UNION OF BLOCKCHAIN

DIGITAL ID DESIGN CHALLENGE

DIGITAL ID & AUTHENTICATION COUNCIL OF CANADA

DATE

31 OCTOBER 2017

PROPOSED TO

LTSA & DIACC

TABLE OF CONTENTS

A NOTE TO OUR READERS

LSTA and DIACC,

In an increasingly digital economy, secure online transactions and verifications are imperative for risk mitigation, increased efficiency, and creating trust in online services. Utilizing blockchain technology, our solution addresses the Land and Survey Title Association of British Columbia's key issues of document access and validity of shared documents to third parties while adhering to the cryptographic standards, blockchain protocols, and the British Columbia government IM/IT standards. Our recommended solution focuses on a Hyperledger implementation, an open-sourced private blockchain to adjust process flow of eSTC retrieval, transaction, and verification from third parties, while maintaining familiar customer experience for end users. Users will have the ability to access their files through the LTSA website, and have third parties verify the file was requested and legitimate via the blockchain ledger and encryption hashes. Through customer verification our solution provides a scalable method that can be applied to other existing areas of the Land and Survey Title Associations services.

We believe our solution will maximize efficiency, reduce data storage cost, and improve third party trust. We hope that you find value in our proposal and how it address the key pain points of access and sharing.

Sincerely,

Union of Blockchain

CURRENT LTSA SYSTEM

As stated in the DIDC use case [1], the LTSA is interested in improving the efficiency of accessing, sharing, verifying and trusting eSTCs among various parties. In this section, we outline the steps a user takes to acquire an eSTC and share it with a third party in the current architecture. The pain points are pointed out as they arise.

To purchase an eSTC, a user first creates an account on the LTSA website. After this, they may submit a request an eSTC for a given property. Users pay a fee per eSTC request as each eSTC represents a snapshot of the state of ownership of that property. Thus each request generates a unique eSTC that must be compiled and generated. The LTSA processes a user's request and sends the user a link to a PDF that contains the requested eSTC. Currently, this link expires after 7 days. If the user forgets to save a copy of the eSTC or forgets to note down the certificate number and access code, there is no way to access the eSTC after the 7 day window. As a result, all users that lose access to their eSTC must submit a new request for a new eSTC from the LTSA. We will explore the impact of changing this expiry window in depth in a later section.

Once the user receives their requested eSTC, they can open the PDF and view the contents. In many cases, a user may request an eSTC in order to prove to a third party that they own a piece of property. Currently, however, third parties such as banks, notaries, lawyers or government officials, find it hard to trust the integrity of an electronically or physically delivered eSTC.

The user now has access to an eSTC that they cannot easily share with others, and thus does not help them prove that they own the stated property. The third parties must independently submit requests for an eSTC in order to verify the user's claim of ownership.

As a result of these difficulties, the LTSA wants to move to a system that facilitates sharing of user eSTCs and thus eliminates the need for redundant eSTC requests. The solution should also be auditable so that requests can be linked back to firms and individuals if necessary. Additionally, participants in the new program should be able to trust the identities of all other participants.

