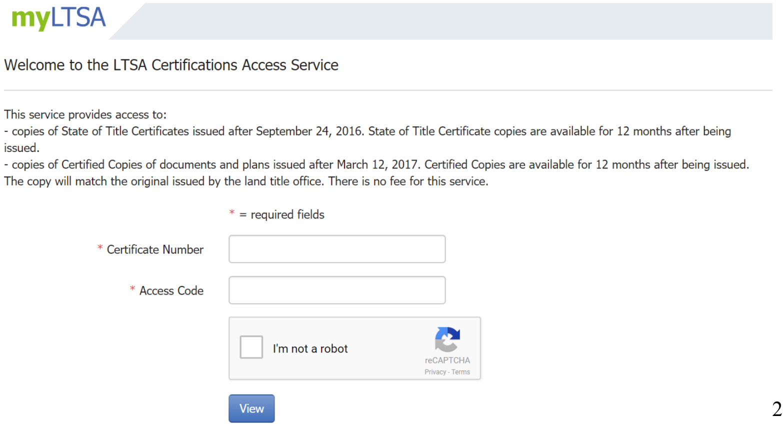
[23]

Figure 1. An example eSTC.

[20] See, https://ltsa.ca/sites/default/files/LTSA-Corporate-Fact-Sheet.pdf.
[21] Ibid.
[22] See, https://help.ltsa.ca/myltsa-enterprise/order-state-title-certificates.
[23] Sample eSTC provided by LTSA.

On the PDF of the eSTC, customers are provided a hyperlink to the LTSA Certifications Access Service. This service enables customers to share their certificates with third parties (e.g., a bank), as well as for third-parties to verify the contents of a certificate. Access to the LTSA Certifications Access Service does not require login and is available free of charge. However, to view a certificate online (**Figure 2**), a user requires:

1. A Certificate Number; and
2. The Access Code from the PDF (valid for 12-months from the date of issue)



Welcome to the LTSA Certifications Access Service

This service provides access to:
- copies of State of Title Certificates issued after September 24, 2016. State of Title Certificate copies are available for 12 months after being issued.
- copies of Certified Copies of documents and plans issued after March 12, 2017. Certified Copies are available for 12 months after being issued.
The copy will match the original issued by the land title office. There is no fee for this service.

[24]

Figure 2. LTSA Certifications Access Service.

The hyperlink to the LTSA Certifications Access Services on the PDF of the eSTC, and the hyperlink provided when viewing the eSTC as an inbox item in myLTSA, embeds the Certificate Number and Access Code, which when selected auto-populates the required information. After selecting the option to View, customers can then open or save the eSTC.

Problems with the Current Processes for Accessing, Sharing, and Verifying Electronic State of Title Certificates

Issue #1: Access

If a customer loses or misplaces the original PDF of the eSTC that was issued to them, the eSTC becomes inaccessible for the remaining time period during which it is valid (i.e., 12 months from the date of issue). This is because the Certificate Number and Access Code can only be found on the PDF. Further, the LTSA has no public facing mechanism that enables retrieval of the Certificate Number and Access Code after the eSTC is issued.

This can be problematic for both customers and the LTSA. Customers who are unable to access their eSTCs may have to submit (and pay for) a new eSTC. This creates dual inefficiencies for the LTSA: 1) LTSA staff receive related enquiries on how to recover their eSTC (which is not possible without access to the original PDF of the eSTC), and 2) lost certificates consume hard-drive space of the LTSA Certifications Access Service, because lost certificates will remain in

[24] Screenshot from the myLTSA website.

storage for the remainder of the 12 months period for which they are valid, even if the service is not being used.

Issue #2: Sharing

Before STCs were delivered electronically, they were originally delivered by mail. Third-parties such as banks and law firms identified the mail as coming from LTSA and trusted it to be authentic by the design or style of the certificate and often verifying the title search. With the move to eSTCs, customers have to access the eSTC and then email the hyperlink or the PDF to the third party. Or they can print out the PDF and deliver it in person or by mail. However, third-parties are not comfortable with electronically delivered STCs and still have a need for print for their internal records. For security reasons (e.g., authentication of individuals' identities), some third parties (e.g., law firms, banks) will not accept a printed-PDF copy of the certificate, or an email with the hyperlink or PDF.

5. Documentary

Historically, land titles were recorded in register books of "absolute fees" or indefeasible fees", but today, they are created and maintained electronically on a secure computerized system which is discussed further in this case study under section **6. Technological**[25]. Land title records from 1990 and onwards, as well as most documents and plans, are stored online and available electronically through LTSA's Search Services via myLTSA Enterprise or myLTSA Explorer accounts. However, land title records prior to 1990 are stored on microfilm or paper, and requests for these records incur extra fees for the provision of access. This is because direct access to original land title and survey records is limited only to LTSA employees and to those with direct access privileges including land surveyors, historical researchers and registry agents.[26] Traditionally, the privilege of "going behind the counter" and searching LTSA records has been given to lawyers, notaries public and land surveyors out of professional courtesy. This privilege has been extended to include title search agency employees, certain researchers and specified public servants over the years. For such persons to gain direct access privileges, LTSA requires a process of accreditation in order to respect records security and the protection of personal information.[27]

6. Technological

eSTCs are generated from the electronic land registry system and stored in a proprietary operational transaction database[28]; more specifically, eSTCs are stored via an application which writes them to disk and indexes them in a database. As previously described, eSTCs are requested and accessed through the myLTSA web portal. When an eSTC is retrieved, the application retrieves the eSTC from disk. Then another application which interfaces with the document storage application handles authentication and authorization to permit access to an eSTC.[29]

[25] See, https://ltsa.ca/property-information/what-information-title.
[26] See, https://ltsa.ca/practice-information/access-records.
[27] See pg. 4-6, https://ltsa.ca/sites/default/files/Direct-Access-to-Operational-Records.pdf.
[28] Type of database provided by Al-Karim Kara.
[29] Storage details regarding eSTCs provided by Jonathan Oliver.

D. Answers to the Project's Applicable Set of Questions

a. Analytic Framework

The following provides an evaluation of each of the proposed solutions submitted to the DIDC: eSTC using an emerging understanding of a blockchain solution reference architecture.[30] If a blockchain is present in the solution architecture, a breakdown of all of its components and how they interact will be identified following Lemieux's (2017) Generic Blockchain Recordkeeping Reference Architecture[31], as depicted in **Figure 3** and further explained below.

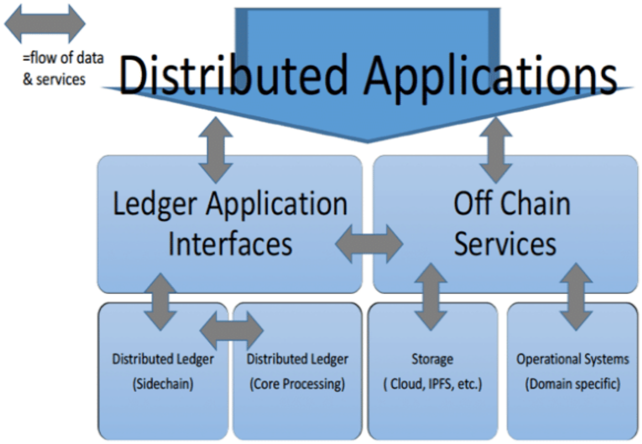

=flow of data
& services
Distributed Applications
Ledger Application Interfaces
Off Chain Services
Distributed Ledger (Sidechain)
Distributed Ledger (Core Processing)
Storage (Cloud, IPFS, etc.)
Operational Systems (Domain specific)

Figure 3. Generic Blockchain Record Keeping Reference Architecture.[32]

Distributed Applications (DApps)

- A DApp is a user-facing web-based application layer that reads or writes to other layers of the blockchain technology stack such as a the blockchain itself, or off chain services such as storage or operational transactional databases through application interfaces.[33]

Ledger Application Interfaces

- A blockchain or ledger application interface is an application which runs separately from the blockchain system that acts as a client to the DLT system, used by users or administrators.[34]

[30] There is, as of yet, no international standard reference architecture for blockchain technology, though one is under development by the International Standards Organization (ISO).
[31] Lemieux, Victoria L. "Blockchain and Distributed Ledger as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework," Proceedings of the Future Technologies Conference, Vancouver, Canada, November 29-30. IEEE, 2017.
[32] See, pg. 4 Lemieux's (2017).
[33] Ibid.
[34] See, pg. 11, Blockchain@UBC Research and Education Cluster (n.d.). "Key Blockchain Concepts." Contributors: Luciana Duranti, J.Z. Garrod, Victoria Lemieux, and Ning Nan.

