University of British Columbia
Records in the Chain Project

Title and code:	**Real Estate Transaction Recording in the Blockchain in Brazil (RCPLAC-01) – Case Study 1**
Document type:	Case Study
Status:	Pre-press
Version:	1.1
Research domain:	N/A
Date submitted:	September 3, 2017
Last reviewed:	January 9, 2018
Author:	Records in the Chain Project
Writers:	Daniel Flores, CNPq UFSM Ged/A Research Group Claudia Lacombe, National Archives of Brazil Victoria Lemieux, University of British Columbia
Test bed participants:	Rafael Mezzari, Real Estate Registry Office, Pelotas – RS, Brazil Nathan Wosnack, Ubitquity LLC.
Research team:	Daniel Flores, CNPq UFSM Ged/A Research Group Claudia Lacombe, National Archives of Brazil Victoria Lemieux, University of British Columbia Sérgio Rodrigues, CNPq UFSM Ged/A Research Group Matheus Baumgarten, CNPq UFSM Ged/A Research Group Danielle Batista, University of British Columbia

Document Control

Version history			
Version	Date	By	Version notes

0.1	18 August 2017	Victoria Lemieux	First draft in English
0.2	25 August 2017	Daniel Flores	Second draft in English (some new additions with its original version in Portuguese inside a box under the English version)
0.3	3 Sept. 2017	Victoria Lemieux	Review of Second draft in English, and integration of additional Portuguese text into a consolidated English version of the text
0.4	3 November, 2017	Daniel Flores	Draft correction according to the reviews and guidelines received from Victoria Lemieux, Rafael Mezzari, Nathan Wosnack and Claudia Lacombe review.
1.0	December 18, 2017	Victoria Lemieux	Review of the Third draft in English, and updating of text based on feedback received from Testbed participants.
1.1	December 27, 2018	Nathan Wosnack Anastasiya Maslova	Review of version 1.0 and additional edits/points of clarification.
1.2	January 4, 2018	Victoria Lemieux	Corrections to version 1.1 based on feedback from Nathan Wosnack and Anastasiya Maslova
1.3	January 8, 2018	Daniel Flores	Final review received from Victoria Lemieux with Nathan Wosnack orientations about “Real Estate Transactions Recording in the Blockchain in Brazil (RCPLAC-01) – Case Study 1” Project
1.4	January 21, 2018	Danielle Batista	Final corrections and edits

Table of Contents

Abstract

This document reports on a pilot study of the application of Blockchain technology to land transaction recording in the Municipality of Pelotas, Rio Grande do Sol, Brazil. It was carried out between May to September, 2017 as part of the University of British Columbia's "Records in the Chain" Project and CNPQ UFSM Ged/A Digital Records Research Group.

A. Overview

This case study has been conducted in cooperation with the Real Estate Registry Office – Pelotas – RS, Brazil, Ubitquity LLC, the National Archives of Brazil, and CNPq UFSM Ged/A Research Group. It discusses a solution developed by a US-incorporated blockchain technology company called Ubitquity which specializes in blockchain-based recording of titles and ownership transfers. The solution is currently being piloted in partnership with the Cartório de Registro de Imóveis (the real estate registry office) in the Brazilian State of Rio Grande do Sul, Municipalities of Pelotas and Morro Redondo. This paper concentrates on the pilot in Pelotas. Data on the solution were gathered between May to July, 2017 from examination of company documentation, videos, newspaper articles and other reports about the project. Information about the architecture of the system was validated by Ubitquity and the Real Estate Registry Office. The gathering of information about the operation of the solution involved interviews with staff of the real estate registry office and further verification of information about the functioning of the solution. The report uses a version of the InterPARES case study report template specifically adapted for the Record in the Chain Project. The report summarises the current state of the areas covered in the case study template related to the case study goals. It could also function as a base for further cooperation or studies.

Case study goals

The case study has several broad goals, which are to describe:

- How the Blockchain solution is being be used
- What Blockchain platform is being used
- How the Blockchain solution is using information
- How the Blockchain solution operates
- How the blockchain solution works under the law
- How the Blockchain solution affect the citizens of Brazil
- How the blockchain solution affects the trustworthiness and long-term preservation of records

B. Statement of Methodology

The research was carried out under the overall direction of Dr. Victoria Lemieux of the University of British Columbia. Dr. Lemieux first contacted Claudia Lacombe, Digital Archive Specialist at the National Archives of Brazil in April 2017 to collaborate on the preparation of the case study of a pilot project on blockchain-based real estate transaction recording taking place in the state of Rio Grande do Sul, municipality of Pelotas. Claudia Lacombe then reached out to the CNPq UFSM Ged/A Research Group to participate in the study.

As soon as the CNPq UFSM Ged/A team received the invitation through the Digital Archive Specialist of the National Archives, Cláudia Lacombe, the team proceeded to investigate and systematize sources about Blockchain.

An initial videoconference was carried out in order to familiarize the team with the project's theoretical framework and methodology and later with the specific theme of Blockchain. The first video conference was held with the leader of the Brazil-based research group, Prof. Daniel Flores, and Cláudia Lacombe.

In the second video conference, the team was enlarged and included Prof. Daniel Flores, CNPq Group researcher Sérgio Rodrigues, CNPq Group technician Matheus Baumgarten, Cláudia Lacombe and Mr. Rafael Mezzari, from the Real Estate Registry Office in Pelotas - RS.

A subsequent meeting was held in Pelotas - RS. During the visit, audio recordings were made of interviews, and the 5 files of audio recordings contents are: observations, dialogues and documentary surveys, as well as direct archival analysis of the institution, its blockchain system and its records, have been stored in a Google drive to facilitate transcription, as shown in Figure 1.

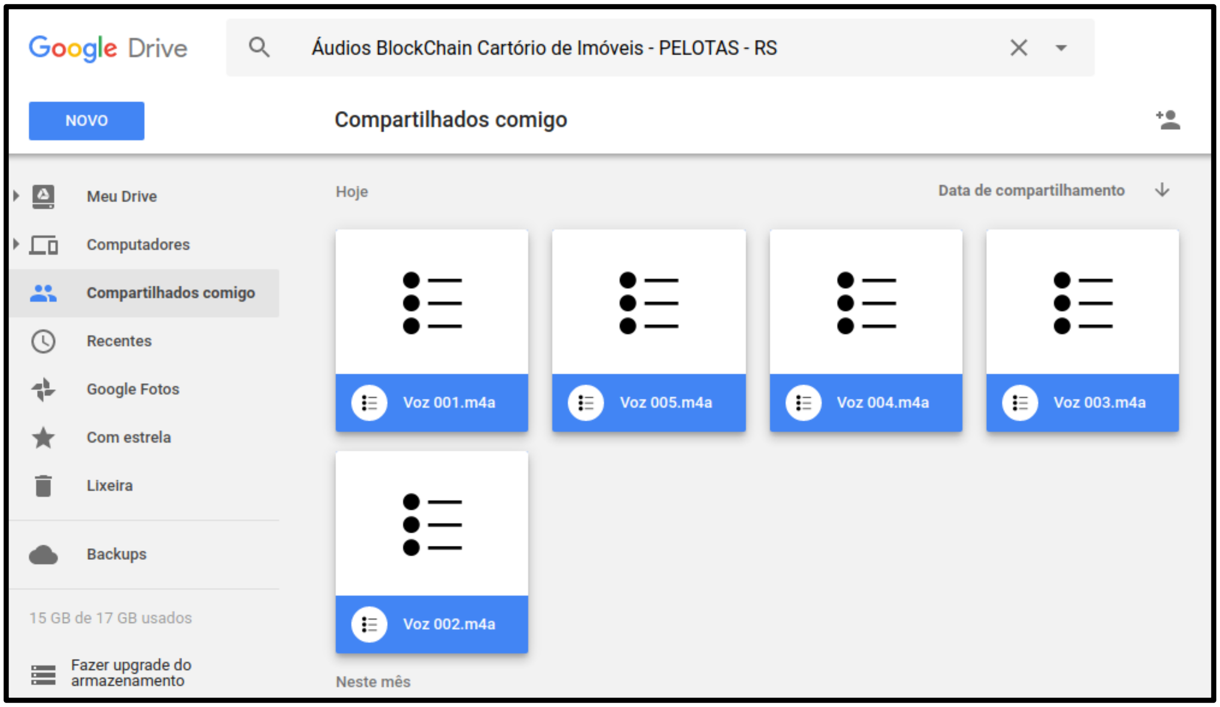


Figure 1: Audio files that recorded interviews with the Real Estate Office

There were 5 audio files in .m4a format, which were transcribed, revised and, following this, the information in the transcriptions then was used to answer the specific research questions.

C. Description of Context

1. Provenancial

Test-bed Name

- Real Estate Registry Office - Pelotas, RS.

Location

- Pelotas – RS, Brazil.

Origins of the Test Bed

According to information given by the notary Mr. Mario Mezzari, the government carries out public tenders for Notaries and Notary Officers (Lawyers), which are appointed to a Civil Registry Office or to a Real Estate Office. The mandate of the Notary at the office lasts until his retirement or transference to another Real Estate Office.

2. Juridical-Administrative

Brazil lacks an integrated system of land management. Thus, land administration is fragmented and occurs at different government levels, depending on the type of land and its use.[1] The World Bank's doing business index provides a detailed analysis of the steps, time and cost involved in registering property in Brazil, assuming a case of an entrepreneur who wants to purchase land and a building in Rio de Janeiro that is already registered and free of title dispute. The process entails at least 13 separate steps. The cadastral database and the registration databases kept by the real estate registry offices are not integrated and different identifiers are used for the same piece of land, creating uncertainty around identification of the property. There is also no electronic database for checking encumbrances (liens, mortgages, restrictions, etc.).[2] According to some sources, lack of integration and systematization in Brazil's system of land registration opens the door to abuse by wealthy landowners who sometimes bribe land registry offices to register someone else's land in their name.[3]

Recently, Brazil introduced the SRE - Electronic Property Registry System project to modernize the current paper-based land registry system and established the National Registry Operator responsible for coordinating property registration between previously isolated property

[1] Eduardo Pereira Nunes, "A Case Study in Brazil: The Main Challenges Faced by Land Administration," (UN, FIG, PC IDEA Inter-regional Special Forum on The Building of Land Information Policies in the Americas, Aguascalientes, Mexico 26-27 October 2004) 15 https://www.fig.net/resources/proceedings/2004/mexico/papers_eng/ts5_nunes_eng.pdf accessed 31 July, 2017

[2] World Bank, 'Doing Business – Registering Property in Brazil, Rio de Janeiro' (2016) http://www.doingbusiness.org/data/exploreeconomies/rio-de-janeiro/registering-property accessed 31 July, 2017

[3] http://news.trust.org/item/20170706130235-xzkye/

registration offices and to define the architecture and operating model for an Electronic Property Registry System.[4]

On April 5, 2017, Ubitquity announced a pilot project in partnership with the real estate registry office in the State of Rio Grande do Sul, Municipalities of Pelotas and Morro Redondo. The goal of the project was to create a pilot program for the region's official land records in an effort to help lower costs while improving accuracy, security, and transparency of land records. This ongoing pilot aims to introduce a parallel platform to replicate the existing legal structure of property ownership and transferring recording . In announcing the pilot, Nathan Wosnack, President/CEO of Ubitquity articulated the aims of the project: "The blockchain allows ownership and title disputes to be handled in a fair and transparent fashion, and serves as a backup in case the original is destroyed or misplaced."[5] Longer term, the project anticipates creating a system that incorporates the features of blockchain technology to transform the existing recording and property transfer processes.