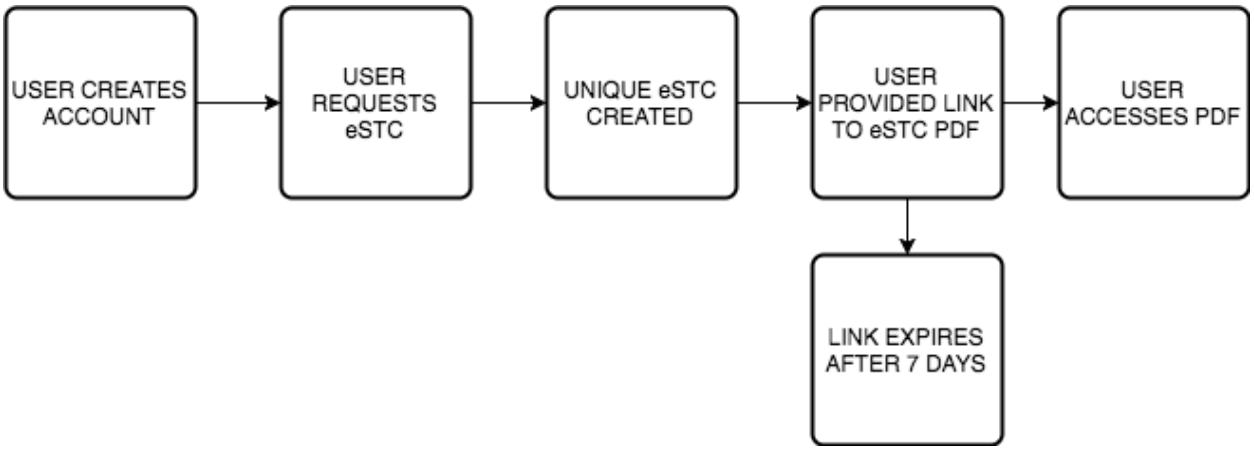

Figure 1: Current LTSA eSTC retrieval process

We now outline our proposed framework for the distribution and sharing of eSTCs among interested parties. Our solution incorporates a permissioned blockchain which acts as an open ledger of all eSTC requests. We also reimagine the architecture of LTSA's online platform to facilitate sharing of eSTCs among users. We wrap the entire framework in a strict Know-Your-Customer barrier to prevent access by untrusted users and we show how the combination of these changes helps alleviate the pain points explored above.

The permissioned blockchain acts as an open ledger showing the creation and history of all eSTCs that have been issued. Each participating user can independently track the history of the eSTC back to its generation by the LTSA. Our solution encrypts the eSTCs using the requesting user's public key and stores the eSTC itself directly on the blockchain. The eSTC is encrypted with RSA 2048-bit public key cryptography, in accordance with BC's IT cryptographic standard [2], to ensure only the requesting user may view the eSTC contents. Blocks in the chain will record instances of each eSTC request, publication and share for all participants. We call each instance of requesting, publishing and sharing eSTCs a **transaction**.

Each entity that wants to request an eSTC (or wishes to verify the authenticity of an already-requested eSTC) must create a LTSA account following identity verification standards such as, at minimum, those outlined in the Medium Identification Level in BC's Identity Assurance Standard document [3]. This ensures that everyone participating in the network is who they say they are. With this account, entities can now request eSTCs from the LTSA as well as send them to other parties. As an example, if a user Alice wants to request, and share, an eSTC with another user, Bob, both must create an account with the LTSA.

Below, we walk through an example of how our proposed solution helps a user, Alice, shares her eSTC with another user, Bob, in a trusted and secure manner.

Request Transaction

Once Alice's identity has been verified in accordance with (at minimum) the Medium Identification Level, she will produce a **request** transaction from her account to the LTSA account. The **request** transaction is simply a transaction published to the global blockchain ledger that announces that Alice is requesting an eSTC on a specific property. Once this request is added to the blockchain, the LTSA will fetch the relevant property's data from their private database and create an eSTC. The LTSA will encrypt this eSTC using the public key that Alice included in her **request** transaction. The LTSA will then **publish** the resulting encrypted eSTC to the global blockchain.

Publish Transaction

The LTSA will create a **publish** transaction in response to Alice's **request** and will publish the newly created (and encrypted) eSTC to the blockchain, along with a reference to Alice's **request** transaction and a hash of the eSTC itself. The hash is included to provide evidence of tampering, as we will show below. This transaction updates the global state of the blockchain, allowing every participant to see that Alice was issued an eSTC by the LTSA, but without allowing other users to read the contents of the eSTC. The **publish** transaction

will also have a timestamp which can be used to auto-delete this eSTC after a certain amount of time has passed managing data storage size. Now that Alice has received her eSTC, she can share it securely with Bob, again using the blockchain. Alice now publishes a **share** transaction.

Share Transaction

Alice creates a **share** transaction which encrypts her eSTC using Bob's public key. She then publishes this transaction to the blockchain and includes a reference to the original **request** transaction she issued to the LTSA. Bob now has access to the eSTC Alice has shared with him. But how can Bob trust that Alice is who she says she is? Moreover, how can Bob trust that Alice has the authority to share this eSTC with him and that the eSTC Alice is sharing has not been tampered with?

Luckily, our solution prevents these events from occurring in three ways. First, every participant in the network has been verified in accordance with, at minimum, the Medium Identification level discussed above. Thus every participant in the blockchain network is, with a high degree of certainty, who they say they are. Second, every **share** transaction must include a reference to the original **publish** transaction that requested a new eSTC. As mentioned above, each **publish** references its associated **request** and thus Bob can directly reference the blockchain history and verify that Alice issued the request for this eSTC. Third, every **publish** and **share** transaction must include the SHA256 hash of the (unencrypted) eSTC document itself. If Bob suspects that the eSTC Alice is sharing with him has been altered in any way, he can simply compare the hash he has been given with the hash indicated in the **publish** transaction which generated the eSTC. If they are different, he refuses to trust Alice's version. If they are the same, he can be sure the eSTC has not been altered. Bob can then decrypt the eSTC and verify its contents with confidence in their integrity.