Distributed Ledger (Sidechain)

- Sidechains are specialized, permissioned, and private blockchains that handle the processing of transactions of the "main" blockchain. Sidechains are utilized to improve the efficiency of processing transactions, as well as to allow flexibility to customize consensus mechanisms, smart contract capabilities, data capabilities, and other aspects of the operation of the blockchain-based recordkeeping service within the sidechain.[35]

Distributed Ledger (Core Processing)

- The main blockchain, is where transactions are bundled into blocks and cryptographically "hashed", and where the hash is put into the header of a proposed block, mined and propagated to the distributed network, thereby updating the blockchain.[36]
- Smart contracts are computer programs stored and distributed with the blockchain or distributed ledger.[37] Smart contracts usually have the ability to read and write through program interfaces to data stores separate from the blockchain.[38]

Off Chain Services - Storage (Cloud, IPFS, etc.) or Operational Systems (Domain Specific)

- Off chain access services provide secure means to access capabilities outside the blockchain system such as storage or operational transactional databases.[39]
- Generally, data representing transactional records are created off-chain in operational systems and usually stored off chain in a database or cloud-based repository, though distributed storage options are emerging.[40]

b. Competition Participants

Team Name: Union of Blockchain

- Person of Contact: Usman Mukaty, *UBC Student*
- Number of Team Members: 5
- Team Members:
    - Usman Mukaty, *UBC Student*
    - Alexander Lee, *UBC Student*
    - James Asefa, *UBC Student*
    - Joseph Thomas, *UBC Student*
    - Hudhaifah Zahid, *UBC Student*

Team Name: UBC iLab

- Person of Contact: Sanjeeva Rajapakse, *UBC Student*
- Number of Team Members: 3

[35] See, pg. 4, Lemieux (2017).
[36] Ibid.
[37] See, pg. 11, Blockchain@UBC (n.d.).
[38] See, pg. 4, Lemieux (2017).
[39] See, pg. 11, Blockchain@UBC (n.d.).
[40] See, pg. 4, Lemieux (2017).

- Team Members:
  - Alberto Cavalles, *UBC Student*
  - Nuwan Rajapakse
  - Sanjeeva Rajapakse, *UBC Student*

Team Name: Face-based Identity Authentication and Digital Signatures

- Person of Contact: Don Waugh, *Applied Recognition Ltd.*
- Number of Team Members: 1
- Team Members:
  - Don Waugh, *Applied Recognition Ltd.*

Team Name: OnePair Technologies

- Person of Contact: Noah Bouma, *OnePair Technologies Ltd.*
- Number of Team Members: 1
- Team Members:
  - Noah Bouma, *OnePair Technologies Ltd.*

Team Name: Credophy

- Person of Contact: Andrew Rose
- Number of Team Members: 3
- Team Members:
  - Andrew Rose, *Business*
  - Walid Al Habboul, *Simon Fraser University Student*
  - Davia Brown, *Business* (pending)

Team Name: Global Digital Cybersecurity Authority

- Person of Contact: Xiu Lei, *Global Digital Cybersecurity Authority CO., LTD*
- Number of Team Members: 4
- Team Members:
  - Wei Yicai, *Global Digital Cybersecurity Authority CO., LTD*
  - Lu Weilong, *Global Digital Cybersecurity Authority CO., LTD*
  - Zheng Huitao, *Global Digital Cybersecurity Authority CO., LTD*
  - Xiu Lei, *Global Digital Cybersecurity Authority CO., LTD*

Team Name: AlphaBeta

- Person of Contact: Mike Brown, *ATB Financial Ltd.*
- Number of Team Members: 2
- Team Members:
  - Mike Brown, *ATB Financial Ltd.*
  - Matt Gaiser, *Computer Engineering Student at Queen's University*

Team Name: Team Moe

- Person of Contact: Mohammad Afilal
- Number of Team Members: 1
- Team Members:
  - Mohammad Afilal

c. Competition Results

The following section provides a high-level overview of the competition results. The strengths and weaknesses of each solution reflect the judges' assessment of the solutions at the time of the competition (i.e., November 2017) using the judging rubric (**Appendix A**) and may not reflect more recent developments as blockchain technology development is fast-moving.

WINNER: OnePair Technologies

Team Members:

- Noah Bouma, *Developer and Proprietor of OnePair Technologies*

Name of Solution: OnePair

Description of Solution:

OnePair proposed a solution leveraging decentralized electronic certificate issuance, registration, presentation, and a verification scheme using a verifiable claims model while utilizing a blockchain as a registry.

Architectural Components:

The solution architecture is based on and adapted from a Twitter Thought Experiment[41] using verified claims, which was proposed by Tim Bouma and Anil John in 2017. The proposed solution architecture enables the use of independent apps to issue and register eSTCs through the LTSA App, store and present eSTCs through a Customer App, and verify eSTCs through a Third Party Verification App (**Figure 4**).

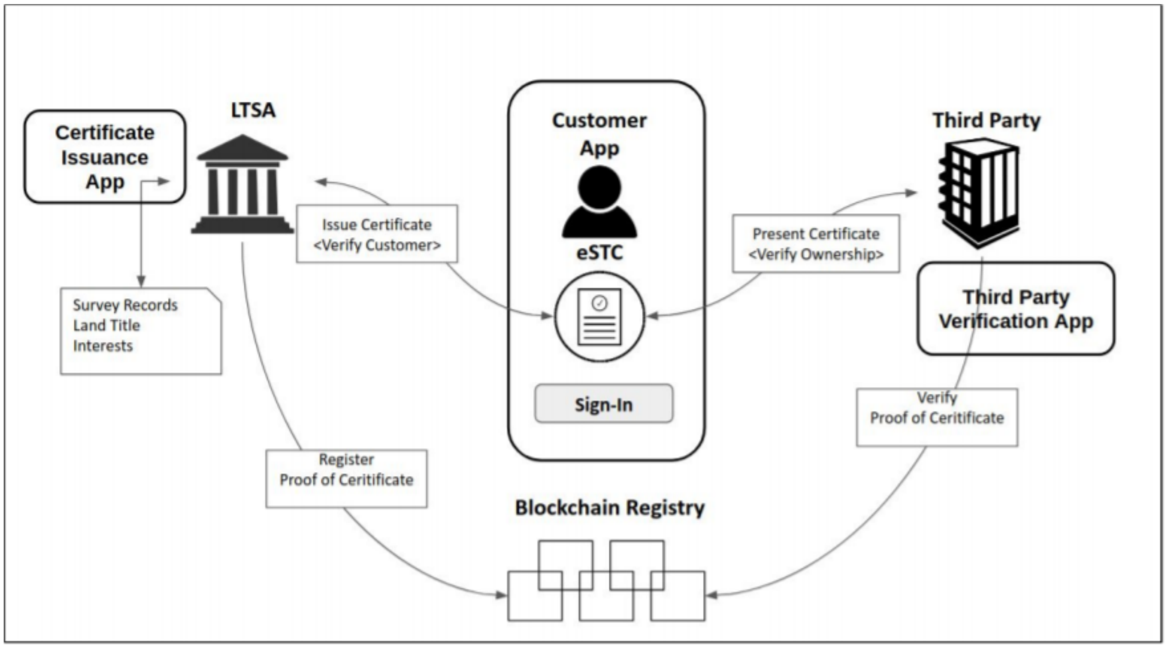


Figure 4. OnePair Solution Architecture.

[41] See, https://twitter.com/i/moments/888780606334787584.

Utilizing the Generic Blockchain Record Keeping Reference Architecture (**Figure 3**), the following components of the solution are identified:

DApps

- *Certificate Issuance App*

  This app would be used by the LTSA to generate certificates using registered land title and survey records using the Blockcerts[42] standard and open source software. Blockcerts gives control of a tamper-proof electronic certificate to the customers, who can present this certificate to any third party. Third parties can then independently perform their own verification of the certificate.

- *Customer App*

  This app is used by customers authorized by the LTSA, which is used to enforce the conditions of the customer agreement (e.g., signing in before requesting a certificate).

- *Third Party Verification App*

  This app is used by third parties (e.g., financial institutions) to validate the signature of the issuer and the certificate data, as well as to check the status of a certificate if it has expired or been revoked.

Ledger Application Interfaces

Blockcerts consists of open-source libraries, tools, and mobile apps for verification of proofs using blockchain technologies. These open-source components form all the parts needed for the operation and interoperability of the different parts of a blockchain ecosystem. Blockcerts, in turn, relies upon the following open standards: IMS Open Badges, W3C Verifiable Claims, W3C Linked Data Signatures, and W3C / Rebooting Web of Trust Decentralized Identifiers.