3. Legal

The real estate registry office is subordinate to the judiciary branch of government, with notaries now being nominated through public tenders.
The real estate registry office operates according to Government of Brazil, Title IV, Chapter 2 *Lei N^o 6.216* (30 June, *1975*).

Funding
The financial control is managed by the Notary himself.

Resources (Physical)
With respect to facilities, the Office is located in a building occupying two full floors and one more room in a third floor. There are three rooms for archiving the records, one of them is used for active and semi-active records, because it is in a place of easy access.

Human Resources
Each Real Estate Office usually has an average of 25 Employees hired under CLT regime. Among them there are: IT professionals (3), Cashier (1), Protocol unit (1), Registration unit (7), Certificate unit (8), Mr. Rafael Mezzari, who is responsible for the IT Security, and Mr. Mario Mezzari (referenced as the Notary) is the *Oficial de Registrio* (Registrar).

The personnel management is outsourced.

4. Procedural

There are two activities related to real estate registration:

[4] Adriana Jocoto Unger, Flavio S. Correa da Silva, Joao Marcos M. Barguill, 'Blockchain Technology: The Last Mile for Electronic Property Registration *Systems'* (*IPRA-CINDER International Review* January-June 2017) 52-55

[5] Nathan Wosnack, 'UBITQUITY, the First Blockchain-Secured Platform for Real Estate Recordkeeping, Announces Historic Pilot with a Land Records Bureau in Brazil' (*Medium* April 5, 2017) https://medium.com/@nathanwosnack_75360/ubitquity-the-first-blockchain-secured-platform-for-real-estate-recordkeeping-announces-historic-46c2b0d9f895 accessed 31 July, 2017

1. Request for property information, addressed to certificate/information unit, with immediate response.
2. Property registration, which initiates in the Protocol unit, is then sent to the Registration unit (which researches the property), then to the Certificate unit. At the end, if everything is acceptable, the property registration record is created and delivered to the requesting party, after payment of the fees at the cashier.

Currently, the certificate creation and the recording of some information is done digitally and printed at the end (hybrid process). Some records are in paper form: Negative Ownership Certificates, Positive Copy and Property Registration, while others remain in digital form (those that are kept at the institution): the Registry act, the enrollment, the certificate of enrollment, internal enrollment and the public deed of sale.

Previously, the index books were handwritten (which are still in use when necessary), and included:

- Name Indicator - indexed by people's names;
- Real Indicator - by address, street names.

There is still in use for consultation an Auxiliary Register that was used from January 1976 to October 1996, which contains endorsement and data of a given property, on typewritten cards indexed by enrollments. However, currently, this register is almost unused, following the introduction of IT systems in the office. In case of doubt about the digital record, it is sometimes used to confirm data.

Regarding the Blockchain, which is used just as a test with a little more than half a dozen records, to date nothing has changed the institution's workflow.

5. Documentary

There is no Classification Plan. There is no archivist in the institution, because, according to those interviewed for this case study, the records management at the office is straightforward.

The real estate registry's records are stored in corrugated polyethylene boxes. These boxes are indexed by the creation date, and receive new documentation every two or three days, according to the daily movement, until the box is full. There is still a large amount of files in metal binders within the Office, which are used to store some auxiliary recordings.

6. Technological

There is a real estate management system in the institution preserved in a database, but there is no archival management system or Archival Repository that complies with standards or requirements nationally or internationally recognized, like e-ARQ Brasil, Moreq-JUS, Moreq, DoD 5015, and so on.

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

- *How is/will the Blockchain be used?*

Blockchain will be used to ensure the authenticity of information related to real estate property, that is, to affirm for sure that a particular property belongs to a particular person. The real estate registry office is only running a test with half a dozen records, to try out the security that Blockchain's methodology offers. Mr. Mezzari affirms that such service is very expensive and they need to calculate the cost-benefit ratio, but he considers that it would be possible to use Blockchain in a distant future.

- *What Blockchain platform is being used? How is the Blockchain using information? How is the Blockchain run?*

The solution uses Ubiquity Platform Blockchain version 1.1, Colu's API (alpha).

Ubitquity's solution operates using a software-as-a-service (SaaS) business model, for the recording of land transactions on behalf of companies and government agencies. Fees are charged for adding and updating documents onto its blockchain platform. An overview of the Ubitquity platform is depicted in Figure 2 below.

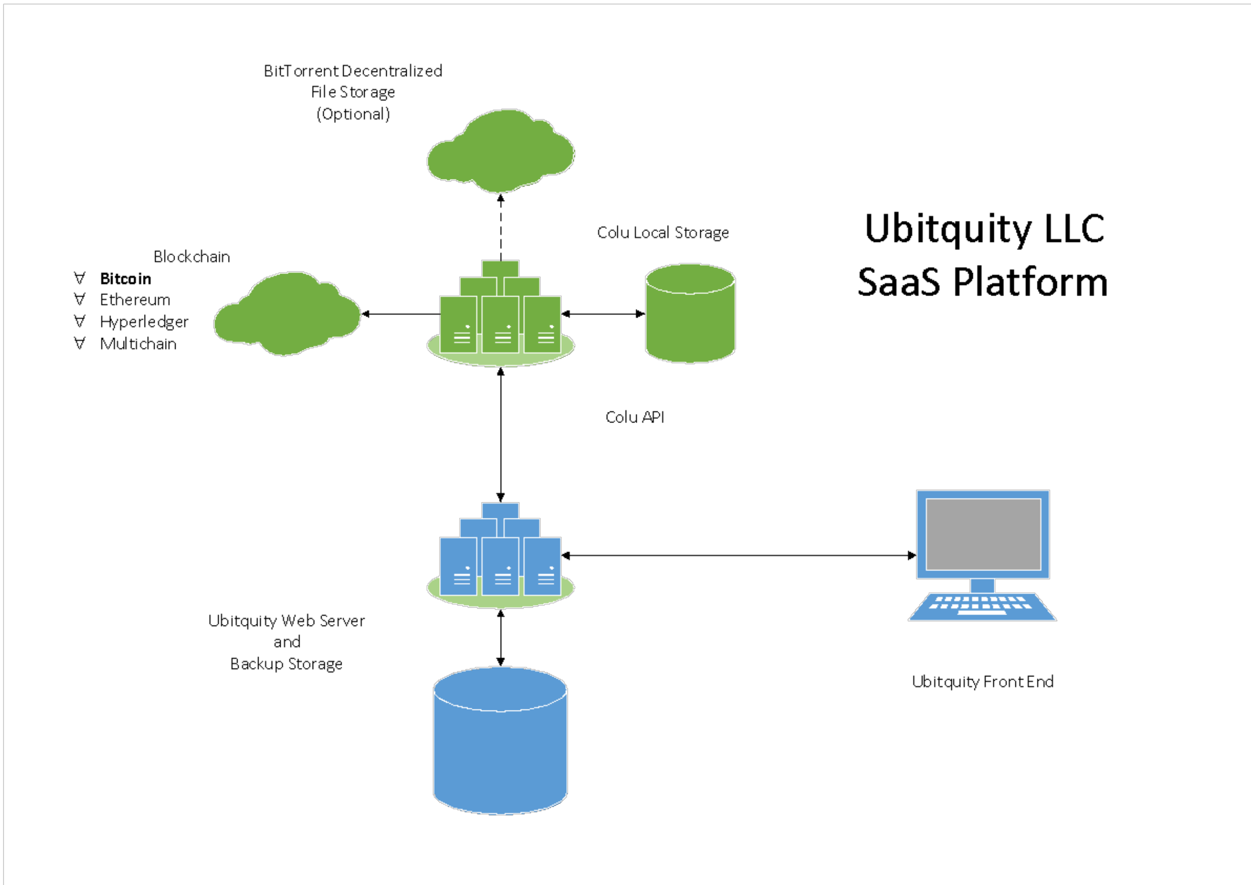
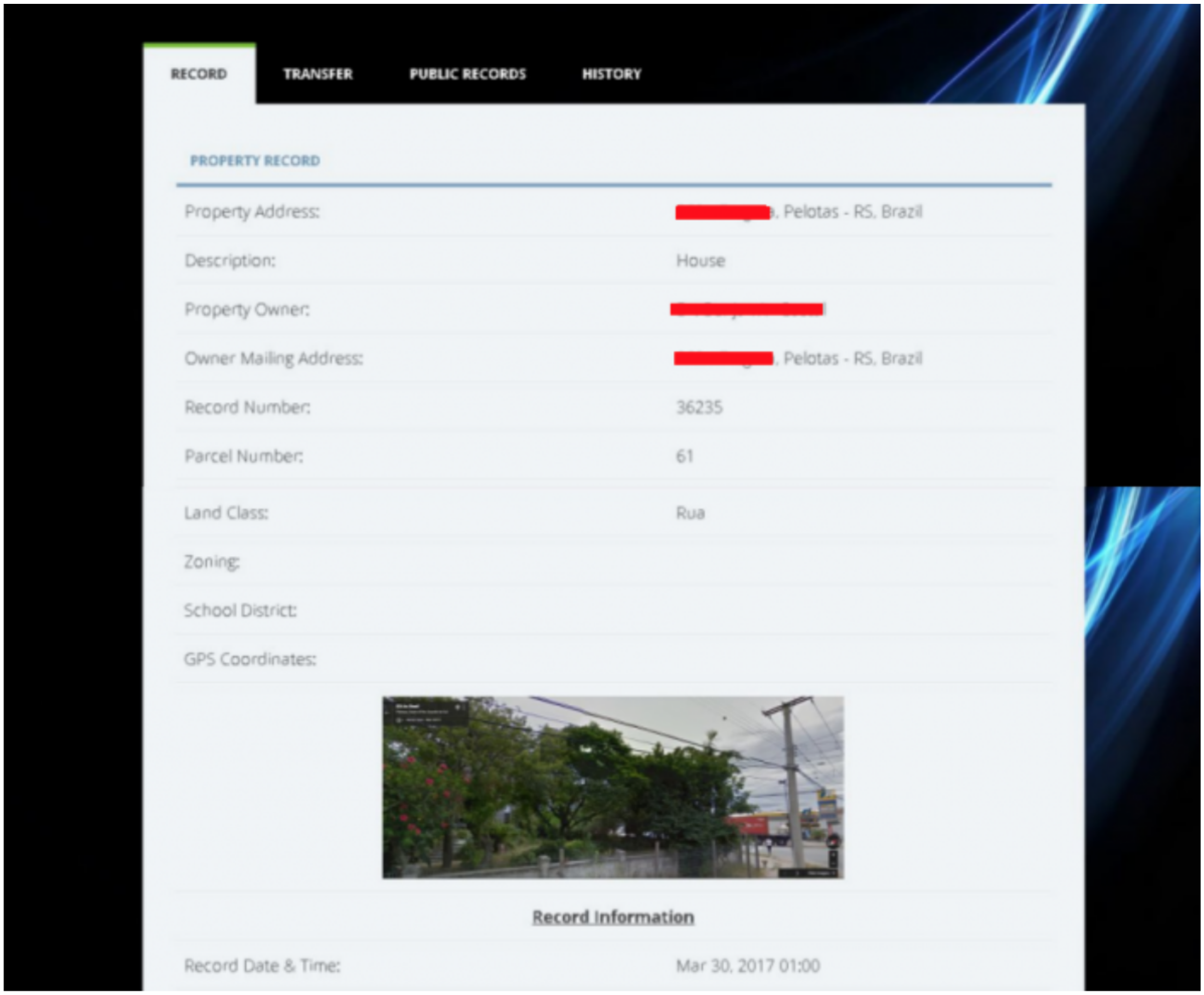


Figure 2. Ubitqity Platform Architecture[6]

The solution comprises a web front end (see screenshot of the front end in Figure 3 below), that captures information taken from the real estate registry's "Book 2" – the general real estate registry[7], as well as a web server and backend storage. Book 2, the general real estate registry exists as a database, containing the registration number for the property, the name of the owner, the address of the property, as well as the image of the property, photos of books, and the certificate. Ubitquity's backend storage hosts the images of the property as well as PDFs of deeds and other documents relating to the property.