Notice that in the above case, Bob could have been an enterprise participating in the network, rather than a single user and the protocol would be no different. Enterprises, who may choose to run full nodes in this blockchain (for instance to cache all data locally), can independently verify the eSTCs they receive via the blockchain. The entire history of each eSTC is open to audit, but the content itself is permissioned.

Transaction Fields

Our proposed blockchain has three transaction types. Each transaction's fields are outlined in the table below:

Transaction ID	Transaction Type	From Account	To Account	Timestamp	Encumbrance	Hash	Other Data
integer	Request_eSTC	User_To	LTSA	timestamp	none	None	Property ID, User_To's Public Key
integer	Publish_eSTC	LTSA	User_To	timestamp	User_To's public key	eSTC	Encrypted eSTC, Reference to Request Transaction
integer	Share_eSTC	User_From	User_To	timestamp	User_To's public key	eSTC	Reference to Publish Transaction

Figure 2: The transaction structure for each proposed transaction in the permissioned blockchain.

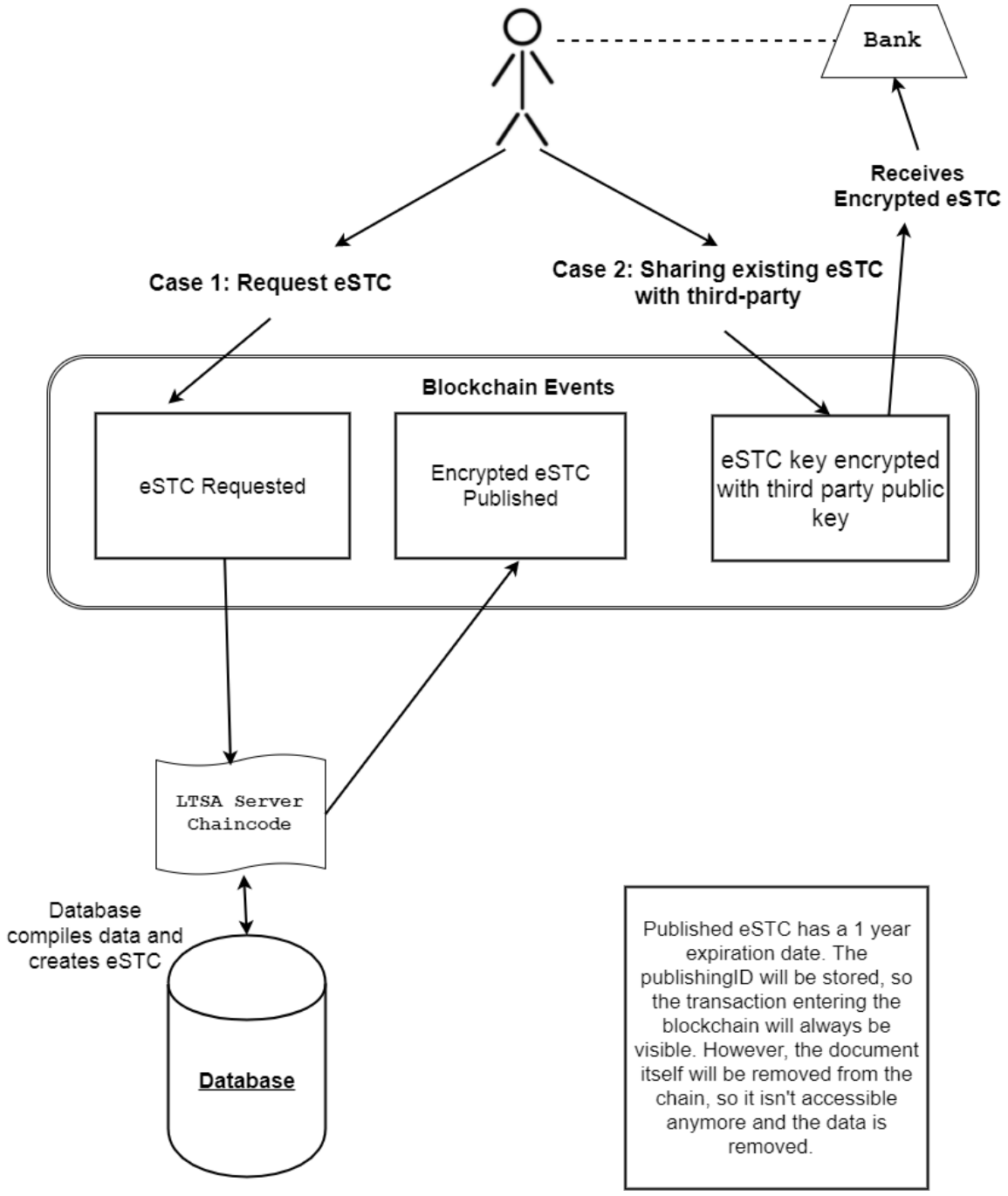

Figure 3: Architecture of our proposed solution. The LTSA database and server are used to create and publish eSTCs to the blockchain. The blockchain tracks the state of these distributed eSTCs among all participants in an open ledger of transactions. The entire history of each eSTC is auditable by each participant, but users can only access the contents of eSTCs that have been shared with them.

Participant Verification

All participants are verified using, at minimum, the standard outlined in the Medium Identification Level in BC's Identity Assurance Standard. Once identity is confirmed by the trusted entity and added to the blockchain, it can be trusted by all.

Document Expiry/Loss

All documents in the blockchain are tied to a block with a timestamp. eSTCs can easily be retired based on time since request: 7 days, 6 months, 1 year etc. Additionally, using our solution, as long as ID is verified and the eSTC exists, an eSTC cannot be lost before timeout.

Document Verification

The blockchain proposal allows us to store the eSTC across participating nodes on the network. To showcase the sharing process, let us assume 3 actors - the LTSA, bank and customer. When an eSTC is requested and paid for, the LTSA publishes a transaction to the network containing the unique eSTC, encrypted using the requesting party's public key. This eSTC can be seen to exist by everyone on the network but only be decrypted and viewed by the requester. The requester can then publish a transaction that allows a third party (bank) to look at the eSTC as well "co-owning" the eSTC. The bank may still alternatively request an eSTC for themselves

Security of Transaction