Blockchain/Distributed Ledger (Core Processing)

The blockchain or distributed ledger functions as a register of certificates. When a certificate is issued by the Certificate Issuance App, a one-way cryptographic hash is generated and anchored to the blockchain as a proof of issuance and to enable verification of the certification for third parties using a Third Party Verification App. OnePair recommends a public, permissionless blockchain (e.g., Bitcoin blockchain) for broadest access, however they also state that other blockchain platforms can be considered (e.g., Ethereum, Hyperledger).

Off Chain Services - Storage

- *Customer App*

  Certificate storage is managed via a cert-store library in the Customer App, which is a key-value storage for binary data that supports many backends. The actual certificates would be stored in a traditional file store (e.g., database) or a grid file store (e.g., MongoDB). Sharing options for certificate verification include email, secure file transfer, NFC, or QR code.

[42] See, https://www.blockcerts.org.

OnePair asserts that by utilizing the Blockcerts standard, there is no longer a requirement to retain a duplicate PDF of an eSTC in central storage (e.g., LTSA storage) since the certificate can be verified against its hash on the blockchain. However, the process of verification would entail having the LTSA send a requestor an eSTC. The requestor would have to retain a copy of the PDF of the eSTC in a file store to have the ability to forward a copy of it to any verifiers (e.g., banks) that want to establish who holds the title to a specific piece of land. The verifier would ascertain the authenticity of the eSTC by comparing a hash of it to a hash held on the blockchain.

Strengths:

- Addresses how to overcome customers' lost access to their eSTC through the use of Blockcerts anchoring proof of issuance of the certificate onto a blockchain.
- Uses the Blockcerts standard to cryptographically guarantee the integrity of the certificate electronically.
- Increases security and privacy for the LTSA by creating a decentralized validation service that uses zero personally identifiable information (PII) cryptographic proofs. Team OnePair points out that in the current system, that if someone gains access to the certificate number and access code, they can view the entire contents of the certificate, and that PDF certificates can be hacked and inserted with malware, or that hackers can use the link of a legitimate certificate in a fraudulent transaction. On the other hand, content of the certificate is public information and any verifying party can validate the eSTC by simply performing a title search.
- OnePair does not delve too deeply into proposing a solution for digital identification. OnePair suggests taking advantage of emerging standard-based authentication processes in the process of being implemented such as BC Services Card and My Alberta Digital Identity. OnePair argues that the LTSA should focus on first improving the processes of certificate issuance, distribution, and verification. Since the OnePair solution is built on open source standards, the LTSA services and apps would be able to evolve and adopt standardized digital identity and authentication services as they become available.

Weaknesses:

- Lack of clarity on where exactly eSTCs are stored via the Customer App, and devolution of the responsibility for the storage and backup of the eSTCs to the customer.
- Does not provide a detailed exploration of how blockchain technology would benefit (or not benefit) the current system for issuing, distributing, and accessing eSTCs, and how exactly it would interface with their proposed solution.

Links:

- Paper: https://diacc.ca/wp-content/uploads/2017/11/OnePair-Paper.pdf/
- Presentation: https://diacc.ca/wp-content/uploads/2017/11/OnePair-Preso.pdf
- Technical Overview Video: https://www.youtube.com/watch?v=lNkgLRtYCxk&feature=youtu.be

- Solution Overview Video: https://www.youtube.com/watch?v=YR3adjgH7iQ&feature=youtu.be
- Example eSTC with QR Code: https://docs.google.com/document/d/1vkishnZSUnxMNaLqLKmEYYXn9qZl8uE-EjhNy9R5clk/edit
- GitHub: https://github.com/boumba100
- Website: https://onepair.github.io/

RUNNER UP: AlphaBeta

Team Members:

- Matthew Gaiser, *Computer Engineering Student at Queen's University*
- Mike Brown, *Director of Innovation at ATB Financial*

Name of Solution: N/A

Description of Solution:

AlphaBeta's proposed solution leverages the Sovrin blockchain network[43], a free global public blockchain-based utility for sharing verified information. In 2017, the source code for Sovrin was donated by Evernym, a private for-profit company, to the Sovrin Foundation, who then contributed it to the Linux Foundation to become Hyperledger Indy.[44] Indy is now a community open source project in the Hyperledger family.[45] The Sovrin Foundation is a non-profit governed by 12 Trustees.[46] The legal foundation for the Sovrin Network is established by the Sovrin Trust Framework.[47] Stewards of the Sovrin network run the validator nodes of the Sovrin ledger and are individually qualified and approved by the Sovrin Board of Trustees.[48] Sovrin is entirely based on open standards. Evernym, Blockstack, uPort, Gem, Microsoft, and Digital Bazaar are contributing to the decentralized identifiers (DID) specification[49] at the W3C Credentials Community Group[50], and approximately 40 companies are contributing to the W3C Verifiable Claims Working Group.[51] AlphaBeta's solution proposed that LTSA would join the Sovrin network, and onboard other participants such as customers or banks.

[43] See, https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf.
[44] A discussion about the formation of the Sovrin Network can be found here: https://forum.sovrin.org/t/relationship-between-sovrin-and-evernym/390/3.
[45] See, https://www.hyperledger.org/projects/hyperledger-indy.
[46] See, https://sovrin.org/people/.
[47] See, https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Provisional-Trust-Framework-2017-06-28.pdf/.
[48] See, https://sovrin.org/stewards/.
[49] See, https://w3c-ccg.github.io/did-spec/.
[50] See, https://w3c-ccg.github.io.
[51] See, Ibid.

Architectural Components:

Utilizing the Generic Blockchain Record Keeping Reference Architecture (**Figure 3**), the following components of the solution are identified:

DApps

- *Customer Client App*

  The Customer Client App would be accessed through the LTSA web portal, and later a mobile app. It acts as an identity wallet that manages customer relationships between the LTSA, banks, lawyers and other third parties as necessary. Additionally, the Customer Client App has the ability to generate a PDF based on the eSTC data for third parties who require it.

Blockchain/Distributed Ledger (Core Processing)

- *Sovrin Identity Network*

  Team AlphaBeta plans to leverage an already existing global public blockchain for self-sovereign identity, which is public and permissioned. Anyone can obtain a Sovrin identity in which individuals or organizations own and control their own identities (i.e., self-sovereign identity management).

Off Chain Services - Storage

- *Customer Client App*

  eSTCs are stored on the Customer Client App. However, no further details about the storage mechanisms are provided.

Off Chain Services - Operational Systems (Domain Specific)

- *LTSA Agent Software*

  The existing system of the LTSA would be connected and managed through Sovrin interactions.

- *Third Party App or Agent Software*

  The Third Party App/Agent Software manages requests for eSTCs from customers. It also would have the ability to connect to existing data systems for the storage of eSTCs.

Strengths:

- Integrates with the current LTSA data system.
- Existing blockchain network infrastructure with no transaction fees (e.g., compared to the Bitcoin network).
- Security is handled by the Sovrin network with access controlled through APIs, which relieves the LTSA from building their own secure blockchain.
- Customers can revoke their proof at any time, thus giving them more control of their personal information.

- Eliminates centralized storage of the PDFs and reduces administrative efforts to manage access to PDFs since it puts control into the customers' hands.
- Potential of adding other related use cases to the Sovrin network, such as registering mortgage on a property, issuing property insurance on a home, as well as registering property owners with the local municipality.

Weaknesses:

- Viability of the Sovrin blockchain network is uncertain compared to other well-known blockchain networks (e.g. Bitcoin, Ethereum).
- Security is handled by the Sovrin network.