PROPERTY RECORD

Property Address:	[redacted], Pelotas - RS, Brazil
Description:	House
Property Owner:	[redacted]
Owner Mailing Address:	[redacted], Pelotas - RS, Brazil
Record Number:	36235
Parcel Number:	61
Land Class:	Rua
Zoning:	
School District:	
GPS Coordinates:	

Record Information

Record Date & Time:	Mar 30, 2017 01:00

Figure 3. Ubitquity Web Front End User Interface. The screenshot shows a land transfer of a doctor's house in the southern city of Pelotas that was entered on March 30, 2017. The address information was given to Ubitquity as a test by the real estate registry office, and more

[6] Diagram supplied to author by Ubitqity

[7] Government of Brazil, Title IV, Chapter 2 *Lei Nº 6.216* (30 June, *1975*) http://www.planalto.gov.br/CCIVIL_03/leis/L6216.htm#art1 accessed 31 July, 2017

registrations have been added since, both from the city of Pelotas and the nearby, more rural municipality of Morro Redondo.[8]

These components communicate with the Colu Application Programming Interface (API), translating what is entered using the front end web user interface into a format that permits assets (i.e., land) and transactions involving those assets (i.e., land transfers) to be recorded on a blockchain. At present the solution uses the Colu "Colored Coins" protocol to record transactions on the Bitcoin blockchain; however, Ubitquity is looking into migrating away from Colu to using the Colored Coins Open Assets protocol in order to ensure the solution is adhering to the best practices for data storage within the jurisdiction.[9] The future plan is to link directly into Colored Coin's decentralized protocol which will be installed within the proper jurisdictions in Brazil, thus adhering to any data export rules.[10]

Colored Coins is a group of protocols and methods for representing and managing real world assets, such as real estate, as a data layer on top of a blockchain. In this case, Bitcoin is being used as the blockchain recording layer, but it is possible to use other blockchains.[11] The Colored Coins implementation developed by Colu and released in June of 2015 attaches metadata to transaction outputs using the OP_RETURN field as well as using a multisignature ("multisig") address when necessary.[12] A multisig is a digital signature scheme that allows multiple parties to partially control a Bitcoin address or wallet. When multisig is implemented, if someone wants to complete a transaction, such as transfer land ownership, they need other people to sign their transaction in order for the transaction to be completed. The needed number of signatures is agreed upon in advance when the address is created.[13] Multisig addresses can be used for storage when there is free space left after storing the digital signatures; for example, when only one of three signatures is used, there is an additional 32 bytes of space for each unused signature that can store data. This allows for the storage of additional data "on chain" in other than the space-constrained number of bytes available using OP_RETURN.[14] Storage of information on chain in this manner allows for association of that transaction output (more commonly referred to as a "utxo") with a piece of property – a process known as "coloring", hence the use of the label Colored Coins as the name of the protocol.

Since the OP_RETURN field and use of multisigs is still limited and may be insufficient for the amount of data a user wishes to associate with a particular transaction, Colu's "coloring scheme" allows for association of unlimited amounts of metadata (e.g., the name, address, photo

[8] Luke Parker, 'Brazil pilots Bitcoin solution for real estate registration' (*Brave Newcoin* April 9, 2017) https://bravenewcoin.com/news/brazil-pilots-bitcoin-solution-for-real-estate-registration/ 31 July, 2017

[9] Email from Nathan Wosnack to Victoria Lemieux 27 July, 2017

[10] Email from Nathan Wosnack to Victoria Lemieux September 18, 2017.

[11] The Colored Coins protocol, and thus in theory the Ubitquity platform, is compatible with other blockchains such as Multichain, Ethereum, and Hyperledger.

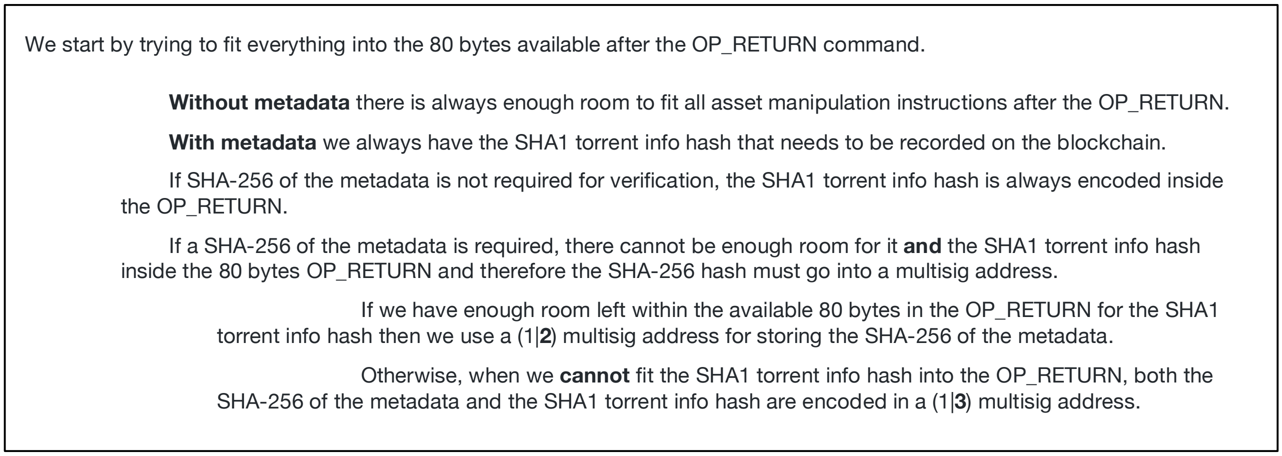
[12] 'Colored Coins' (*Bitcoin* Wiki 2015) https://en.bitcoin.it/wiki/Colored_Coins#Colu.27s_ColoredCoins.org_Block_Explorer accessed 31 July, 2017

[13] InterPARES Trust Terminology Project (n15)

[14] 'What are multi-signature transactions' (*Bitcoin Stack Exchange* 2017) https://bitcoin.stackexchange.com/questions/3718/what-are-multi-signature-transactions accessed 31 July, 2017; Note that, with the recent forking of the Bitcoin blockchain, block size, and thus the amount of data that can be stored on chain, has increased in the new BCC version of the Bitcoin blockchain.

of property, location data, property value, etc.) through the use of publicly available torrent files as described in Box 1.

Box 1. Recording Data using the Colored Coins Protocol, Colu API[15]



We start by trying to fit everything into the 80 bytes available after the OP_RETURN command.

Without metadata there is always enough room to fit all asset manipulation instructions after the OP_RETURN.

With metadata we always have the SHA1 torrent info hash that needs to be recorded on the blockchain.

If SHA-256 of the metadata is not required for verification, the SHA1 torrent info hash is always encoded inside the OP_RETURN.

If a SHA-256 of the metadata is required, there cannot be enough room for it **and** the SHA1 torrent info hash inside the 80 bytes OP_RETURN and therefore the SHA-256 hash must go into a multisig address.

If we have enough room left within the available 80 bytes in the OP_RETURN for the SHA1 torrent info hash then we use a (1|**2**) multisig address for storing the SHA-256 of the metadata.

Otherwise, when we **cannot** fit the SHA1 torrent info hash into the OP_RETURN, both the SHA-256 of the metadata and the SHA1 torrent info hash are encoded in a (1|**3**) multisig address.

In this way, data or metadata relating to the asset can be stored and associated with a transaction using BitTorrent. This is a peer-to-peer protocol in which peers coordinate to distribute requested files, much as Bitcoin nodes coordinate to record transactions on a distributed ledger. And, as with Bitcoin, peers can be located anywhere in the world. Data is uploaded to BitTorrent through a process called “seeding”, which, in theory, is handled by Colu. Ubitquity has successfully tested the seeding process. The continued existence of the data online depends upon at least one, preferably many, peers holding the downloaded data and continuing to participate in the public BitTorrent network. At time of writing, data and metadata relating to land transactions in the Municipality of Pelotas has not been seeded to BitTorrent and is, therefore, currently unavailable on the Internet.

Other possible methods of storing data linked to land transactions recorded through Ubitquity’s platform include establishing a private consortium to the seed torrents rather than using the public BitTorrent network, using another decentralized storage solution such as the Inter Planetary File System (IPFS), or – more traditionally - setting up centralized storage in the Cloud or in a database.