The blockchain proposal allows for greater trust of documents in three ways. First, the blockchain contains a trusted history of all valid eSTC requests and shares, viewable and auditable by any party participating in the network. Second, these requests are tied to User/Enterprise accounts, which have been set up with a strict KYC interface. Third, the eSTC's are stored in an encrypted format on the blockchain. Only the requesting user can decrypt the eSTC and share decryption ability with other users. This ensures that any user that received decrypt access to an eSTC can check that the eSTC is valid and was created by a known user's request. No links or PDFs need to be accessed or shared outside of the system, thus reducing the potential for malicious actions.

ALTERNATIVE SOLUTION

Due to cost of development and implementation issues, if the LTSA is not able to utilize the proposed blockchain solution and update their digital ID process, changes in current process flow can help mitigate redundant user requests and create efficiency without adding new technical components. The two pain points of access and sharing can be fixed with minor improvements to the current system by:

1. Extending the 7-day expiry window to one year

By giving a user access to the eSTC PDF link for a full year (the same amount of time that the eSTC is valid), customers will always be able to access their documents by logging into their LTSA account, solving the access pain point and redundant request from the same user.

2. Allow LTSA accounts to share information through the website

Due to the fear of document tampering and replicas, financial third parties are skeptical towards the validity of eSTCs. By allowing individual users to directly share eSTCs to other LTSA account holders internally through the website, third party institutions can verify directly that the document is legitimate. The enterprise receiving this information can see who has sent them the eSTC, and can trust the data as it will be through the LTSA website.

ADDRESSING THE ISSUES

Q) How can the process for expiration and removal of the eSTCs stored with LTSA be automated?

A) As a user no longer loses their access to the eSTC, there will no longer be an issue with removing an eSTC (users won't be requesting redundant eSTCs). When the eSTC is published onto the blockchain, it will also have an expiration date of one year, which will remove the document from the blockchain after a year. The transaction, with the hash of the eSTC still remains, so there is proof that the document was published there at one time.

Q) How can third-parties trust an electronically delivered eSTC?

A) Documents are now shared to another user through the LTSA blockchain. A third-party can now trust that they are receiving access to an official document, and that the person sending it to them has received permissioned access to the document as well.

Q) How can third-party's digitally verify a customer's identity?

A) The platform only allows sharing of eSTC with a thorough know your customer procedure. Therefore, third-parties can be confident that documents being shared through the LTSA site, are being sent from the actual person.

Q) How can participants involved with eSTC (e.g. property owners, lawyers, banks, LTSA, etc.) be connected to streamline the process of sharing and using eSTCs?