Links:

- Presentation: https://diacc.ca/wp-content/uploads/2017/11/AlphaBeta.pdf

HONORABLE MENTION: Union of Blockchain

Team Members:

- Hudhaifah Zahid, *Student*
- Alexander Lee, *Student*
- Usman Mukaty, *Student*
- Jamie Asefa, *Student*
- Joseph Thomas, *Student*

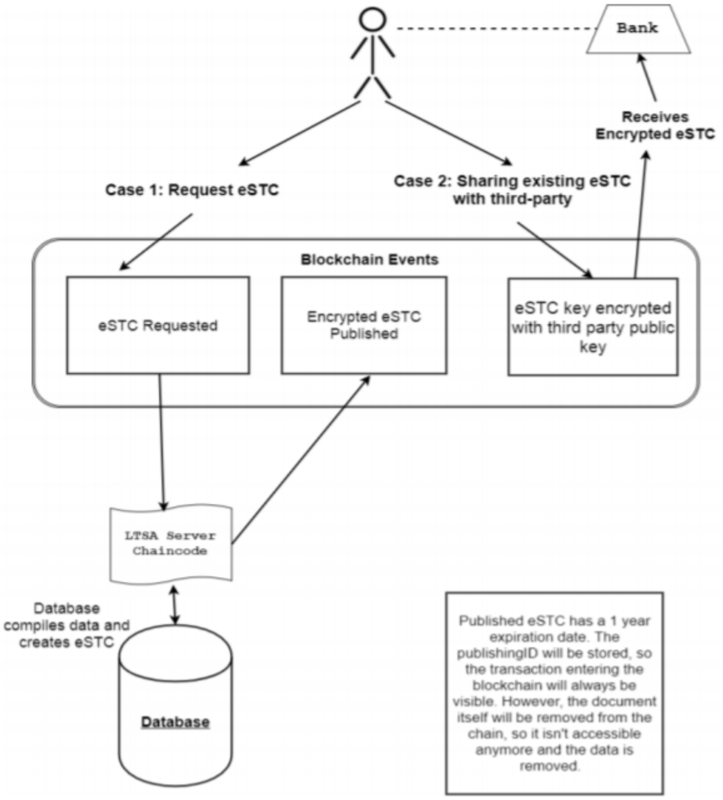
Name of Solution: N/A

Description of Solution:

The Union of Blockchain's proposed solution utilizes a permissioned blockchain implemented through Hyperledger Fabric[52], which functions as a ledger recording the creation and history of all eSTCs that have been issued. To participate on the blockchain network, every participant (e.g., customers or third parties) is required to create an account with the LTSA. The Union of Blockchain's proposed solution adjusts the process flow of eSTC retrieval, transaction, and verification for third parties, and focuses on maintaining the familiar customer experience of the current system.

[52] See, https://www.hyperledger.org/

Architectural Components:



Published eSTC has a 1 year expiration date. The publishingID will be stored, so the transaction entering the blockchain will always be visible. However, the document itself will be removed from the chain, so it isn't accessible anymore and the data is removed.

Figure 5. Architecture of Union of Blockchain's proposed solution.

Utilizing the Generic Blockchain Record Keeping Reference Architecture (**Figure 3**), the following components of the solution are identified:

Blockchain/Distributed Ledger (Core Processing)

- *Hyperledger Fabric*

  Tokens:

  The LTSA can add an eSTC to a token, in which the token as an asset contains details of ownership, the encrypted eSTC and other variables controlling access permissions to the eSTC.

  Transactions:

  Transactions are events which are executed by participants in the network. Transactions make changes to the ledger (i.e., change in ownership of a token). Different user types may have access to different types of transactions.

  Nodes:

  Nodes function as the identity layer in the blockchain, since in order to become a participant on the network, customers or third party users operating nodes are required to make an account with the LTSA. Permissions will be given to nodes to be able to read/write transactions, as well to create blocks on the blockchain through mining.

Chaincode (Smart Contracts):

Smart contracts give the ability to automate some processes. However, which processes can be automated are not specified in the solution.

Off Chain Services - Storage

- *Database*

  The LTSA database and server are used to create and publish the hashes of eSTCs to the blockchain.

Off Chain Services - Operational System

- *LTSA Website*

  Customer identities are created and managed through the LTSA website, which determines permission to join the blockchain network. Customer requests are made from their account and then published to the blockchain. Additionally, Union of Blockchain proposes to allow LTSA accounts to share eSTCs through the LTSA website. This way, third party institutions can verify the validity of eSTCs and trust the data since it is coming through the LTSA website.

Strengths:

- Expiration dates of eSTCs are built into the blockchain since all documents in the blockchain are tied to a block with a timestamp, and therefore, eSTCs can be expired based on time (e.g., 7 days, 6 months, 1 year, etc.). This automates the process for expiration and removal of eSTCs for the LTSA.
- No links or PDFs need to be accessed or shared outside of the system, which reduces the potential for malicious activities. This is because eSTCs are shared between trusted users on the LTSA blockchain.
- Integrable with the current LTSA database and web system.
- All participants must be verified against the standard outlined at minimum in the Medium Identification Level in BC's Identity Assurance Standard. [53]

Weaknesses:

- Identity needs to be verified by the LTSA in an unspecified manner.
- Customers are burdened to know and understand public key cryptography in order to encrypt the eSTC.

Links:

- Paper: https://diacc.ca/wp-content/uploads/2017/11/Union-of-Blockchain.pdf

[53] See, https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/identity_assurance_standard.pdf.

HONORABLE MENTION: Moe

Team Members: Mohammad Afilal

Name of Solution: Sawtooth Lake Solution

Description of Solution:

This solution proposes extending the LTSA Explorer into a blockchain consortium of LTSA authorized subscribers.

Architectural Components:

DApps

- *Extended LTSA Explorer*
  After submission of required documentation, users are assigned a wallet and select a specific verifier to confirm the validity of the person. Registered subscribers may verify identity of users on the system based on knowledge of the user and previous trust relationships.

Blockchain/Distributed Ledger (Core Processing)

- *Smart contracts*

  eSTCs are tokenized and sent to the blockchain consortium wallet that requested the document using a smart contract.

- *Sharing*
  The user specifies which enterprise user to which to send the eSTC, including length of time that the certificate will be available to the user and privacy settings. The user will send the eSTC to the enterprise user's wallet. The enterprise user will be able to see details about the user (sender) to verify that the user is the rightful property owner.
- *Hyperledger Sawtooth deployed on a Microsoft Azure Cloud*
  The solution proposes to be implemented on Hyperledger Sawtooth, which is described as being highly modular enabling flexibility in policy decisions. It relies on the Proof of Elapsed Time (PoET) consensus mechanism. Use of this consensus mechanism will support expiration of the eSTC, since PoET can be written into the transaction family code and tracked. Microsoft Azure Cloud is used for increased efficiency of system administration (e.g., consortium members can easily be added or dropped) and transaction throughput.

Strengths:

- Allows for privacy settings so users can specify which identity attributes will be shared with enterprise users (e.g., Banks, insurance companies, etc.).
- Allows for third parties to verify the identity of system users, based on previous trust relationships.
- Hyperledger Sawtooth is said to have several advantageous features:
  - It decouples the ledger from the transactions.

  - It incorporates the concept of Transaction Families which provides support for different data models and transaction semantics, making it extensible to many different business domains.
  - It has pluggable consensus which enables differing consensus protocols for both permissioned and non-permissioned networks.

Weaknesses:

- Sawtooth is not as well-specified and supported as Hyperledger Fabric or Indy.
- Processes for issuance, generation and verification of eSTCs are not fully specified.
- Approach may not work well with the LTSA's current business model because users can share eSTCs.
- Not truly decentralized as it uses MS Azure Cloud. It would have to introduce sufficient new functionality to justify the cost of acquiring MS Azure Services.
- Cross-border data flow/service reliance could be in conflict with data localization laws.
- Proposal to incorporate Microsoft's Coco Framework to improve network transaction speed, which has little to no adoption by other organizations to base success from.
- Solution provides no mechanism for reissuance/access to eSTCs if a user loses their private key because the solution relies on verification, which is similar to the current process of authentication for the LTSA.

Links: N/A

TEAM: Credophy

Team Members:

- Andrew Rose, *Business*
- Walid Al Habboul, *Academic Student SFU*
- Davia Brown, *Business*

Name of Solution: N/A

Description of Solution:

Team Credophy's solution proposes a semi-private blockchain system, that is under the control of the LTSA and third party participants certified by the LTSA, in which each LTSA office has a copy of the blockchain and controls the block mining process.

Architectural Components:

Utilizing the Generic Blockchain Record Keeping Reference Architecture (**Figure 3**), the following components of the solution are identified:

DApps

- *LTSA eSTC Application*

Third parties certified by the LTSA are qualified to use the LTSA eSTC application, which provides a copy of the LTSA blockchain to the third party.

Blockchain/Distributed Ledger (Core Processing)

- *LTSA Blockchain*

  The solution does not specify or recommend any particular blockchain platform to use. The solution proposes that the LTSA builds a semi-private blockchain, in which the LTSA controls the mining nodes while third party participants only have access to view the blockchain via the LTSA API.

- *Smart Contracts*

  eSTCs will be implemented as a smart contract within the blockchain system in order to track changes of state to the land title, and also to automatically expire an eSTC after a defined amount of time. The three states the smart contract will track are active, expired, and amended.

Off Chain Services - Operational System

- *LTSA Website*

  Customer creates an account and verifies their identity through the LTSA's website. Land title transactions are recorded onto the private LTSA blockchain.

Strengths:

- Method of verifying ID in person (Government ID number & PIN) is used to hash and encrypt an eSTC.
- Automatic expiration of eSTCs are built in through the use of smart contracts.

Weaknesses:

- Concerns about personal information of customers is at risk due to the utilization of smart contracts to represent land titles on the blockchain. Even though this is a private blockchain, all blocks and thus smart contracts are viewable to all participants in the network, even third parties with "view only" permissions.