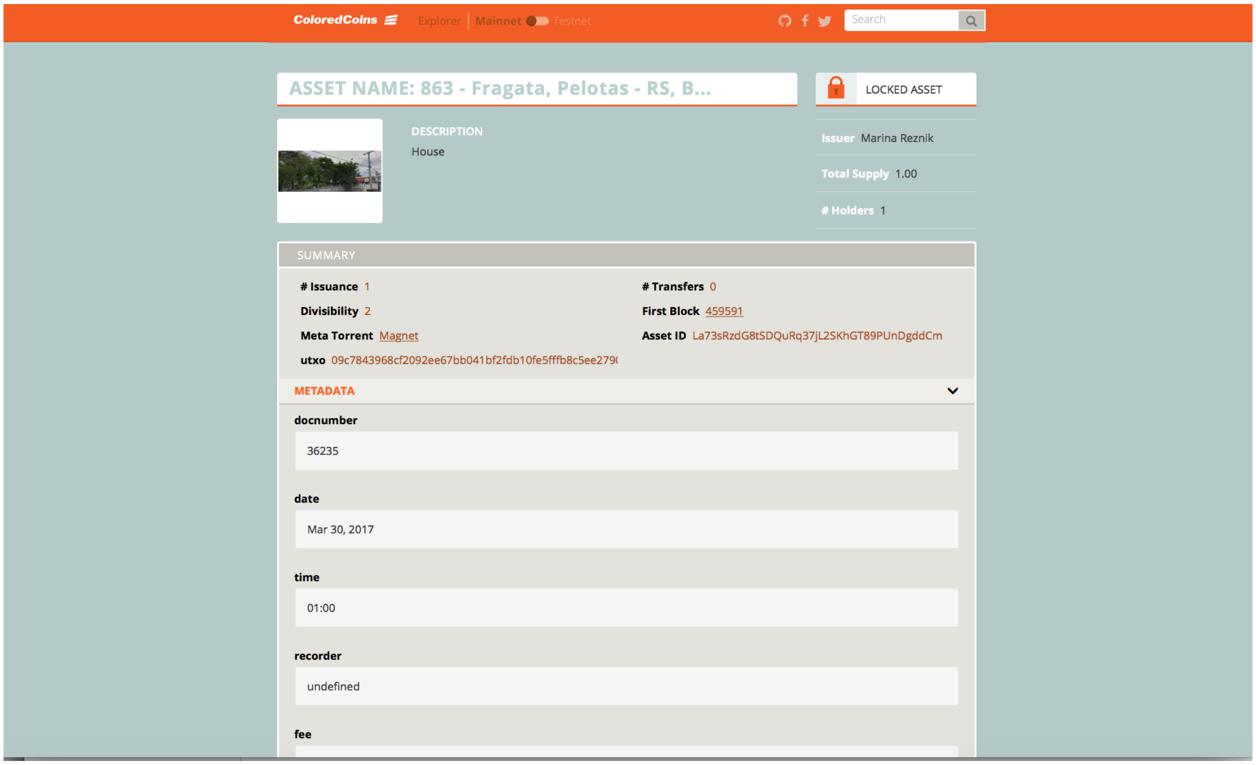
A magnet link (see Figure 4) is a hypertext link that contains information that the torrent client uses to find data linked to a blockchain transaction that a user wishes to download from BitTorrent. This link affords an easy way to download files from BitTorrent peers without the need to run a torrent server. Magnet links can therefore be distributed by email, messaging, web interfaces and other forms of communication to anyone in order to provide access to BitTorrent content.[16] Thus to download content, a user running a torrent client (e.g., µTorrent) is able to

[15] ‘Colored Coins – Colored-Coins-Protocol-Specification – Coloring Scheme’ (*Github* 2016) https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki/Coloring%20Scheme 31 July, 2017

[16] Martin Brinkman, ‘What Is A Magnet Link And How Does It Differ From Torrents?’ (*ghacks.net* June 5, 2010 edited December 2, 2012) https://www.ghacks.net/2010/06/05/what-is-a-magnet-link-and-how-does-it-differ-from-torrents/ accessed 31 July, 2017

enter the magnet link into their browser to begin downloading – as long as the content has been seeded to the BitTorrent network.[17]

Coloring of blockchain transactions facilitates easier identification, search and retrieval of those transactions as in the example at Figure 4. In this example, the property is represented by the Asset ID, which corresponds to a colored token. Conducting a title search involves searching for the Asset ID using the Colored Coin public search engine, which returns all the transactions involving that asset (see Figure 5). In this manner it is theoretically possible to see the title of ownership transferred to different people by going back through the transactional history of a specific coloured token (i.e., the one that represents the piece of property). In the example below, however, no transfer transactions are found because this entry represents the first recording of title to ownership on the blockchain. The UTXO hash provided in the search results also allows a user to search for the transaction, and check its validity, on the public Bitcoin blockchain as in the example in Figure 6.



ASSET NAME: 863 - Fragata, Pelotas - RS, B...

LOCKED ASSET

DESCRIPTION
House

Issuer Marina Reznik

Total Supply 1.00

Holders 1

SUMMARY

Issuance 1

Transfers 0

Divisibility 2

First Block 459591

Meta Torrent Magnet

Asset ID La73sRzdG8tSDQuRq37jL2SKhGT89PUnDgddCm

utxo 09c7843968cf2092ee67bb041bf2fdb10fe5fffb8c5ee279(

METADATA

docnumber
36235

date
Mar 30, 2017

time
01:00

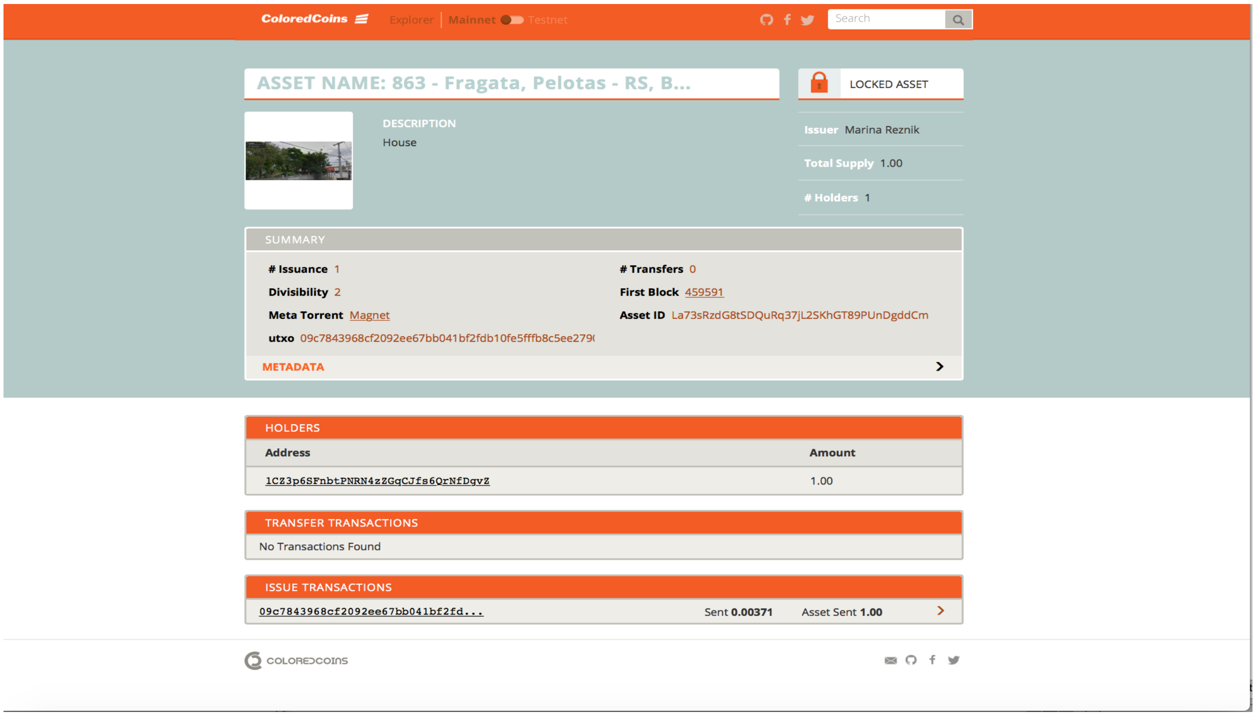
recorder
undefined

fee

Figure 4. Results returned for the March 30, 2017 transfer of a doctor's house using the Ubitquity Platform. The search was conducted using the Colored Coins public search engine for digital assets, based on the Colu Coloredcoins implementation.[18]

[17] Bram Cohen, 'The BitTorrent Protocol Specification' (*BitTorrent.org*, February 4, 2017) http://www.bittorrent.org/beps/bep_0003.html accessed 31 July, 2017

[18] See <http://coloredcoins.org/explorer/asset/La73sRzdG8tSDQuRq37jL2SKhGT89PUnDgddCm/09c7843968cf2092ee67bb041bf2fdb10fe5fffb8c5ee27909331d1eb6032852/0>



ASSET NAME: 863 - Fragata, Pelotas - RS, B...

LOCKED ASSET

DESCRIPTION
House

Issuer Marina Reznik

Total Supply 1.00

# Holders 1

SUMMARY

# Issuance 1

# Transfers 0

Divisibility 2

First Block 459591

Meta Torrent Magnet

Asset ID La73sRzdG8tSDQuRq37jL2SKhGT89PUnDgddCm

utxo 09c7843968cf2092ee67bb041bf2fdb10fe5fffb8c5ee279(

METADATA

HOLDERS

Address	Amount
1CZ3p6SFnbtPNRN4zZGqCJfs6QrNfDgvZ	1.00

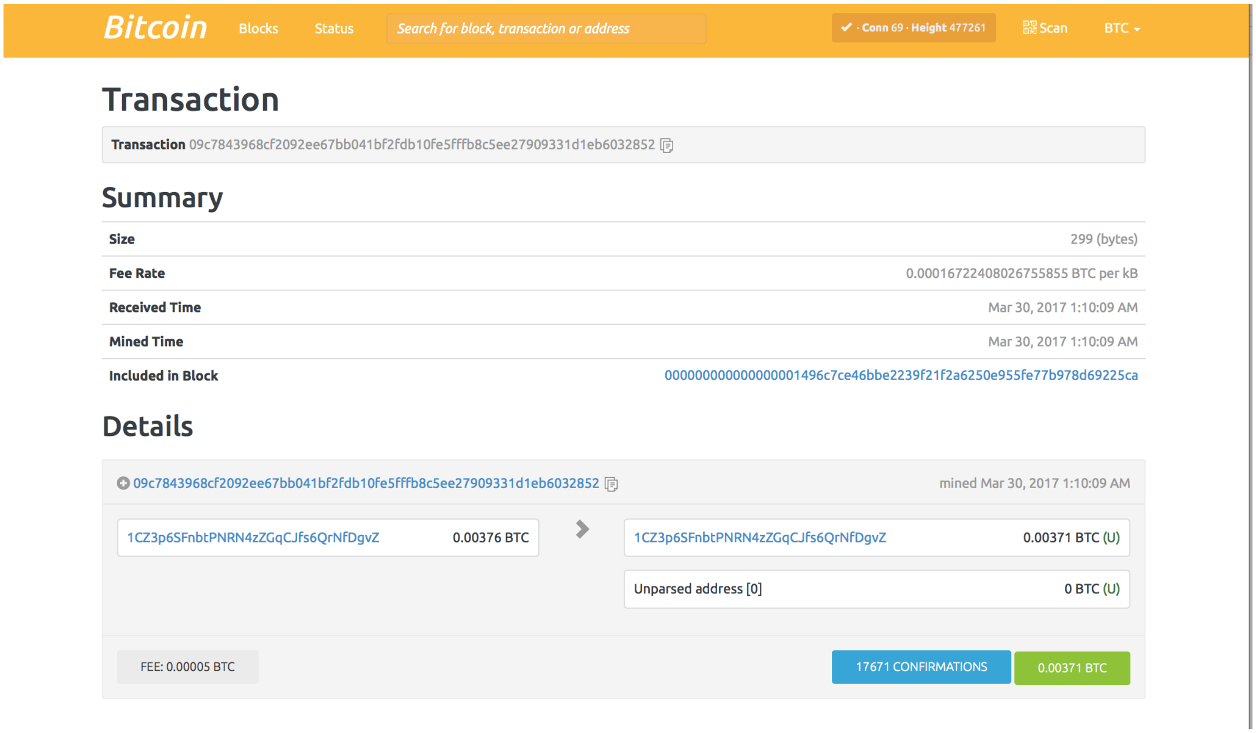
TRANSFER TRANSACTIONS

No Transactions Found

ISSUE TRANSACTIONS

09c7843968cf2092ee67bb041bf2fd... Sent **0.00371** Asset Sent **1.00**

Figure 5. Results for title search concerning the piece of land sold in the March 30, 2017 using the Colored Coins Block Explorer.



