<Danielle Batista, Victoria Lemieux>
<University of British Columbia>, <Vancouver, BC, Canada>

BOUNDED AND SHIELDED: ASSESSING SECURITY ASPECTS AND TRUSTWORTHINESS OF SMART CONTRACTS. (Paper)

Abstract or Résumé:

This is an in-progress research project that aims to explore how archival science and cybersecurity can be applied to evaluate the trustworthiness and security of smart contracts. The analysis will be made using the requirements of trustworthy records and the investigation of vulnerabilities related to the development and implementation of smart contracts. The expected contribution is to improve smart contracts' trustworthiness as archival records and evidence.

1. Introduction

Imagine losing all the assets accumulated in an entire life, like your house or savings. That is what could happen if insecure smart contracts are implemented to execute transactions in business and governmental agencies. Smart contracts are software that execute business transactions in an automatized way using consensus mechanisms present in blockchain systems. They are now being used in a diverse range of procedures such as land title transactions and informed consent to use of personal health data.

Given the increasing use of smart contracts in transactions involving personal rights and entitlements, how can we guarantee that smart contracts will be trustworthy and long-lasting archival records? Smart contracts are already being used to support civil and individual rights and entitlements such as identity and property rights that might be compromised if the records are not secure, not available anymore, or if they are not acceptable as evidence of the transactions that they represent. The trustworthiness of the information contained in smart contracts, therefore, must be assured.

The research proposal presented in this paper aims to explore how archival science and cybersecurity can be applied to evaluate the trustworthiness and security of blockchain-based records, specifically smart contracts. The research is scheduled to be carried out in two phases: 1) comparing the characteristics of smart contracts with the requirements of trustworthy records according to the theory and principles of archival science and 2) collecting and analyzing issues related to the development and implementation of smart contracts. The results of the work will contribute recommendations for improvements in the design of blockchain systems to produce trustworthy smart contracts and other types of blockchain-based records.

2. Smart contracts as trustworthy records

Digital records are not a novelty. They have existed since the invention of computers and are ongoing objects of study in archival science. Since the 1990s, technology has evolved quickly and so have the problems of keeping authentic digital records. A new form of digital record is the

smart contract, an automatized version of traditional contract clauses using a programming language (Christidis & Devetsikiotis, 2016) and providing for each contract the promise of immutability on the blockchain system (Lemieux, 2016). There is no consensus about the Blockchain concept, so this proposal considers blockchain as "an open-source technology that supports trusted, immutable records of transactions stored in publicly accessible, decentralized, distributed, automated ledgers" (Pearse-Moses, 2018a). Smart contracts promise to become the new protocol for recording transactions such as land title registration, health recordkeeping, and digital identity ("Smart Contracts: 12 Use Cases for Business & Beyond" 2016).

In the brief history of smart contracts, many cybersecurity breaches have occurred, which raises questions about the reliability and authenticity of these records. The first significant event related to the security of smart contracts involved a "DAO", a decentralized autonomous organization that used long-term smart contracts to raise funds for new ventures on the Ethereum blockchain (Buterin, n.d.). A DAO has its rules and decision-making processes codified, eliminating the need for people or physical documents in the governance of new blockchain-based ventures (Siegel, 2016). The famous attack on The DAO occurred in June 2016 when an attacker drained more than U$D60 million from U$D150 million raised on its initial coin offering (ICO). The attack was possible because of a computer programming flaw detected in its code. Many other security issues have been detected, and many studies have investigated the effects of (Luu, Chu, Olickel, Saxena, & Hobor, 2016) or the solution for some of those issues (Atzei, Bartoletti, & Cimoli, 2016), but none has explored cybersecurity aspects of smart contract as trustworthy of records and evidence of business transactions, which is the focus of the research presented herein.

Archival Science is the discipline underpinning recordkeeping. It is the field that studies the records per se, their sociocultural context, their context of creation, management and use (Duranti & Franks, 2015). A record is said to be trustworthy when it presents accuracy, reliability and authenticity (Duranti & Preston, 2008). An accurate record is precise, correct and truthful, free of error or distortion, or pertinent to the matter (Pearse-Moses, 2018b). Reliability is the capacity of a record to stand for the fact it is about (Lemieux, 2017b) being complete - presenting all the necessary elements to generate effects; consistent with the procedures of creation (Duranti, 1995); and naturally created – being objective and impartial. Authenticity is related to the identity and integrity of a record. A record keeps its identity by keeping its archival bond, its relationship with the specific context of creation and use. This characteristic defines the group (archival fonds) where the record belongs and demonstrates the relationship it presents with the records documenting the same transaction or human activity (Lemieux, 2017b). The integrity of the record is guaranteed when it is not manipulated, altered or falsified after its creation and/ or transmission (Duranti, 2002). Besides trustworthiness, a record must present persistence, being preserved and remaining accessible until the end of its prescribed retention period.

The characteristics of trustworthy records are not guaranteed in some blockchain systems, like Ethereum - one of those that keeps smart contracts. For example, the identity of the record in the case of smart contracts may be compromised, since the relationships among smart contracts involved in the same transaction, their context of creation and other records of the same context are not necessarily established.