Links:

- Paper: https://diacc.ca/wp-content/uploads/2017/11/Credophy.pdf

TEAM: Face Based ID

Team Members:

- Don Waugh, *Applied Recognition*
- Partners:

  Applied Recognition

  A Toronto-based company that has developed facial recognition for the authentication of customers utilizing photo IDs and digitally signed transactions. Enables customers to have control over their privacy and security.

  Blockchain Acuity

  A Vancouver-based consultancy and full stack development firm that builds custom solutions on a variety of different platforms such as Bitcoin, Ethereum, Ripple, and Hyperledger.

  Yongle Technologies

  A Vancouver-based company which developed the first platform for allowing a completely paperless new home sale from start to finish.

  Sourabh Siddharth

  A blockchain enthusiast and Software Engineer of Application Management and Services.

Name of Solution: Applied Recognition

Description of Solution:

The proposed solution leverages digital identification and authentication through face recognition technology to access and distribute eSTCs on a blockchain land title system.

Architectural Components:

The proposed solution did not provide enough detail to present a complete analysis of its architectural components and how they integrate.

Blockchain/Ledger Application Interfaces

There appears to be at least two different applications:

- *Photo ID Authentication & Document Signing*

  Identifies required authentication for the LTSA utilizing face and photo ID to automate authentication.

- *Acuity Wallet with Face Authentication*

  Authentication through facial recognition and authorizes transactions. The wallet stores eSTCs.

Blockchain/Distributed Ledger (Core Processing)

The solution mentions a non-specified blockchain platform but does not detail how the blockchain is to be used.

Strengths:

- Customer authentication is bound to an eSTC through digital signatures.

Weaknesses:

- The proposed solution does not recommend or specify a blockchain platform or how the blockchain is actually used.
- Concerns about the storage of biometrics.

Links:

- Paper: https://diacc.ca/wp-content/uploads/2017/11/FaceBased-ID.pdf

TEAM: Global Digital Cybersecurity Authority Co., Ltd. (GDCA)

Team Members:

- Xiu Lei, *Global Digital Cybersecurity Authority Co., Ltd.*
- Lu Weilong, *Global Digital Cybersecurity Authority Co., Ltd.*
- Zheng Huitao, *Global Digital Cybersecurity Authority Co., Ltd.*

Name of Solution: N/A

Description of Solution:

GDCAs proposed solution utilizes a mobile app to authenticate customers' identities, as well as a blockchain, in which the LTSA issues eSTCs, and third parties, after being authorized by the customers, can access and verify the eSTCs.

Architectural Components:

The proposed solution does not provide enough detail to present a complete analysis of its architectural components and how they integrate.

DApps

- *Mobile App (LTSA)*

  The LTSA provides customers this app in order to generate key pairs and send verification codes to the LTSA. The LTSA then receives the keys and wallet addresses of the customers, and binds them to authorization codes, which are used to digitally link a customer to the eSTC.

Blockchain/Distributed Ledger (Core Processing)

LTSA encrypts the eSTCs using the AES-CBC algorithm to get a Ciphertext. The LTSA then uses the digital certificate from the CA to digitally sign the Ciphertext. As a result, the LTSA uploads the Ciphertext, and its signature to the blockchain. Third parties can verify the signature through the LTSA's public key certificate and Ciphertext.

- *Smart Contracts*

  Smart contracts are used to securely send the Ciphertext of an eSTC to third parties automatically, as depicted in **Figure 6**.

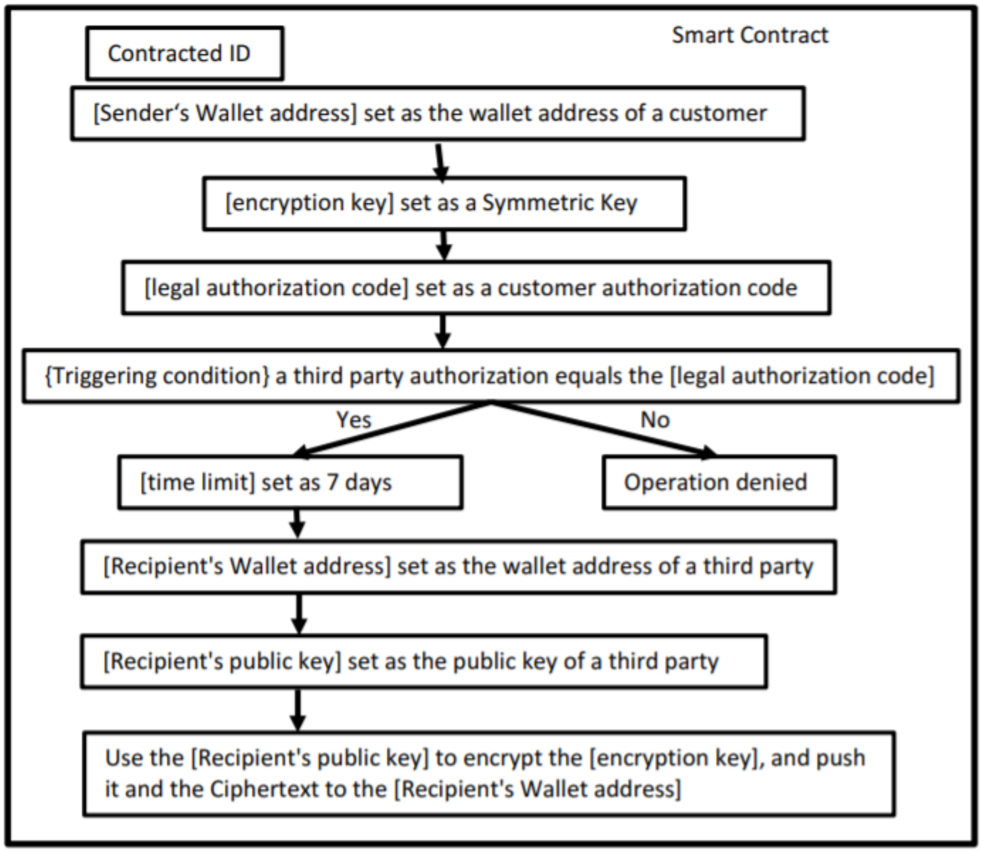

Smart Contract
Contracted ID
[Sender's Wallet address] set as the wallet address of a customer
[encryption key] set as a Symmetric Key
[legal authorization code] set as a customer authorization code
{Triggering condition} a third party authorization equals the [legal authorization code]
Yes
No
[time limit] set as 7 days
Operation denied
[Recipient's Wallet address] set as the wallet address of a third party
[Recipient's public key] set as the public key of a third party
Use the [Recipient's public key] to encrypt the [encryption key], and push it and the Ciphertext to the [Recipient's Wallet address]

Figure 6. Smart Contract Architecture & Process.

Strengths:

- Customer authentication is bound to an eSTC.
- Ensures the integrity of the eSTC by digitally signing it to the blockchain.

Weaknesses:

- Solution does not recommend or specify a blockchain platform or indicate whether the blockchain is public or private
- No app or web portal described for how 3rd parties verify a customer's eSTC.
- Remote ID authentication not further explained (e.g. is it a feature of the mobile app provided by the LTSA?)

Links:

- Paper: https://diacc.ca/wp-content/uploads/2017/11/GDCA.pdf
- Website: https://www.gdca.com.cn/

TEAM: UBC Bitcoin

Team Members:

- Yori Ding, *Psychology at UBC*
- Stephen Thompson
- Jagriti Sona Sharma, *Combined Major in Computer Science & Business at UBC*
- Calvin Chu, *Commerce at UBC*
- Joshua Matettore, *Candidate Masters in Law - Law and Technology*

Name of Solution: N/A

Description of Solution:

The UBC Bitcoin Club proposes two solutions to address the use case. The first solution leverages Hyperledger frameworks and toolsets to build a blockchain network. However, the UBC Bitcoin Club argues that a blockchain based solution is not compatible or effective; mainly because implementing a blockchain as a solution would be expensive and unnecessary in which the government is required to have a centralized role and their authority embedded into the system.

Their second solution proposes a repository at the LTSA which stores eSTCs and allows access to authorized third parties, as well as a public key infrastructure (PKI), run by the DIACC, which identifies each individual eSTC to the owner of the title. The UBC Bitcoin Club endorses this solution to be more ideal, since the solution is decentralized, in which there is no single authority that runs both platforms, nor does it require a blockchain, though it contains aspects of a blockchain solution such as decentralization, using public/private keys, digital certificates, and hashing algorithms.

Architectural Components:

For the first solution (Hyperledger Blockchain), the UBC Bitcoin Club does not provide enough detail to present a complete analysis of its architectural components and how they integrate since it is not the solution they endorse.