Bitcoin
Blocks
Status
Search for block, transaction or address
✓ · Conn 69 · Height 477261
Scan
BTC

Transaction

Transaction 09c7843968cf2092ee67bb041bf2fdb10fe5fffb8c5ee27909331d1eb6032852

Summary

Size	299 (bytes)
Fee Rate	0.00016722408026755855 BTC per kB
Received Time	Mar 30, 2017 1:10:09 AM
Mined Time	Mar 30, 2017 1:10:09 AM
Included in Block	000000000000000001496c7ce46bbe2239f21f2a6250e955fe77b978d69225ca

Details

09c7843968cf2092ee67bb041bf2fdb10fe5fffb8c5ee27909331d1eb6032852 mined Mar 30, 2017 1:10:09 AM

1CZ3p6SFnbtPNRN4zZGqCJfs6QrNfDgvZ 0.00376 BTC

1CZ3p6SFnbtPNRN4zZGqCJfs6QrNfDgvZ 0.00371 BTC (U)

Unparsed address [0] 0 BTC (U)

FEE: 0.00005 BTC

17671 CONFIRMATIONS

0.00371 BTC

Figure 6. Search results for the March 30, 2017 transaction using Bitcoin Block Explorer[19]

The solution does not incorporate records management or digital preservation and it does not serve as a digital repository; it only keeps the information about the property (real estate x owner) with a digital signature.

- *How does the blockchain work under the law?*

This section presents a discussion of some related legal and financial issues associated with the use of blockchains for recordkeeping.

Legal recognition, admissibility and weight

An "archivally" reliable record does not necessarily imply a legally reliable record. The record also must be recognized and accepted in law as a memorial of the transaction, which often requires updating relevant legislation to recognize blockchain-based land registration, as a number of jurisdictions have begun to do.[20] Among the laws that may need updating are those relating to the signing of contracts. Legal acceptance of digital signatures is a necessary precondition for acceptance of blockchain-based records as legally binding records of property transfers. In cases where physical signatures alone are acceptable, the law can present a barrier to using blockchain-based land transaction recording.[21] There is currently no state regulation recognizing blockchain-based land registration in Brazil. Study participants indicated that recognizing such records could be threatening to governments, because blockchain and Bitcoin is not vulnerable to political pressures, disintermediating enormous government power.

Data localization, protection and privacy

Data localization laws may stem from laws and rules requiring retention of documents at a business premise or from laws that address data protection and privacy in relation to technology.[22] For countries relying on storing elements of their public records on the Bitcoin Blockchain, or any blockchain not operating entirely within a particular country's sovereign jurisdiction, it is necessary to consider whether the system complies with data localization, data protection and privacy laws and rules. In the case of the Brazilian pilot, the platform's metadata files contain details of property transfers which are kept on a Colu server located in Israel.

[19] See <https://blockexplorer.com/tx/09c7843968cf2092ee67bb041bf2fdb10fe5fffb8c5ee27909331d1eb6032852
>

[20] Sheppard Mullen, 'Nevada Passes Pro-blockhain Law,' (June 14, 2017) http://www.jdsupra.com/legalnews/nevada-passes-pro-blockchain-law-15604/ accessed 31 July, 2017

[21] Mats Snäll (n 62) 7

[22] Nigel Cory, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?' (*Information Technology & Innovation Foundation*, May 1, 2017) https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost accessed 31 July, 2017

Although there are currently no laws or rules that preclude this architecture,[23] Ubitquity is actively looking at providers within Brazil in order to ensure adherence to good, ethical practice with data handling and in anticipation of possible data localization requirements.[24]

- *How does the blockchain affect others?*

There is no regulation in Brazil for Blockchain use as yet. Governments in general are afraid of this kind of technology, because Blockchain and Bitcoin enable the existence of a "central bank" regulated by mathematical formulas such as digital signatures. Moreover, it is not vulnerable to political pressures, which is perceived as taking away power from government.

When blockchain authenticates transactions between parties that do not trust each other, it gives the financial market what internet brought to information. It enables transmission of financial information instantly around the world at almost (supposedly) little cost.

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

This section presents an archival theoretic evaluation of the aforementioned solution.

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 7. Each of these characteristics is discussed below in relation to the solutions presented in the previous section.

[23] In September 2013, Brazil began considering a policy that would have forced Internet-based companies, such as Google and Facebook, to store data relating to Brazilians in local data centers. It withdrew this provision from the final copy of the bill. Furthermore, in 2016, Brazilian government agencies, including the Secretary of Information Technology of the Ministry of Planning, Development, and Management, have included forced data localization as a requirement for public procurement contracts involving cloud-computing services [See Cory (n 111)

[24] For guidance on good practice, Ubitquity has been following the 7 best practices by the American Land Title Association [See American Land Titles Association, 'ALTA Best Practices Framework: Title Insurance and Settlement Companies Best Practices, Version 2.5' (ALTA October 7, 2016)

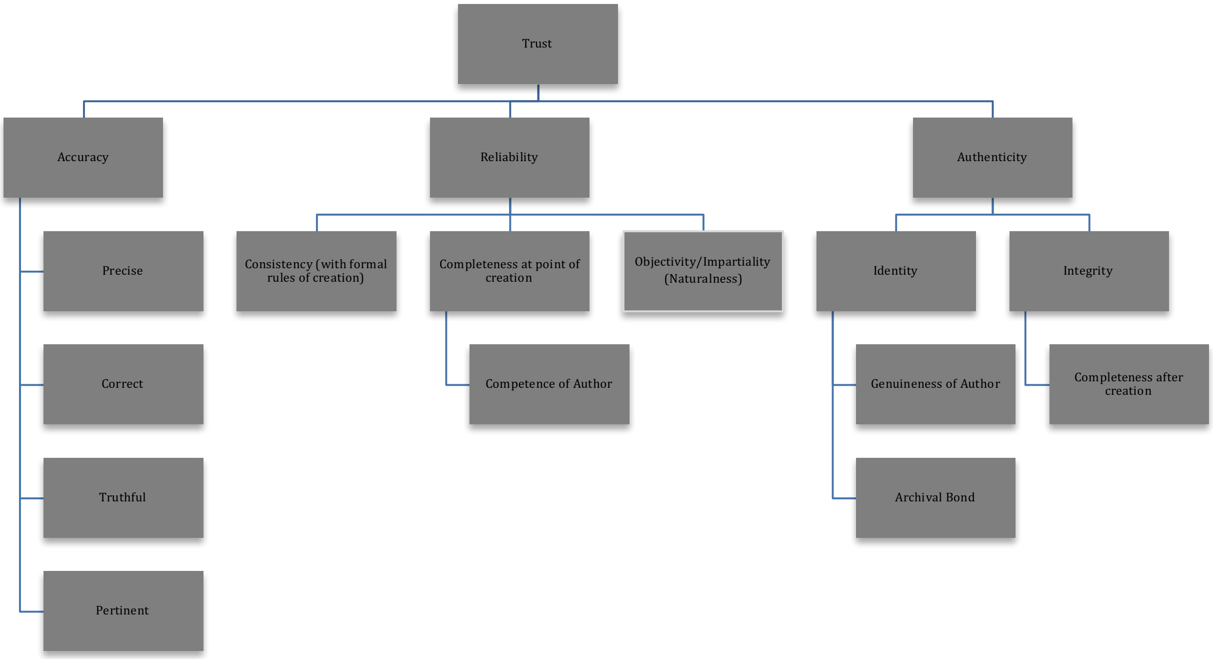

Trust
Accuracy
Reliability
Authenticity
Precise
Consistency (with formal rules of creation)
Completeness at point of creation
Objectivity/Impartiality (Naturalness)
Identity
Integrity
Correct
Competence of Author
Genuineness of Author
Completeness after creation
Truthful
Archival Bond
Pertinent

Figure 7: A taxonomy of key archival concepts and their relationship to trust[25]

Accuracy. Accuracy is "The degree to which data, information, documents or records are precise, correct, truthful, free of error or distortion, or pertinent to the matter."[26] Accuracy thus refers directly to the truth-value of the content (facts) of the record. Although one of the project's aims is to improve accuracy of land transaction records, there is *nothing inherent in the blockchain that fundamentally alters the accuracy of recording*. Rather, accuracy is dependent upon the procedural and technical controls over entry of data into these systems. If the data are derived *ex postfacto* from a land registry's registration database, as in the case of the current Ubitquity pilot in Brazil, accuracy of land transaction records depends upon the accuracy of the entries recorded in the original registry of land ownership as well as upon what is transcribed into the new blockchain-based land transaction recording system. It is possible to increase the accuracy of data transferred from such systems using system controls and audits. For example, where data are manually transferred from an original paper registry to a computerized blockchain-based system multisigs could be used to help improve accuracy of any data transferred into the blockchain by requiring that one key be used to record the entry and one or more keys be used to validate the correctness of the data entered into the blockchain system (i.e., a check that the data match). The roles could be divided between staff within the land registry itself (i.e., one data entry clerk and one quality control clerk) or between staff within the land registry and the company providing the blockchain-based recording system. For cases where data are transferred from a computerized registry into a blockchain-based system, an original record in the registry could be hashed and automatically compared with the hash of its mirror entry in the blockchain-

[25] Author's own rendering

[26] R. Pearce-Moses, (ed) 'Accuracy' In InterPARES Trust Terminology Database (2017) http://arstweb.clayton.edu/interlex/expandedSearch.php?term=accuracy accessed 6 April, 2017

based land transaction recording system. A comparison of the hashes would ensure that the records match before a final commit to the blockchain. Proof of the accuracy of the blockchain-based records could be affixed as metadata to the blockchain transaction record (i.e., by including the hash of the original record with the metadata associated with the blockchain transaction). This could be designed to work in a manner similar to how the Colu Colored Coin protocol handles the insertion of hashes of data seeded to BitTorrent described in Box 1. Note that this approach would only ensure that the land transaction records have been accurately transcribed from the original registry into a blockchain-based system, not that the original records were accurate in the first place.

If the data are derived contemporaneously with a land transaction, such as by means of end user input or data drawn from linked systems (cf. Swedish Land Registry pilot), accuracy depends upon the degree to which data from originating sources are precise, correct, truthful, etc. In such cases, increasing the probability that data will be accurate relies upon establishing data entry input controls and constraints (e.g., uniqueness constraints, logical value constraints, etc.) and requirements for linking to transaction records that support or corroborate the truthfulness of data entered into the system (e.g., the requirement to upload and attach digital copies of property deeds.

