Secure Notarization using Blockchain for the FDRE Document Authentication and Registration Agency (DARA)

Ashenafi Zena
HiLCoE, Computer Science Programme, Ethiopia
IMC Worldwide, Ethiopia Ltd.
ashenafizena@gmail.com

Mesfin Kifle
HiLCoE, Ethiopia
Department of Computer Science, Addis Ababa University, Ethiopia
kiflemestir95@gmail.com

Abstract

Notarization is an important facet of civilization. It creates trust between interacting parties enabling them to do mutual exchanges. Financial services and civil service organizations in Ethiopia are among the consumers of notarized documents. These organizations resort to authenticating notarized documents against registered copies at the notary as a measure of security. Being subjected to such a lengthy security measure leads to customer dissatisfaction and delayed service delivery. Automating this key process has been slow until recently due to the difficulty of creating efficient and effective digital trust relationship between transacting parties as well as legal framework unavailability and incompatibility across jurisdictions. In this paper, we compare blockchain with similar technologies and adapt it for the purpose of notarization. The proposed solution is a notarization, registration and verification system based on an open source blockchain infrastructure. The proposed solution promises instantaneous and independent verification and immediate dissemination of revocation closing potential security gap while still protecting fraudulent activities as well as the brick and mortar notarization institution.

Keywords: Document Notarization; Document Security; Blockchain; Distributed Database

1. Introduction

Notarization, the action or process of notarizing a document, a record of this, as stamped and signed by a notary directly on a document, or in the form of a certificate [1] is ubiquitous. It plays a big part in the healthy functioning of a modern society. In all sovereign countries, there are always one or more entities constituted by law to perform the function. The Federal Democratic Republic of Ethiopia (FDRE) Document Authentication and Registration Agency (DARA), the primary focus of this paper, is established by the FDRE Proclamation No. 922/2015 [2].

The current predominant method of paper-based notarization requires that the notary physically sign and stamp or emboss the paper document being notarized [3]. "This has historically been a norm and was effective in achieving the goal of security-traditional notarizations were difficult to forge, modify or erase, because the signatures and seals are impressed or embossed into the very fiber of the paper, and they explicitly track back to a government-commissioned notary who can verify the facts related to the notarial act" [3]. However, technological advances are easing this difficulty thereby increasing the risk that forgery afflicts on the traditional signing of paper documents. Forensic science cannot guarantee that any given ink signature can be verified. Scientists can only offer an educated opinion as to whether the signature is authentic, and they can do so only under the right circumstances. This includes, for example, the availability of several good specimen signatures [4]. One possible approach to mitigate forgery is for the notary to keep a notarial journal and copy of notarized documents. Greenwood, in a review of electronic notarization [3] provides examples of how the mere existence of a notary journal served as a deterrent and a prosecutorial tool. By law, the Federal Democratic

Republic of Ethiopia requires the notary to keep a register (journal) and deposit copies of authenticated documents for itself [2]. When issues of authenticity arise, reauthentication is made against said deposits. Thus, it can be argued that the FDRE has installed a mechanism to deter forgery.

On the other end of the spectrum, financial services and civil service organizations in Ethiopia are among the consumers of notarized documents where the said documents are routinely presented for execution by agents like the Attorney-in-Fact. Such organizations are cognizant of potential economic loss to Principals that may arise from transactions involving high value assets like property and liquid assets. In practice, organizations resort to authenticating notarized documents against registered copies at the notary as a measure of security. This occurs at the expense of an expedited service delivery to the detriment of both the service rendered and the customer (Attorney-in-Fact). The authentication process conjures up the security-usability trade-off described in Saltzer and Schroeder's principle of psychological acceptability [5]. The principle says that a security mechanism should not make accessing a resource, or taking some other action, more difficult than it would be if the security mechanism were not present. In practice, this principle states that a security mechanism should add as little as possible to the difficulty of the human performing some action [6]. *In stark contrast, the Attorney-In-Fact, by being subjected to a lengthy security measure is denied an immediate response to execute its Representative Capacity.*

We hypothesize that through implementing automated, secure and easily verifiable notarization employing blockchain technology, we can significantly improve service delivery responsiveness of these organizations while at the same time guaranteeing the same or improved level of security as currently practiced. Thus, the following research questions are formulated to address the research.

- How secure is notarized document verification as currently practiced in financial and civil service providers of (how effective is the security) and how long does it take, on average, to verify notarized documents by such providers (how efficient is the security)?
- What are the desirable characteristics of a technology based notarization?
- Among potential technological solutions including the hypothesized blockchain, which is better suited to provide effective and efficient security?
- How can a notarization solution with the desired characteristics be built and evaluated?

Our primary research approach is design science- we design a secure notarization system with properties geared towards solving the efficiency problem of existing practice. The hypothesis is, blockchain, a distributed trustless consensus database, can deliver a secure, open and efficient solution to notarization. We have anecdotal understanding of how a manual notarial system can be improved by the application of technology. However, to make this understanding concrete, we employed a qualitative research design using interview as instrument to seek an understanding of different groups of users experience and perception about the state of affair in current notarization systems. Blockchain is an innovative technology with great promise. However, there are contending proposals that can potentially be applied to automate notarial process. As a consequence, we followed the qualitative study with a comparison of alternative technologies to select an appropriate technology from an array of alternatives based on desirable properties. The desirable properties are garnered from industry best practice documents, regulatory requirements as well as requirements gathered as a result of the interviews conducted.