The second solution is composed of a repository and a public key infrastructure (PKI).

- *LTSA Certifications Access Service*

  User interface for customers to request eSTCs.

  Repository:

  The repository is part of the LTSA Certifications Access Service, in which the eSTCs are stored and only authorized stakeholders can access.

- *PKI*

  The UBC Bitcoin Club proposes that the DIACC runs the PKI, which is used to identify each individual eSTC to the owner of the title. The PKI would be run from the DIACC as a plug-in to the LTSA Certification Access Service, and it would be closed in order to be compatible with current proprietary software that the LTSA uses.

Independent Certificate Authority (CA):

The CA issues the public key certificate to the DIACC PKI, and the DIACC PKI relays the certificate to the LTSA who can then verify it against their record of eSTCs to determine a user's ownership of the eSTC.

Strengths:

First Solution: Hyperledger Blockchain

- A blockchain solution can improve the effectiveness of the LTSA, but the UBC Bitcoin Club does not specify how. However, the UBC Bitcoin Club argues that a blockchain solution is incompatible for this use case because the government would have to be the sole source of trust and authority in the system.

Second Solution: Repository & PKI

- The LTSA issues eSTCs to customers who are verified by the government.

Weaknesses:

First Solution: Hyperledger Blockchain

- According to the UBC Bitcoin Club, a blockchain solution is incompatible with this use case because having the government required as the sole key source of trust is ineffective, since an eSTC remains unverified until the government endorses the claim. As a result, this could lead to inefficiencies in the system waiting for endorsements from the government.
- Implementing a blockchain based system as a solution would be costly and ineffective compared to the second solution (i.e., Repository & PKI).

Second Solution: Repository & PKI

- Secrecy of the code behind the PKI is not available to the public, and therefore difficult to know whether the code and its components are truly safe.
- The LTSA could be liable for software installation, problems, troubleshooting, and the cost of maintaining and updating the software.
- eSTCs are stored in a single storage area putting them at risk to system outages and hacking.

Links:

- Paper: https://diacc.ca/wp-content/uploads/2017/11/UBC-Bitcoin.pdf

TEAM: UBC i-LAB

Team Members:

- Sanjeeva Rajapakse
- Alberto Cevallos
- Ren Wang

- Nuwan Rajapakse

Name of Solution: N/A

Description of Solution:

The solution proposed by the UBC i-LAB is a private, permissioned blockchain leveraging Hyperledger Fabric. Authentication of customer and third party identities, as well as the issuing, accessing, and distribution of eSTCs are all done utilizing a Hyperledger blockchain.

Architectural Components:

Utilizing the Generic Blockchain Record Keeping Reference Architecture (**Figure 3**), the following components of the solution are identified:

DApps/Ledger Application Interfaces/Off Chain Services - Operational System

- *LTSA Email Portal*

  An email application in which eSTCs are shared with third parties, in which the LTSA functions as the "Endorser" of the transaction. The eSTC is emailed to a third party as depicted in **Figure 7**.

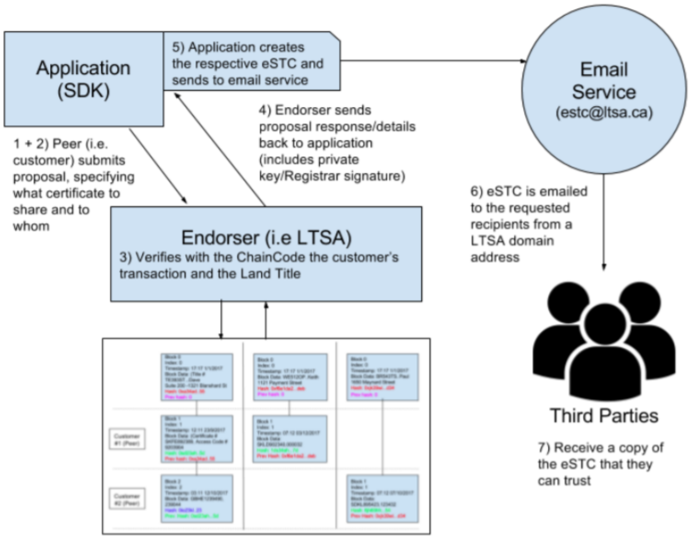

Application (SDK)
5) Application creates the respective eSTC and sends to email service
Email Service (estc@ltsa.ca)
4) Endorser sends proposal response/details back to application (includes private key/Registrar signature)
1 + 2) Peer (i.e. customer) submits proposal, specifying what certificate to share and to whom
Endorser (i.e LTSA)
3) Verifies with the ChainCode the customer's transaction and the Land Title
6) eSTC is emailed to the requested recipients from a LTSA domain address
Third Parties
7) Receive a copy of the eSTC that they can trust

Figure 7. Email System Flowchart.

Blockchain/Distributed Ledger (Core Processing)

- *Hyperledger Fabric*

  The Hyperledger blockchain is a private-based blockchain which is also permissioned; meaning that all participants in the network are identified.

  Chaincode (Smart Contracts):

  Smart contracts are created using the Time Stamp feature of Hyperledger, in order to update the ledger and to deactivate a certificate or access codes if the eSTC is not accessed within 7 days and when they have expired after 12 months.

Blockchain/Distributed Ledger (Side Chain)

- *Hyperledger*

  Channels:

  Channels function as an internal level of authentication and authorization and create permissions to view data. Participants in the network are identified automatically and separated into their appropriate channel for access. As a result, all data (which includes transaction, member, and channel information) on a channel are invisible and inaccessible to any participants of the network not explicitly granted access to that channel (**Figure 8**).

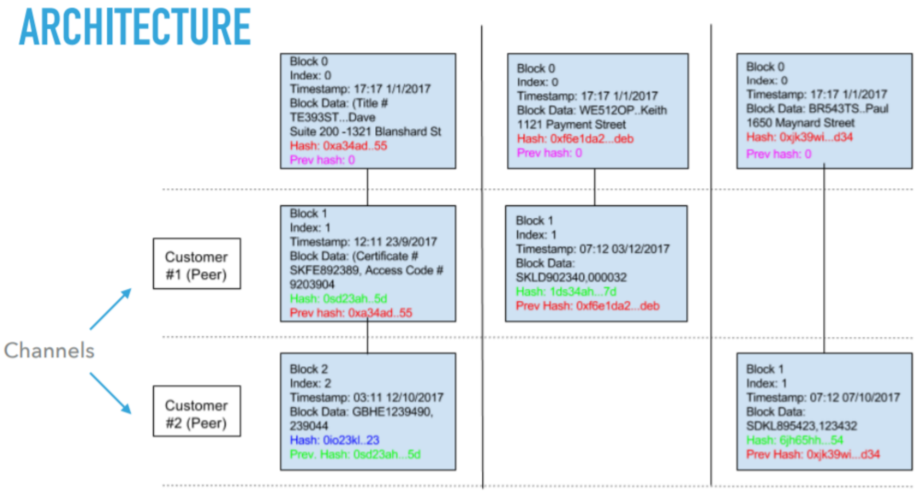

ARCHITECTURE
Channels
Customer #1 (Peer)
Customer #2 (Peer)
Block 0
Index: 0
Timestamp: 17:17 1/1/2017
Block Data: (Title # TE393ST...Dave Suite 200 -1321 Blanshard St
Hash: 0xa34ad..55
Prev hash: 0
Block 1
Index: 1
Timestamp: 12:11 23/9/2017
Block Data: (Certificate # SKFE892389, Access Code # 9203904
Hash: 0sd23ah..5d
Prev hash: 0xa34ad..55
Block 2
Index: 2
Timestamp: 03:11 12/10/2017
Block Data: GBHE1239490, 239044
Hash: 0io23kl..23
Prev. Hash: 0sd23ah...5d
Block 0
Index: 0
Timestamp: 17:17 1/1/2017
Block Data: WE512OP..Keith 1121 Payment Street
Hash: 0xf6e1da2...deb
Prev hash: 0
Block 1
Index: 1
Timestamp: 07:12 03/12/2017
Block Data: SKLD902340,000032
Hash: 1ds34ah...7d
Prev Hash: 0xf6e1da2...deb
Block 0
Index: 0
Timestamp: 17:17 1/1/2017
Block Data: BR543TS..Paul 1650 Maynard Street
Hash: 0xjk39wi...d34
Prev hash: 0
Block 1
Index: 1
Timestamp: 07:12 07/10/2017
Block Data: SDKL895423,123432
Hash: 6jh65hh...54
Prev Hash: 0xjk39wi...d34

Figure 8. Proposed Architecture of Channels.