One question that frequently arises with respect to the treatment of records on the blockchain is what to do when inaccurate information has been discovered. Since the blockchain is intended to provide an immutable ledger, information cannot (or, more accurately, should not) simply be overwritten or updated as with traditional database technology. None of the information gathered about the solution has so far indicated how this requirement will be handled, but in other solutions corrections to transactional records on the blockchain are being made by entering a transaction that corrects the information. One challenge with this approach is ensuring that an end user or linked system is accessing the latest version of a transaction. For example, if a user is retrieving information using the utxo hash (transaction A) but there has been another transaction (transaction B) which has updated information relating to the previous hash, a search using the hash for transaction A may not reveal the existence of transaction B and the user may only see the outdated information. The risk of this occurring is less likely when assets are colored, since a user is able to search for all transactions relating to that asset and thus would be able to see a transaction updating information relating to an earlier transaction. In principle, any solution which instantiates and preserves the archival bond (see below) should be able to address this issue in a similar manner. However, an unresolved issue occurs in a scenario involving the use of the original, erroneous transaction in a downstream, unlinked system or manual transaction (e.g., use of the land title as security for a loan). In such a scenario, the downstream transaction may be invalidated by the inaccuracy of the supporting blockchain-based record. In this case, it will be incumbent upon those who must have accurate information on ownership of land to see subsequent certification of land title (e.g., through requesting a certificate of title from the land registration authority).

Reliability. In archival science, the term reliability refers to "the trustworthiness of a record as a statement of fact; that is, to *its ability to stand for the facts it is about* (emphasis added)."[27] Thus, an original copy of a land title registration stands for the transfer of title to a piece of land to a

[27] Luciana Duranti and Corrinne Rogers, 'Trust in digital records: An increasingly cloudy legal area' [2012] 28.2 *Computer Law & Security Review* 525

new landholder. In some jurisdictions, registration is the act that actually gives effect to the land transfer; in other jurisdictions, registration serves only to provide proof that the act has taken place (in a manner similar to the registration of an act of marriage), and execution of a document transferring deed of title gives effect to the land transfer.

One important sub-component of reliability is the existence of formal rules of procedure for the creation and keeping of records, and proof that a given record was made and kept in a manner consistent with such procedures. In the case of land transaction records, these procedures – at least at a high level – are defined by law.

At present, the consistency of the records retained on the Ubitquity platform - wherein data are entered *ex postfacto* from the original land registry - with formal procedures for creation and keeping of records depends upon two conditions: 1) consistency of the original records on which the blockchain records are based with formal rules of records creation and keeping, as defined in law and 2) the existence of formal rules of creation for reliably generating the "mirror" records on the blockchain system. Rules for the completion of a registration and its recording in a property registry are defined in Title IV, Chapter 2 of Law Number 6.216 of 30 June, 1975.[28] Rules for generation of "mirror" records on the Ubitquity platform have not yet been worked out, given the newness of the pilot project, but will be needed to ensure that creation of the blockchain-based registration record is compliant with legal requirements and that initial reliability is not lost in the process of transcribing pre-existing records to the blockchain. Table 1 presents a comparison of these rules with the metadata entered into the Ubitquity system. There is significant variation in what is captured in the Ubitquity platform with what is required by law for the registration of the property, which, if legally required information were missing, or the information in the Ubitquity platform were not to match what is recorded in the register, could lead to a legal dispute challenging the validity of the registration.

Table 1. Comparison of registration recording requirements under Brazilian Law with Metadata recorded in Ubitquity blockchain solution for property transfer recording

Registration Requirements	***Registration Recording Requirements***	***Ubitquity Metadata***
Order number	N/A	Document number Book number (RG2)
Date	Date	Date
N/A	N/A	Time
N/A	N/A	Recorder (undefined)
		Fee (field empty)
Identification of the property, made by indicating its characteristics	NA	Mailaddress (863 - Fragata, Pelotas - RS, Brazil) Parcel number (61)

[28] Government of Brazil, Lei No. 6.216 (n 41)

and confrontations, location, area and denomination, if rural, or street and number, if urban, and its cadastral designation, if any		Class (Rua) Zoning (field empty) School (field empty) Latitude (field empty) Longitude (field empty) Structure (field empty) Occupancy (field empty) Use (residential dwelling) Units (1) Condition (field empty Fire (field empty) Damage (field empty) Trespass (field empty) Maintenance (field empty)
Name, domicile and nationality of the owner, as well as:	The name, domicile and nationality of the transferor, or of the debtor, and of the purchaser, or creditor, and:	Grantor (field empty) Grantee (personal name of the grantee included)
In the case of an individual, the civil status, the profession, the registration number in the Physical Register of the Ministry of Finance or the General Registry of the identity number or in the absence thereof, its membership	In the case of a natural person, the civil status, the profession and the registration number in the Physical Register of the Ministry of Finance or the General Registry of the identity card, or, failing that, his / her membership	No separate field for profession/civil status but this information is indicated in the Name field. Corroborating identity information is not provided.
In the case of a legal entity, the registered office and the registration number in the General Register of Taxpayers of the Ministry of Finance	In the case of a legal entity, the registered office and the registration number in the General Register of Taxpayers of the Ministry of Finance	N//A
N/A	Title of the transmission or the burden;	
Previous registration number.	N/A	N/A

N/A	Form of the title, its origin and characterization;	Deedfile (field empty) Deedfile2 (field empty)
N/A	Value of the contract, of the thing or the debt, term of this, conditions and more specifications, including interest, if any.	Sale price (field empty) Land value (6141000) Bigdvalue (field empty) Assessdate (field empty)
N/A	N/A	Icon (image) (link to an image of the property)

Another important aspect of archival reliability is completeness. In archival terms, completeness is linked to the transactional nature of records and refers to the presence of all the elements required by the creator and a legal-administrative system for the record to be capable of generating consequences.[29] This typically includes signatures and dates of creation.[30] Thus, a contract for sale of land that does not possess a signature and date would not be considered complete. Legal acceptance of digital signatures is still a barrier in many jurisdictions, and is one of the factors that is holding back the transition to full implementation of blockchain land recording in Brazil. Dating of land transaction records is also potentially an issue in blockchain land registration. Although blockchain transactions are time ordered, and often time stamped, system generated time stamps may be out of sync with or unrelated to calendar time. Further, the timing of the actual validation of transactions may be subject to factors unrelated to the actual timing of a land transfer (e.g., length of time it takes to mine a transaction).[31] Thus, it may be necessary to create an additional link between a transaction and calendar time through, for example, publication of the transaction hash in a newspaper.[32]

A trustworthy record is also one that possesses physical and formal elements which are consistent with authentic records of similar type and provenance (e.g., in paper recordkeeping systems, whether the ink used to write a document is contemporaneous with the document's purported date, or whether the style and language of the document is consistent with other related documents that are accepted as authentic).[33] With blockchain recordkeeping forms being very new and, as yet, lacking in standardization, especially in the context of pilot projects, there is the possibility of inconsistency of formal elements even between records of the same type and provenance.

[29] R. Pearce-Moses (ed), 'Completeness' in InterPARES Trust Terminology Database (2017) http://arstweb.clayton.edu/interlex/expandedSearch.php?term=completeness accessed 6 April, 2017

[30] Luciana Duranti, 'Reliability and authenticity: the concepts and their implications' [1995] 39 *Archivaria* 5-10.

[31] Gallego (n 21)

[32] This is an approach employed in Enigio and Guardtime blockchain solutions, for example

[33] Ibid

Reliability also depends on the competence of a document's author to carry out a transaction and hold power sufficient to give effect to that transaction's intended outcomes.[34] It must be possible to establish that the parties entering into the contract consent to enter into the contract freely, that they were not incapacitated or limited in the powers to enact the transaction, that the parties were of sound mind, and that if they went through a legal representative, that representative had the power to act.[35] It is difficult to imagine how a blockchain system alone could be used to establish such facts.

What can be achieved within the scope of a blockchain system, having independently verified the competence of the parties to the transaction, is the establishment of procedures which strictly determine which users should be allowed to modify information relating to a piece of land. Clearly, to prevent fraud and to avoid losing the ability to further transfer ownership of an asset, this must be tightly controlled and carefully thought out, both in relation to a scenario where the land registration authority alone (or agent operating on its behalf) records the information as well as for a situation in which multiple stakeholders update information as the process of transferring title proceeds (e.g., the future state proposed for the Brazilian pilot or the current status of the Swedish pilot).

In any system, such as blockchain-based land transaction recording, that relies on cryptography, he who holds the key, in theory holds the power to transfer land, although in practice this depends on how the system is procedurally designed and the specific requirements for legal transfer of property within a given jurisdiction. Key management includes consideration and design of processes and technical features of key generation, exchange, storage, use and replacement of keys. In a system where each property is associated with a token and a Bitcoin address, potentially millions of keys must be accessible, linked to a competent and legally responsible authority, resistant to digital theft and resilient to loss or inaccessibility (i.e., when a death occurs and the heirs do not have access to the key). These requirements have often been difficult to meet in cryptographic systems, and there is no reason to expect that it would be any easier in a blockchain system.[36] The complexity of key management potentially leaves private keys, such as those created to support blockchain-based systems, vulnerable to loss, open to theft, and subject to exploitation.

To illustrate, it would be undesirable if a single private individual (e.g., the purchaser of a property) were to hold the private key that ultimately records his own ownership of title, since it may be possible for such individual to record fraudulent or inaccurate information, or to confer upon himself recording power that exceeds what he is legally competent to effect under the law. To protect against potential fraud, the registration authority has a continuing role to play in ensuring that this does not happen by assuming some oversight of the recording process. Registration authorities have a role to play in this regard because, in theory at least, they are disinterested in the outcome of transactions, and therefore, able to act as trusted intermediaries. In the case of the Ubitquity pilot in Brazil, Ubitquity holds the private key, acting as the designated (but not yet legally recognized) agent of the real estate registration authority, and is

[34] Duranti and Rogers (n 68)

[35] Gallego (n 21)

[36] S. Eskandari, D. Barrera, E. Stobert, J. Clark, 'A First Look at the Usability of Bitcoin Key Management' (*USEC 2015*, San Diego, CA) http://www.internetsociety.org/sites/default/files/05_3_3.pdf accessed 21 November, 2015

recording ownership of the property. This arrangement is only temporary due to the preliminary stage of the pilot. Conferring oversight of the blockchain registration process on the registration authority does not assure complete protection from fraud or misuse, however. In practice, registration authorities may also be bad actors. For this reason, good practice suggests that it would be wise to adhere to the "four eyes" principle in which two individuals (at least) involved in the property transfer process must sign off on a transaction in order to have it recorded in the blockchain. This approach reduces the possibility of fraudulent or inaccurate recordings.