A) All participants will now exist on the LTSA platform. Requests for eSTCs will all be on the blockchain, and allowing other users access to an eSTC will also be on the blockchain. All these transactions (requests, sharing, publishing) will be visible, and all stakeholders using the platform will allow for a streamlined system for sharing and using eSTCs.

Q) How can access to an eSTC be controlled or permissioned by a property owner to share with other interested parties?

A) The individual requesting the eSTC is the only person that has access to the requested eSTC on the blockchain. The user has the power to share access to the eSTC to other interested parties. All instances of the eSTC being shared are recorded on the blockchain, so an audit could allow a property owner to identify how many people, and if necessary, who is accessing an eSTC.

BLOCKCHAIN AND HYPERLEDGER

Blockchain technology maintains a history of messages between parties that may distrust each other. There are four components that make it advantageous over other systems: nodes, tokens, transactions and smart contracts. Here we look at Hyperledger [4]. It is the primary open-sourced private blockchain. It uses REST API to allow easy implementation across a diverse technical ecosystem. Four components:

Tokens – These are components of the world state of the blockchain. In Hyperledger, there is no inherent token, but they may be created by participants in the network. In this case, the asset contains details of ownership, the (encrypted) eSTC and variables controlling access to the eSTC. Only the LTSA can add an eSTC to the token.

Transactions – These are events that are executed by participants in the network. They make changes to a token and this change is automatically published to the blockchain. Different user types may have access to different types of transactions.

Nodes – This is the identity layer in Blockchain. Anyone signed up to the system as a participant becomes a node. They may be given different read/write transaction permissions. If they are allowed to execute a transaction, they create a block on the chain (mining). Total node size given BC household projections [5] is 160 GB, comparable to that of Bitcoin core node size.

Smart Contracts – Hyperledger allows for a human interface as it operates with REST API. Basic URL calls by a person acting as a node can execute a transaction. This can be updated in future to automate some processes.

SCALABILITY

Our solution insists on a better 'Know Your Customer' process, which in turn allows for future scalability of the system. Using other services that the LTSA provides to customers as a use case, we can implement those services into the blockchain. For example, registering property ownership. With the digital ID being much stronger on the LTSA system, property transfers and registration can be shown on the blockchain using the same methodology. In place of the eSTC, a contract may be signed by parties - buyer, seller, mortgage provider, lawyer, realtor, etc. Users could prove ownership of land by having their identity linked to the land on the blockchain. As record keeping on land titles traditionally contain key attributes, this solution can be applied to similar companies worldwide.

CONCLUSION

We have shown that our blockchain-based solution helps alleviate the current pain points around eSTC access and sharing. By implementing our proposed Hyperledger permissioned blockchain and a more stringent customer verification process, third parties can confidently trust the integrity of all eSTCs issued by the LTSA. Additionally, by giving third parties co-ownership privileges and the ability to share directly via the LTSA website, users can securely share and trust in eSTC titles. Allowing banks and other third parties the opportunity to host a node locally helps improve security, ease of access and fault-tolerance of the eSTC blockchain. Recording customer transaction requests on the permissioned blockchain reduces inefficiencies from redundant requests and gives all participants in the network auditing privileges. Overall, the LTSA can expect an increase in customer satisfaction, improved operational efficiency, and a secure and trustworthy platform upon which many further products can be built.

REFERENCES

[1] DIDC Use Case. (n.d.). Retrieved October 31, 2017, from https://diacc.ca/didc-use-case/

[2] British Columbia, Architecture, Standards and Planning Branch, Office of the CIO. (2017, February 28). CRYPTOGRAPHIC STANDARDS FOR INFORMATION PROTECTION. Retrieved from https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/cryptographic_standards_v17.pdf

[3] British Columbia, Architecture, Standards and Planning Branch, Office of the CIO. (2017, February 28). IDENTITY ASSURANCE STANDARD. Retrieved from https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/identity_assurance_standard.pdf

a. Public keys must be 2048 bits RSA as explained in the above document. (page 7)
b. Encrypted files must be done with 256-bit AES (page 8)

[4] Cachin, C. (2016, July). Architecture of the Hyperledger Blockchain Fabric* [PDF]. Zurich: IBM Research.

[5] Ministry of Technology Innovation and Citizens Services. (2017, July 31). Household Projections. Retrieved October 31, 2017, from https://www2.gov.bc.ca/gov/content/data/statistics/people-population-community/population/household-projections