Strengths:

- Customers are identified, and transactions with certificates/access codes are linked to the corresponding LTSA account. As a result, the LTSA does not require PDFs.
- Channels add an extra level of security and privacy that protects customers' competing business interests and intentions.
- Channels are capable of auto-populating an eSTC with the correct details, thus reducing hardware space for eSTCs.

Weaknesses:

- eSTCs are mistakenly assumed to be stored on the blockchain - only a hash of the document should be recorded onto the blockchain.
- No discussion on where eSTCs are stored.
- Method of delivery of eSTCs are not specified (e.g., QR Code, link to blockchain, etc.).
- Privacy and security concerns of eSTC information sent via email to third parties.

Links:

- Paper: https://diacc.ca/wp-content/uploads/2017/11/UBC-iLab.pdf

b. Analysis in relation to Archival Theoretic Evaluation Framework

How does the blockchain affect the trustworthiness and long-term preservation of records?

This section presents an archival theoretic evaluation of the aforementioned solutions. In archival science, a record is said to be trustworthy if it is assessed as being accurate, reliable and authentic. These main attributes can be decomposed as shown in **Figure 9**. Each of these characteristics is discussed briefly below in relation to the solutions presented in the previous section.

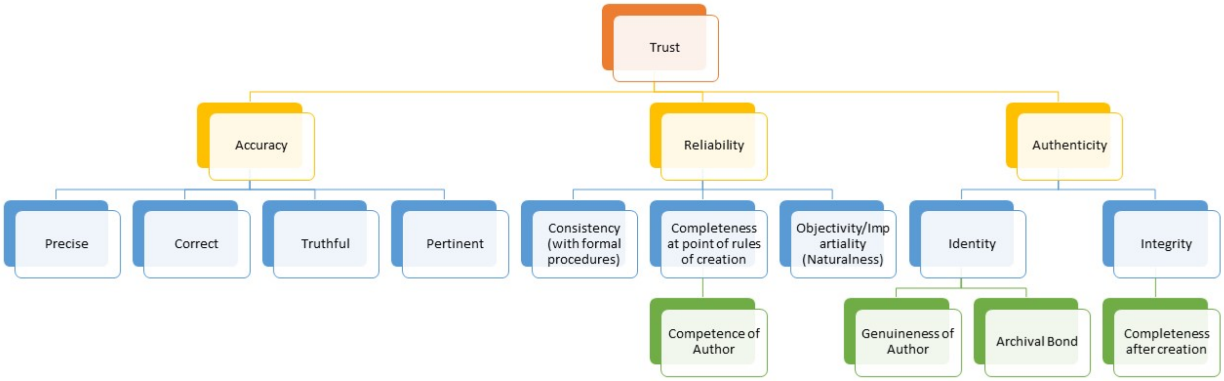

Trust
Accuracy
Reliability
Authenticity
Precise
Correct
Truthful
Pertinent
Consistency (with formal procedures)
Completeness at point of rules of creation
Objectivity/Imp artiality (Naturalness)
Identity
Integrity
Competence of Author
Genuineness of Author
Archival Bond
Completeness after creation

Figure 9. A taxonomy of key archival concepts and their relationship to trust[54]

Accuracy

Accuracy is "[t]he degree to which data, information, documents, or records are precise, correct, truthful, free of error or distortion, or pertinent to the matter."[55] None of the solutions are specifically designed to make improvements to the accuracy of eSTCs as accuracy was not identified as a problem area needing to be addressed during the DIDC. As the eSTC would continue to be generated from the LTSA's database of land titles, accuracy of the eSTCs is directly dependent upon the accuracy of this database. Further, since none of the solutions proposed a change to the source data from which the eSTC would be generated, no change to the accuracy of the eSTC would result.

Reliability

[54] Author's own rendering.

[55] Pearce-Moses, R. (ed.) (2018) *InterPARES Trust Terminology*, InterPARES Trust, https://interparestrust.org/terminology/term/accuracy.

Reliability concerns "[t]he trustworthiness of a record as a statement of fact," encompassing the notion of a record having been generated by systems that operate reliably and consistently as well as created by a competent authority, according to established processes, and being complete in all formal elements.[56] Aspects of systems that will increase reliability include characteristics of having been built according to standards and a high level of assurance and being provably free from operating errors and security vulnerabilities. None of the solutions discussed in this report are operating systems, they are proposed solution designs. As such, the effect on reliability of each solution is largely still quite speculative.

In general, however, the winning solution from OnePair Technologies and the runner up solution from AlphaBeta discuss how the designs leverage standard specifications (e.g., BlockCerts, Decentralized IDs), and Union of Blockchain discussed use of the BC Identity Assurance Standard. Incorporation of standards into these designs suggests that the solutions may operate more reliably (i.e., than systems that do not incorporate the use of standards).

Aside from reliable operation of eSTC generating systems, reliability includes the notion that eSTCs would be generated by a competent authority, according to established processes, and complete in all formal elements. The winning solution proposed that the LTSA, which, by BC law, is the authorized authority for the maintenance of BC land titles, would generate certificates to be used in a certificate issuance app. As the certificates would originate from an already trusted, competent authority, and could be verified as such using blockchain technology, it is anticipated that third parties (e.g., banks) would be willing to accept the certificates as reliable evidence of land title. A similar approach was proposed by AlphaBeta, which proposed to offer a customer client app through the LTSA portal (and presumably would access LTSA land title data to generate eSTCs). Similar approaches were proposed by the other competition participants, with no shift away from reliance on the LTSA as the competent authority.

All solutions, however, did propose modifications to the existing LTSA eSTC issuance process designed to address the pain points of the current process. For example, in the OnePair solution, eSTCs are generated by a special certificate generation app and registered on a blockchain. Individuals that request eSTCs hold the certificates in a customer app and are then able to present the certificates to third parties who are able to verify the certificates using a verification app.

Not all of the proposed solutions had fully worked out revised processes for issuance, registration and verification by third parties of eSTCs. Most solutions did not explicitly propose alterations of the form of the eSTCs (i.e., the data to be represented in the eSTC and how it would be rendered in a PDF version of the document), but team Credophy proposed that the eSTC be implemented as a smart contract, which would involve a transformation of the current form of the eSTC into a new form. As the form of the STC is specified by law, this solution may be harder to implement due to the requirements to amend existing legislation.

All solutions proposed that a hashed version of the eSTC be registered on a blockchain as a means for third parties to independently verify the authenticity of the eSTC, though each had differences in how they proposed to achieve this. Union of Blockchain's solution also proposed to add an eSTC token to control permissions to the eSTC, etc.

[56] Pearce-Moses, R. (ed.) (2018) *InterPARES Trust Terminology*, InterPARES Trust, https://interparestrust.org/terminology/term/reliability%20~paL~record~paR~.

Authenticity

Authenticity is "[t]he trustworthiness of a record as a record; i.e., the quality of a record that is what it purports to be and that is free from tampering or corruption."[57] Authentication of a record involves a determination of its genuineness, based on internal and external evidence. This includes assessing "the identity and the integrity of the record to determine what the record is, when it was created, by whom, what action or matter it participated in, and what its juridical/administrative, cultural, and documentary contexts were . . . It must also be possible to ascertain the wholeness and soundness of the record: whether it is intact or, if not, what is missing."[58] Blockchain solutions work relatively effectively to establish the integrity of records (i.e., that they are free from tampering and remain intact).[59] They are often less effective when it comes to establishing the identity of records and their creators.[60] That said, in all of the proposed solutions, the hash of the eSTC registered on the blockchain would serve to establish the identity of the record for purposes of this use case as long as the hash could be linked back to the context of its creation (referred to in archival theory as establishing the archival bond). Since the LTSA would remain the issuer of the eSTC, and the origin of the eSTC from the LSTA would be verifiable in the proposed solutions (because the LTSA would digitally sign to generate the eSTC), the identity of the creator of the record would also be verifiable (i.e., it would be possible to determine that the creator of the record is genuine and who it is purported to be).