Bitcoin software manages several private keys by storing them on a node's local storage in a file or database in a pre-configured file system path. A file containing private keys can be read by any application with access to the user's application folder. Attackers may exploit this to gain immediate access to the transaction records. Users must be careful to not inadvertently share their Bitcoin application folder (e.g., through peer-to-peer file sharing networks, off-site backups or on a shared network drive), and must also be cautious about the possibility of physical theft when using portable computers or smartphones.[37] In the Ubitquity pilot, all current private keys are backed up and encrypted in cold storage off device to prevent such exploits. To access a land holder's private keys on the platform an attacker would need to break through the "*nix "server, bypassing Ubitquity's .htaccess security. The ultimate goal is for the Ubitquity API to link directly into Cartorios and e-recording companies without a front-end platform as an attack vector.[38]

Another threat is loss of keys as a result of general equipment failure due to natural disasters and electrical failures, acts of war or mistaken erasure (e.g., formatting the wrong drive or deleting the wrong folder).[39] To prevent loss of control of an asset, and the inability to transfer it to new ownership in future, it is likely a good policy to design a multisig system wherein two of three signatures is required to unlock and sign a transaction. Currently, Ubitquity holds the private keys for the pilot solution, since it is very early days in the testing of the prototype. However, the solution's technical road map includes plans to implement multisig with the options of 2-of-3 and 3-of-5 multisignature.[40] Future plans for key management will include a feature to allow for an escrow holding, home owner holding, and another party such as another duly designated representative (lawyer, spouse). This way, if one of the users who usually signs the transaction loses their private key, or the key is compromised, two other users can sign the transaction instead to make sure that it completes – essentially a "breakglass" procedure. If one of the authorities loses their private key, a challenge will be to manage key re-issuance. This may be a simple matter of transferring the asset to a new address or wallet with a new private key over which the signing authority has control.

Reliability also depends on reliable operation of a system and all of its component parts. One of the most important aspects of reliability is determined by the manner in which the nodes on a blockchain network determine the validity of transaction entries and blocks of transactions, otherwise known as the consensus mechanism. These consensus algorithms may be untested and

[37] Ibid

[38] Email message from Nathan Wosnack to Victoria Lemieux, September 18, 2017.

[39] S. Eskandari et al (n 78)

[40] Email message from Nathan Wosnack to Victoria Lemieux, September 18, 2017.

may not always perform reliably to validate transactions.[41] In the case of the Ubitquity pilot, which currently records transactions using the Bitcoin network, validation is made easier by the relatively open and transparent nature of the network.

The Ubitquity solution is, in principle, blockchain platform agnostic, meaning that transactions could be recorded in future using Ethereum, Hyperledger or some other blockhcain platform. Some caution is required in this regard, however, because there are non-trivial variations in the way in which the consensus algorithms work across these platforms, even in cases when the blockchain uses the same general approach to transaction validation. For example, Bitcoin and Ethereum currently both use the "Proof of Work" consensus mechanism, but there are importance differences in the design of their algorithms which result in different behaviour of the nodes on the network.[42] Benchmarking the performance of consensus algorithms to ensure reliable validation of transactions is thus a necessary development in the advancement of blockchain technology and an ongoing area of research.

Security vulnerabilities in blockchain solutions also can prevent reliable operation of the system. A detailed information technology security risk analysis of the solution goes beyond the scope of this paper; however, it is worthwhile highlighting security risks to which solutions may be prone given their decentralized and distributed architectures. One such vulnerability is the possibility that a miner on the Bitcoin network or set of colluding miners gains 51% of mining power – called a 51% attack. If this occurs, then validity of transactions recorded on the blockchain is open to manipulation.[43] Given this, it is crucial to ask whether concentration of Bitcoin miners (nodes that validate transactions) with their combined computing power could allow collusion among nodes and erode the basis of trust upon which the blockchain solution is built.

Whenever one system passes information to another system there exists a possibility for a Man-in-the-Middle Attack (MitMA).[44] MitMA occurs when an attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other. In the case of the Ubitquity solution, there are two points, where the solution may have been vulnerable to a MitMA. The first is at the point at which a new land registration entry (an entry) in the registration database system enters the Ubitquity solution, particularly if the transmission is unencrypted. The second is at the point at which the solution anchors the transaction in the Bitcoin Blockchain. Since Bitcoin miners do not audit these transactions for validity, it is possible to insert invalid transactions designed to look like valid transactions into the Blockchain. The probability of this type of attack is more likely in an environment where system hacking is already occurring, and where the data may pass between systems in unprotected form.

Another potential vulnerability is a SYN Flood attack, which is a form of Denial-of-Service attack in which an attacker sends repeated, rapid SYN requests to a target's system in an attempt

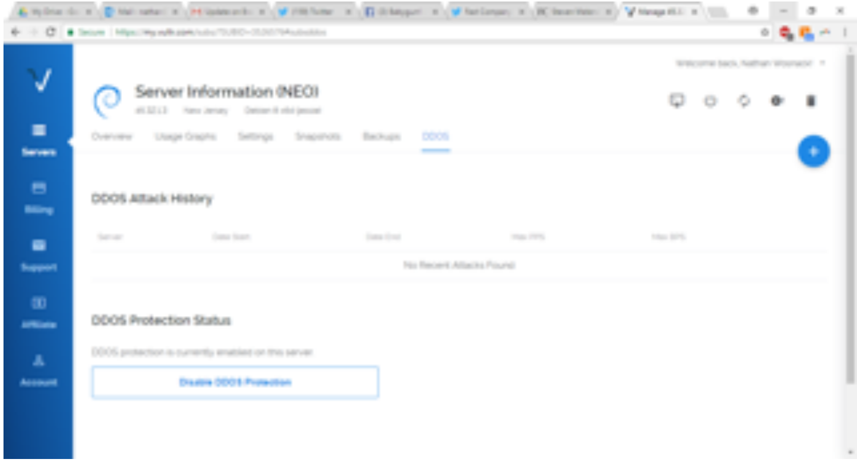
[41] Christian Cachin and Marko Vukolic, 'Blockchain Consensus Protocols in the Wild' (*Arxiv* July 17, 2017) https://arxiv.org/pdf/1707.01873.pdf accessed 17 July, 2017.

[42] Bitcoin does not require the mining of uncles – orphaned chains – on the network; whereas, Ethereum does. This is in order to ensure that the faster speed of transaction processing on the Ethereum network does not generate a large number of unconfirmed transactions and forks that created multiple competing versions of the truth.

[43] Arvind Narayanan, Joseph Bonneau, Edward Felton, Andrew Miller, and Steven Goldfeder (n 21)

[44] Shon Harris and Fernando Maymi, *CISSP Exam Guide, 7th Edition* (McGraw-Hill, 2016) 217-218

to consume enough server resources to make the system unresponsive to legitimate traffic.[45] A SYN request is made when a server requests a connection to communicate with another server by sending a SYN (synchronize) message to the server. This is followed by a "handshake" procedure in which the two servers acknowledge one another. In a SYN Flood attack the server receiving the request is unable to complete the handshake procedure before a new request comes in, which ultimately floods the server's resources with requests and causes it to become unresponsive. Although the Bitcoin Blockchain has implemented several measures to prevent denial-of-service attacks, such as SYN Flood attacks[46], it is still difficult to rule out such attacks, especially in a technology solution that relies heavily on broadcast of communications over a public network. As it seems to imply that Bitcoin is perhaps not protected against SYN Flood Attacks. Ubitquity servers have implemented SYN Flood protections for its website and platform, and have anti-DDoS solutions in place at its internet provider level at Vultr:



Server Information (NEO)

DDOS Attack History

Server	Date Start	Date End	Max PPS	Max BPS
No Recent Attacks Found				

DDOS Protection Status

DDOS protection is currently enabled on this server

Ubitquity also utilizes the CloudFlare Content Delivery Network (CDN) for traffic providing an extra measure to address SYN attacks. Very likely similar measures are in place at Colu, although this has not been confirmed.[47]

A Sybil attack occurs when an attacker fills a Blockchain mesh network with nodes controlled by him, which increases the probability of connecting only to attacker nodes.[48] This type of attack can allow an attacker to refuse to relay blocks and transactions, even disconnecting an entry registration communication from the network. It can also allow an attacker to relay only blocks that he creates.[49] The probability of this type of attack is likely increasing with growing use of pools of miners.

[45] Harris and Maymi (n 84) 696-697

[46] Bitcoinwiki, 'Block Hashing Algorithm' (*Bitcoinwiki* 2015) https://en.bitcoin.it/wiki/Block_hashing_algorithm 21 November, 2015

[47] Email from Nathan Wosnack to Victoria Lemieux, September 18, 2017.

[48] 'Weaknesses' (*Bitcoinwiki* 2011) https://en.bitcoin.it/wiki/Weaknesses#Sybil_attack accessed 21 November, 2015

[49] Ibid

In the Bitcoin Blockchain, each individual block contains a list of transactions and a timestamp representing the approximate time the block was created, among other additional information. The block timestamps allow the system to regulate the production of Bitcoins and generate proof of the chronological order of the transactions as a guard against the double-spending problem. Nodes usually calculate the timestamp based on the median time of a node's peers, which is sent in the version message as nodes connect.[50] Given the reliance of Blockchain technology upon timestamps, it is extremely important that the counters of all the nodes that keep track of the network time be working properly in order to prevent timestamp errors. In addition, even when the counters are working properly, it is possible for an attacker to slow down or speed up a node's network time counter by connecting as multiple peer nodes and reporting inaccurate timestamps.[51] Similar to Sybil attacks, growing concentration of Bitcoin miners may increase the probability of this type of attack.

It must be emphasized that the above analysis by no means represents a complete security risk analysis. It is merely meant to illustrate some of the security risks to which the solution may be subject or more prone.

Finally, reliable records will possess naturalness. This refers to the fact that, typically, records are generated in the course of business or daily life, and are thus not usually designed purposefully to disseminate knowledge or opinion, like, for example, books or other publications. As such, they have traditionally been thought to possess qualities of unselfconsciousness that underpin their reliability as records.[52] This notion relates to the legal “business records exception to hearsay” rule in common law, which accepts a record as standing for the facts referred to in it by virtue of the naturalness of its creation.[53] From this perspective, a system that generates blockchain-based records in real-time as an integrated element of the buying and selling of property, such as the proposed future state for pilot project, is superior to a system that transcribes land registration information from an existing paper-based or computerized land registry, as in the current state of the pilot project. That said, the simple transcription of information from an existing system onto the blockchain can be a useful incremental path of progression to blockchain-based systems supporting a business network given the fact that changes to laws, procedures and the interaction of stakeholders must all be developed and agreed in advance.

Authenticity.

To be considered trustworthy, records must also be judged to be authentic. Archival authenticity is defined as “the trustworthiness of a record as a record; i.e., the quality of a record that establishes that it is what it purports to be and that it is free from tampering or corruption.”[54] There are two preconditions for authenticity: identity and integrity of the record.