3. Methodology

This research project presents the characteristics of an inductive study since it intends to extend existing theory into a new setting (Given, 2008). There is an initial assumption that the theory related to trustworthy digital records can be transformed or extended to contemplate records generated by decentralized trust systems. The first phase of the research resides in the analysis of differences between the characteristics of smart contracts and the requirements of trustworthy records, using, for example, recognized standards like InterPARES Authenticity Task Force (MacNeil & Gilliland-Swetland, 2000) and "Taxonomy of Trust" developed by Lemieux (Lemieux, 2017a). The goal in this first stage is to identify the constitutive elements of smart contracts as a new category of records and compare those elements to the requirements of trustworthy records imposed by digital diplomatics theory. The information collected in the first stage of the study will guide the formulation of the survey instrument on the second stage and provide a theoretical foundation for the analysis of the constitution of smart contracts, usually built by programmers.

For the second phase of the study, it is appropriate to use a survey method through the application of a semi-structured interview with programmers to gain a more detailed understanding of the leading security issues related to the development of smart contracts. The interview questions will be drawn upon the literature review of smart contracts security, a framework based on the most common threats used by an attacker and the results of the first phase of this research. The convenient initial sample for the survey will be composed of 20 smart contract programmers because this is the population able to point out the security issues related to the technical structure of the smart contracts. Programmers are the only ones that could provide relevant information about the difficulties relatin to the formulation of smart contracts, how well aligned the rules to be coded are to established procedures and what are the vulnerabilities detected during the creation of the record. Examples of questions to the survey relate to the standard methods used to capture intentions behind smart contracts, the difficulties in transforming those intentions into code, which software development methodology is used in the construction of smart contracts, if there is and which are the secure coding practices, which aspects of design are considered in the moment of the creation of the record (e.g. privacy, compliance, etc), and the use of standards templates for the development of smart contracts. The continuation of data collection consists of applying the snowball sampling technique given the difficulty in establishing a probability sample. Smart contracts developers are a hard-to-reach population because they deal with a recent technology, launched in 2015. The snowball approach will be used paying attention to age, gender, culture and other features of the population to address issues of representativeness and community bias associated with this sampling technique.

4. Potential contributions

This research intents to construct an audit framework for the creation and preservation of smart contracts. That instrument will refine the creation processes of smart contracts (which touch upon their reliability and authenticity as records), so their identity can be addressed to improve their trustworthiness as archival records. It will also contribute to the improvement of blockchain systems involving smart contracts as evidence of transactions and as recordkeeping systems. This contribution will help governments and private organizations to better evaluate the application of smart contracts as a protocol for their recordkeeping. Smart contracts promise to

be an essential tool to establish numerous types of transactions involving social and individual rights. Archival science as a discipline is a field with a body of theory and principles that show promise to help guarantee and preserve access to these rights.

Reference List:

Atzei, N., Bartoletti, M., & Cimoli, T. (2016). A survey of attacks on Ethereum smart contracts. *Cryptology EPrint Archive*. Retrieved from https://eprint.iacr.org/2016/1007.pdf

Buterin, V. (n.d.). Ethereum White Paper. Ethereum.org. Retrieved from http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Christidis, K., & Devetsikiotis, M. (2016). Blockchain and Smart Contracts for the Internet of Things. *IEEE Access*, *4*(1), 2292–2303.

Duranti, L. (1995). Reliability and Authenticity: The Concepts and Their Implications. *Archivaria*, *39*, 5–10.

Duranti, L. (2002). The Reliability and Authenticity of Electronic Records. In *Preservation of the Integrity of Electronic Records* (Vol. 2). Kluwer Academic Publishers.

Duranti, L., & Franks, P. C. (2015). *Encyclopedia of Archival Science*. Lanham. Boulder. New York. London: Rowman & Littlefield.

Duranti, L., & Preston, R. (2008). Terminology Cross-domain Task Force, "Appendix 22: InterPARES 2 Project Ontologies". In *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*. Padova, Italy: Associazione Nazionale Archivistica Italiana. Retrieved from http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_appendix_22.pdf

Given, L. M. (2008). Induction. In *The SAGE Encyclopedia of Qualitative Research Methods* (Vol. 1, pp. 429–430). SAGE Publications, Inc. Retrieved from http://link.galegroup.com/apps/doc/CX3073600219/GVRL?u=ubcolumbia&sid=GVRL&xid=d061e878.

Lemieux, V. L. (2016). Trusting Records: is Blockchain technology the answer? *Records Management Journal*, *26*(2), 110–139.

Lemieux, V. L. (2017a). Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems (p. 8). Presented at the Future Technologies Conference (FTC), Vancouver, Canada. https://doi.org/978-1-5386-2823-2

Lemieux, V. L. (2017b). Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective. *European Property Law Journal*, *6*(3), 392–440.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making Smart Contracts Smarter. In *CCS'16*. Vienna, Austria. http://dx:doi:org/10:1145/2976749:2978309

MacNeil, H., & Gilliland-Swetland, A. (2000). Authenticity Task Force - Template for the Analysis. In *InterPARES 1 Project Book* (Vol. 1). Retrieved from http://www.interpares.org/display_file.cfm?doc=interpares_book_j_app01.pdf

Pearse-Moses, R. (2018a). Blockchain. *InterPARES Trust Terminology*. Retrieved from https://interparestrust.org/terminology/term/blockchain

Pearse-Moses, R. (2018b). InterPARES Trust Terminology Project. *InterPARES Trust Terminology Project*. InterPARES Trust. Retrieved from https://interparestrust.org/terminology

Siegel, D. (2016). Understanding the DAO Attack. Retrieved August 29, 2018, from https://www.coindesk.com/understanding-dao-hack-journalists/

Smart Contracts: 12 Use Cases for Business & Beyond: A Technology, Legal & Regulatory Introduction. (2016). Chamber of Digital Commerce. Retrieved from https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-12-Use-Cases-for-Business-and-Beyond_Chamber-of-Digital-Commerce.pdf