Persistence and Preservation

Records are created to capture facts about transactions in a fixed and trustworthy form. Depending on the nature of the transaction and ongoing utility, records may need to be retained from very short (e.g., days) to extremely long (in perpetuity) time periods. In the case of the eSTCs, they are communicating the status of title to a particular piece of land. As the record of title is kept in a separate land title register, and the eSTC is simply a reflection of this database used only to communicate to third parties the status of land title at that point in time, the retention period is relatively short. Currently, an eSTC is valid for 12 months from date of issuance, and there is no requirement for longer retention of an eSTC (either by LTSA or by the requestor). Though a blockchain creates an immutable record of the hash of the eSTC in the proposed solutions, which means that the hashes cannot be removed after the eSTC is no longer valid, it is possible to provide for expiration of the validity of the eSTC on a blockchain. For example, team Union of Blockchain proposed tokenizing the eSTC and linking it to a smart contract that controls permissions. Expiration dates of eSTCs for permissions would be read from the timestamp affixed to all documents as they are registered in a blockchain, allowing eSTCs to expire based on time (e.g., 7 days, 6 months, 1 year, etc.). This approach could automate the process for expiration and removal of eSTCs for the LTSA. The winning solution, OnePair, proposed that the third party validator app would both validate the signature of the

[57] Pearce-Moses, R. (ed.) (2018) *InterPARES Trust Terminology*, InterPARES Trust, https://interparestrust.org/terminology/term/authenticity.
[58] Ibid.
[59] Lemieux, Victoria L. "Blockchain and Distributed Ledger as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework," Proceedings of the Future Technologies Conference, Vancouver, Canada, November 29-30. IEEE, 2017.
[60] Op. Cit.

issuer (i.e., LTSA) and check the status of a certificate (i.e., expired or revoked). The OnePair solution does not go into detail as to the mechanisms that the third party verifier app will use to determine whether a certificate is revoked or expired (though this could be achieved through the use of timestamps). Similarly, team AlphaBeta mentions that customers may revoke their proof at any time, thus giving them more control of their personal information, but they do not explain how this will be implemented in their solution. Nor is it clearly explained in the documentation provided for the DIDC, given that the solution is predicated upon customers having control of their own data, how the LTSA would revoke or invalidate a certificate held by an eSTC requestor.

d. Lessons Learned relating to Design Challenge Process

In addition to lessons learned about the application of blockchain technology to the DIDC use case, the organizers of the DIDC drew lessons about the process of running a design challenge of this nature.

Organization of the DIDC

The following reflects aspects that went well during the organization of the inaugural DIDC, as well as feedback for improvement for future DIDCs.

Successful Aspects:

- Audience voting during the IdentityNORTH Western Forum.
- Posting the use case and related resources online to the website.

Areas for Improvement:

- Need to build up a network of mentors to reach out towards for a pool of judges, but also to provide participants with guidance versus only the online Q&A session.
- Additionally, two types of mentors are needed in order to combat the isolating effect of the DIDC. Mentors should include domain experts and technical experts.
- More time for the entire process of the DIDC, such as the overall organization of the DIDC as well as more time for the participants to develop a solution.
- Intellectual Property - Terms & Conditions: Need to ensure that all parties running the design challenge as well as those participating are covered.
- Need to do a better job of providing the use case from a subject matter or client perspective. It was difficult to correct errors in understanding, since the DIDC organizing team tended to be more focused on the technicalities and less on the procedural and legal aspects of the use case.
- Registration of the teams. Too much background work went into trying to put teams together in which there were just individuals who were interested. Participants could have the option for either registering as an individual or as being interested in being a part of a team. Teams could be created automatically through pairing up participants interested in joining a team.
- The organizing team members were either too far removed or too technical, the DIDC needs someone with the right level of expertise to provide the information.

Technical Solution

Aspects Which Went Well:

- There was diversity in submissions; no two solutions were alike. Every solution brought something different in terms of solution design.

Areas for Improvement:

- Submissions should adhere to a required format in order to facilitate a proper analysis of all submissions.

E. Conclusions

This document has reported on the results of a design challenge competition proposed by the Digital ID & Authentication Council of Canada and the Land Title and Survey Authority of British Columbia to offer students and professionals the chance to contribute ideas for a real world, industry application of digital identification in the context of land title transfers within the Canadian province of British Columbia. Eight entries were received, and a winner (OnePair Technologies) and runner up (AlphaBeta) were selected.

The submissions mostly focused on leveraging blockchain technology, and not addressing the Digital ID aspect of the use case. This may have been because the use case was too complex for participating teams to address, and participants may have found it difficult to focus on both given the time limit they had. Of the eight submissions, a variety of methods for embedding identity into an eSTC were proposed (e.g., biometrics, self-sovereign ID, use of digital certificates, distributed verification of identity claims).

All teams proposed blockchain solutions, but one team recommended a traditional PKI instead of using a blockchain-based solution (UBC Bitcoin Club). Several of the solutions were agnostic as to which blockchain platform should be used. Of those platforms mentioned Hyperledger was the most popular with several different varieties being recommended (e.g., Indy, Fabric, Sawtooth). It is likely that Hyperledger proved a popular choice because it is designed to be a private distributed ledger system (i.e., a distributed ledger system in which a controlled and limited set of nodes participate in the operation of the system), which means that the locus of trust is not entirely shifted to the operation of the system but relies, in part, on the participation of parties in which a certain amount of trust has traditionally been placed (e.g., LTSA, banks). In this sense, it is not as disruptive of existing trust models or trusted institutions as relying wholly on a public blockchain model (e.g., a model in which any node, i.e., device or process, can participate in the operation of the system). The proposed Hyperledger solutions are also permissioned ledgers; that is, they are systems wherein nodes and/or users need authorization to perform an activity or activities. This also provides a greater assurance of trust, since permissioned systems allow for additional controls (e.g., authentication) designed to prevent manipulation or misuse of a system.

The solutions also varied in terms of the level of centralization versus decentralization they were proposing. In the most decentralized of the solutions (e.g., AlphaBeta), system users had their own personal wallets, in which they held their eSTCs, and could revoke permissions to them at any time. In more centralized solutions (e.g., UBC Bitcoin Club, Credophy) centralized trust authorities such as the DIACC or LTSA remain largely responsible for operating the system and/or issuing credentials. The fact that many of the solutions, though relying on blockchain technology, continued to rely upon more centralized and traditional sources of trust speaks to one of the key challenges associated with applying blockchain technology: the difficulties of re-envisioning old centralized operating models as new distributed ones.[61] The challenge is further compounded when traditional centralized operating models are tightly integrated with organizational business models (e.g., platform economics). One of the lessons learned from the design challenge is that implementation of a blockchain-based solution will require thinking through whether changes would be needed to the LTSA's current business model and revenue streams (e.g., from issuance of eSTCs).

None of the solutions presented covered every aspect of the reference architecture (**Figure 2**) fully, which is to be expected in a competition that ran over such a short period and did not involve regular interaction between LTSA domain and technical experts and DIDC participants. The winning solution focused on the application layer, while the runner-up solution focused on the core blockchain processing layer. Among the most under-specified aspect of the reference architecture were application interfaces between components of the distributed ledger and storage, with most submissions remaining silent on details of where eSTCs would be stored or placing the onus for storage of eSTCs with end-users. Given that each team focused on different aspects of the solution, with each generating novel ideas to support the use case, it may be that the best approach is to combine solutions (e.g., OnePair's solution of a wallet app with Union of Blockchain proposed blockchain system) to increase efficiency of the current eSTC system.

The organizing team concluded that it would need to do further research because there is evolution in the technology, leading to a fair amount of change, and the technology is developing at a fast pace. A full understanding of how blockchain could be applied is still far away. Moreover, because blockchain is an ecosystem solution (i.e., intended to work across different organizations and business partners), it will not be something that the LTSA will be able to decide to implement on its own. Implementation will require building up and bringing along an entire ecosystem.

Possible next steps were identified by the organizing team:

- Research into a Proof of Concept.
- Blockchain might not be necessary or overkill for the LTSA.
    - Disruptive to current business process.

Next Steps for DIACC & IDN:

- Aim for three IdentityNORTH challenges per year.
- DIACC has launched an Innovation Expert Committee with the scope of identifying and engaging DIACC members priorities for future innovation projects.[62]
- There is a willingness to continue on with a collaborative approach to future DIDC's and engagement in other cities.

[61] Victoria L. Lemieux, "Making the Transition to Blockchain Government Recordkeeping: Why, When, What and How" *From Parchment to Digit Conference on e-Government*, Kazan, Russia, April 18-20, 2018.

[62] Email exchange with Joni Brennan.

APPENDIX A: DIDC JUDGING CRITERIA

Judging Criteria: Scoring Rubric

The Digital ID Design Challenge is not expecting full-blown solutions to the use case. Of course, we will be impressed if you can do it! Here's what our judges will be looking for on a scale of 1-5, with 5 being the highest score.

Judging Criteria and Weighting

Context and Relevance – the solution(s) are relevant to the context of the cases provided.	25%
Security and Privacy – the solutions(s) demonstrate security and privacy principles by design.	25%
Economic and Social Benefit – the solution(s) clearly demonstrate economic and social benefit.	15%
Feasibility – the solution(s) may be developed with the right resources and support.	15%
Usability and Convenience – the solution(s) are convenient and easy to use.	10%
Creativity and Presentation – the solution(s) presentation is creative and presented with high quality.	10%