[50] Culubas, ‘Timejacking & Bitcoin’ [2015] http://culubas.blogspot.com/2011/05/timejacking-bitcoin_802.html accessed 21 November, 2015

[51] Ibid

[52] Luciana Duranti, Reliability and authenticity: the concepts and their implications [1995] 39 Archivaria 39 5-10

[53] Heather MacNeil, Trust and professional identity: narratives, counternarratives and lingering ambiguities’ [2011] 11 *Archival Science* 3, 4

[54] InterPARES Trust Terminology Project (n 8)

Authenticity encompasses the idea that that the origin or authorship of a record is genuine. For a record to be considered authentic, it must have been created by the individual represented as the creator. The presence of a signature, whether it be physical or digital, serves as a test for authenticity; the signature identifies the creator and establishes the relationship between the creator and the record. Note that, in archival authenticity, genuineness of the creator of the record does not imply or provide a basis for inferences about the truth-value of the facts in the record; it merely establishes that the purported creator of the record is genuine.[55] An important requirement to ensure that blockchain transactions have been duly and legally executed is to ensure that each address or wallet can be unequivocally linked to the competent signing authority (e.g., a land registration office). This requires integration of an identity management layer into a blockchain-based land transaction recording solution, an aspect of system functionality that is not yet well defined for this project. It is also necessary to ensure that, if the creator of a blockchain record, typically a land registry office, has held more than one address or wallet for a given asset (i.e., piece of land), that control of each of these addresses or wallets can be traced back to the competent authority in a continuous unbroken chain of control.

The unique identity of a record as a record is established by the instantiation and maintenance of the archival bond. A record is an "intellectual object" that is "made or received in the course of an activity as an instrument or a byproduct of such activity, and set aside for action or reference."[56] Thus, "a record has a determinate relationship to the activity of which it is a record, to the actor who kept it as a record and to other records of the same activity. This relationship, called the "archival bond," not only relates a record to a specific context of creation and use but also defines the Archival Aggregate in which it belongs."[57] In paper-based systems the archival bond often has been established by placing documents relating to the same transaction in the same physical folder or bundle. Without reference to the archival bond, it is impossible to tell if a record is genuine or a forgery. The existence of these linkages, moreover, permits the subsequent reconstruction of a logical chain of events, based on authentic evidence, of relationships between and among the facts pertaining to those events. To instantiate the archival bond in a blockchain-based record keeping system, such systems must establish links between the records, their creators, the transactions that give rise to them, and to other records that form part of the same relationships.

In the Ubitquity solution, the link between a given blockchain record and its originating transaction is established via the colouring of the token representing a particular piece of land. This allows a user to search for transactions relating to a particular property (e.g., as represented by an Asset ID), which corresponds to a colored token. Conducting a title search for all those transactions related to that property, then, involves searching for the Asset ID using the Colored Coin public search engine.

Association of all records relating to the same creator and/or transaction is a more challenging proposition. In the Brazilian case study, the entry in Ubitquity's platform, in theory, links back to a series of documents that are required to ensure that the transfer process has been duly and

[55] Duranti (n 94) and MacNeil (n 95)

[56] International Council on Archives, *ISAAR (CPF). International Standard Archival Authority Record for Corporate Bodies, Persons and Families 2nd. Ed* (ICA 2004)

[57] Ibid

legally carried out.[58] Ideally, all of this documentation, whatever its form, would be linked together and easily retrievable as a set of archival documents relating to a particular land transaction. This bond is established by embedding a link to the information stored on the Colu server or, optionally, BitTorrent, into the transaction record. One challenge is to ensure that these links remain live and are not broken. If the torrent files are kept on private servers, then the information will not be publicly retrievable using the Colored Coins explorer, but would still be retrievable through the platform interface assuming that the servers remain operational and the information is backed up in case of outage. Regular testing is necessary to ensure these requirements are met.

Integrity is also necessary to establish the authenticity of records. If the integrity of a record is compromised, it is impossible to establish a record's genuineness with any degree of certainty.[59] In the pre-digital era of land registration, integrity controls included numbered entries in registers, listing file contents, and numbering individual documents in file folders. In the digital era, the concept of integrity has expanded to include continued reliable operation of information systems in which records are created and maintained, and access controls and systems security controls to prevent tampering. Assuring integrity in such systems consists of a broad range of measures such as access controls and user authentication and verification to prevent tampering, audit trails, and documentation that demonstrates the normal functioning, regular maintenance, and frequency of upgrades of records systems.[60] An illustration of the type of controls that protect integrity of the record is provided by the Ubitquity solution, which currently relies upon the Colu Colored Coins protocol. In this solution, Both the SHA-1 hash of the information stored on BitTorrent and a SHA-256 hash of the SHA-1 hash are included in the metadata recorded with the transaction anchored in the Bitcoin blockchain in order to ensure that the BitTorrent data retains integrity and that what is retrieved from the BitTorrent is the correct information related to the blockchain transaction.

One of the main arguments for blockchain technology is that it assures tamper proof recordkeeping by virtue of the manner in which transactions are recorded and validated (i.e., in a Proof of Work based platform, such as Bitcoin, through solving of a cryptographic puzzle that permits detection of any alteration to transaction records after they have been validated). However, it is not inconceivable for a validated transaction to be overturned after the fact. One of reason that this might occur is governance of the blockchain. In theory, the blockchain is self-

[58] In the case of Brazilian land registration, the documentation includes obtaining a 20-year certificate (Certidão Vintenária); obtaining the certificates of Certificates of Registries and Disputes (Certidão dos Cartórios de Protestos), Acquire a Civil Distributor's Certificate (Certidão dos Distribuidores Cívies), a Fiscal Executive Certificate (Certidão de Executivos Fiscais) and a Bankruptcy Certificate (Certidão de Falencias e Concordatas) from the City Court Office; requesting a Land-Tax Certificate and a Cadastral Certificate (Certidão de Dados Cadastrais do Imovel)from City Hall; acquiring a Clearance Certificate from Tax Agency and a Federal Tax Clearance Certificate; paying transfer tax (ITB I) at the Bank; drafting of Public Deed of Purchase and Sale (Escritura Pública de Venda e Compra) by a Public Notary (Tabelião de Notas); updating the land taxation records (IPTU – Imposto Predial e Territorial Urbano) to the new owner's name at City Hall; and registering the escritura (transfer deed) at the appropriate Real Estate Registry with jurisdiction over the property to finalize registration and name change [See, Government of Brazil. *Lei Nº 6.216* (n 41)].

[59] InterPARES 2, 'Glossary' [n.d.] http://interpares.org/ip2/ip2_terminology_db.cfm accessed 31 July, 2017

[60] International Organization for Standardization (ISO), TC 46/SC 11. *ISO 15489-1:2016. Information and documentation. Records management. Part 1: General 2st ed.* (International Organization for Standardization 2016)

governing, but in practice, its operation is often in the hands of a core group of developers as recent disputes and action relating to the "forking", or division, of the Bitcoin blockchain illustrate.[61] Authorities intending to rely upon blockchain-based recordkeeping must consider the effect of forks and related decisions on the integrity of land transactions records. Given the uncertainty of relying on public blockchains over which it may be virtually impossible to exercise control, many organizations are turning to implementing their solutions using private, permissioned blockchains wherein governance is the responsibility of a consortium of bodies. This does not eliminate threats to the integrity of blockchain records presented by hard forks or forced editing of the ledger, but it does present the possibility to establish rules of operation and procedures for any necessary changes to what is intended to be an immutable record.

Persistence and Preservation

For archival purposes, all of the aforementioned attributes of blockchain records must be made to persist through space and time; that is, they must be preserved. Within the digital preservation community, it is recognized that preserving the integrity of the bit structure of data is not a sufficient form of preservation because semantic loss may prevent later interpretability and accessibility. To illustrate, it may be possible to preserve a bit stream of a digital version of a land title, and even to preserve the software that renders the bit stream interpretable, but the ability to understand the significance and meaning of the bits depends upon preservation of information about the context of their creation in order to render them interpretable and also so that the record does not lose its real world effect, such as conferring a title.[62] It is, moreover, possible to have some degree of bit loss without a detrimental impact upon "renderability", interpretability, or effect. This understanding characterizes the archival notion of completeness after creation. Digital records preservation therefore involves preservation of the integrity of the identity of records, through preservation of the archival bond, in addition to preservation of the integrity of the general semantic context, content, and form of data. Though it is tempting to think of digital preservation as a legacy issue and thus something that can be dealt with at a later point of time, there is now widespread consensus that digital preservation must be designed into systems.

Digital preservation challenges present themselves in the case of the Ubitquity solution for the Brazilian pilot. In this case, the components of the system – and the records created and stored on the system - are loosely coupled, have independent governance, independent lifecycles, and independent technical features. This creates a complex socio-technical environment for recordkeeping that problematizes the work of ensuring long-term preservation and access. As currently configured, long-term preservation depends on long-term cooperation and coordination among the Brazilian land registry, a US-based blockchain startup (Ubitquity), and an Israeli blockchain startup (Colu). The geopolitical challenges alone are daunting. This is not to suggest that such challenges cannot be overcome, as discussed above in regard to Ubitquity's plans to alter the solution architecture to support adherence to any data localization rules; rather, they must be squarely addressed in order to design future ecosystem architectures capable of long-

[61] Alyssa Hertig, 'Bitcoin Cash: Why It's Forking the Blockchain And What That Means,' (*Coindesk* July 26, 2017) https://www.coindesk.com/coindesk-explainer-bitcoin-cash-forking-blockchain/ accessed 31 July, 2017

[62] International Council on Archives. Committee on Best Practices and Standards: Progress report for revising and harmonizing ICA descriptive standards (ICA, 2012)

term preservation. One solution could be to leverage existing trusted archival authorities, such as state archives, or state land registries, within Brazil for storage, rather than relying on the Colu servers, to establish a self-supporting, distributed long-term storage network less dependent on extraterritorial parties or centralized storage options in Brazil. Working together, these trusted recordkeeping authorities could act, in theory, both as blockchain nodes on a permissioned blockchain network and as seeds on a coordinated permissioned torrent network designed to validate and immutably preserve the most important records of the state. At this stage, however, the viability of this, or any, long-term preservation solution for blockchain records is strictly speculative and requires further research.

E. Conclusions

This paper has reviewed a solution designed to record transfers of land ownership in the Municipality of Pelotas, Rio Grande do Sul, Brazil, and assessed it using an archival science theoretic lens, since archival criteria for trustworthy records closely aligns to legal requirements for determining admissibility and weight of evidence and legal status of titles and given the requirements for long-term trustworthiness and accessibility of land title records. Thus, archival requirements offer a useful checklist for those considering blockchains for land transaction recordkeeping. Though the potential benefits of applying blockchain technology in land registration are great – improved efficiency, reduced transactional friction, better security, etc. – it is fair to say that, at this point in time, there are many aspects of the solution that need further examination and, possibly, (re)design from an archival perspective. This finding runs counter to some arguments that the application of blockchains in land transaction recordkeeping are best suited to data archiving.[63]

Attention is due to the technology's impact upon long-term availability and evidential quality of blockchain records. A reduction in evidential quality or loss of access to blockchain records may have a significant negative impact upon transparency and public accountability, and deprive individuals of their entitlement to land. Changes to the legal, administrative and procedural rules may be needed in order for such systems to work effectively.

These challenges are only to be expected when the technology is so new, and still evolving, and where the solutions are still at very early stages of design and piloting. The aim of raising these issues is not to put off potential adopters of blockchain land transaction recording systems; rather, the hope is these findings can be used to further develop potential blockchain solutions as the real estate registry office further pilot tests blockchain land transaction recording.

[63] See, for example, Arrunada (n 13)