The same desirable properties are used to drive the design and implementation of a proof-of-concept of the blockchain based notarization system. We used an open source blockchain infrastructure - Hyperleger Fabric [7] - as the backbone of the

prototype. Access to the blockchain is provided by a RESTful API provided by another Hyperledger project - Hyperledger Composer [8]. We designed a web application using Angular - a JavaScript client-side library - to implement the user access to the blockchain system and effect the notarization domain business logic in coordination with the RESTful API.

2. Related Work

In reviewing the body of research in digital notary, one can observe a rather concerted effort starting from the late 90s to apply the concepts of public key cryptography infrastructure (PKI) to the domain of long term preservation of digital assets using digital signature in a variety of ways. This is likely due to the maturity and wide spread application of PKI with the growth of the web in that era and the rather attractive notion of applying the technology to its natural use of enforcing authentication, non-repudiation (with certificate authority), and integrity which seems to fit nicely to the domain of notarization. In this section, we review related publications highlighting the problems they tackle and their limitations.

Publicized in the 2000 European Conference on Information Systems proceedings, the work in [9] aims at solving disputes between entities on events and/or actions that are of interest to the entities. Claim is made that commercial certification or notarization services are incomplete in that these services do not distinguish the creator from the sender nor store the data itself for a long time, nor prove the action (creation, sending, receiving) in the context of communicating entities. The paper's objective is to address this gap employing an empirical approach through the creation of a typical Trusted Third Party (TTP) service the authors named CYNOS- CYberNOtary System.

The proposed solution is a signature-based system and uses various security techniques to enable the timely certification of entities and fair and highly reliable delivery. First, the *existence notarization* service stores evidence proving the existence of a piece of data and its possessor. Second, the *delivery notarization* service stores the evidence of the delivery and the reception by the intended recipient as well as the existence of the data and the originator. *Notary token* CYNOS issues as the certification of facts containing the evidence stored in CYNOS after each notarization event and is accompanied with a signature of CYNOS. The solution relies on CA (Certification Authority), NA (Notary Authority) and RA (Registration Authority).

A paper presented at EuroPKI 2012 conference [10], proposes a new PKI model for long-term signatures based on X.509 and the real world of handwritten signatures. The problem is framed in the context of using long term keys to sign a document. The paper claims preserving information is useless if authenticity, integrity and datedness cannot be ensured in perpetuity. To address this, PKI has been commonly utilized. However, the paper posits PKI solutions suffer from two major problems. The first is the amount of protection data (which they define as timestamps, certificates and revocation data accumulated in the life time of the document) to store and verify is not optimal both storage wise and processing overhead. The second is the difficulty for verifiers of dealing with trust anchors in terms of unavailability of previously trusted entities. This can happen, for example, with changes to technology and the corresponding data model. The paper's objective is, therefore, focused in finding a solution to reducing the data protection burden and the chain of trust that needs to be verified in continuity.

Their proposed solution to the problems is The Notarial Based Public Key Infrastructure (NBPKI). The notary in their solution is modeled against the real-world notaries which they refer to as Notarial Authorities (NA).

As with the current work, the goal is in finding an effective and efficient notarization solution using PKI. However, in the reviewed work, the NAs are modeled as trusted parties. This is just moving the known weak link of the Certificate Authority (CA) of current PKI systems to a new entity modeled after

the real-life notary which has no valid ramification. Even if a legal framework is coined to institute these digital NAs, the key decay problem tormenting the CA with time passage cannot be mitigated using legislative means alone.

A paper presented at the 12th annual ACM-SIAM symposium [11], proposes a method to notarize a paper document by computing a set of features from the page, inputs these features into a hash function, digitally signs the output, and then prints the resulting signature on the page. The notarized document is self-contained - verification does not require reference to online information.

The proposed solution is to have a digital scan of the document from which feature sets are extracted (glyphs or symbols) and hashed, employing public-private key cryptography, into a short string which can later be verified by a third party running the same algorithm as the authenticator on the same set of features of his/her scanned copy.

The authors' creative solution is to come up with a concept they named an assist channel. The value of the assist channel is to compensate and regulate for scan variations in a predictable manner so that any verifier can get the same hash compute result as the original authenticator provided the document has not been altered.

An article published in the Institute of Electrical Engineers of Japan journal [12], proposes storing document timestamp in the blockchain by encoding into Bitcoin addresses. The paper focused on the proliferation of data on the Internet without adequate ownership ascertaining mechanism for those who require it due to the nature of the digital data - creative assets that the owners would like to have copyright over. The authors believe the available solutions- timestamping, either by a central timestamping authority (TSA) or a scaled version of such service- suffer from a single point of failure and costly deployment respectively. The two further have a shared shortcoming of being easily exposed to security breaches. Thus, the paper's objective is to find a solution that has no single point of failure, economically scalable and tamper resistant.

The proposed solution is a method called decentralized trusted timestamping based on a blockchain. While they provide examples of services that provide timestamping on a distributed tamper free database they discount them on the basis of their data limitation. They all depend on Bitcoin's blockchain that put a 40-byte data constraint on extraneous data. Moreover, the 40-byte hash data cannot be reversed, which makes determining the creators and other related information difficult.

Thus, they propose a methodology for storing a maximum of N*20 bytes in the blockchain. For creators who prefer not to anonymously timestamp their creations, their proposed method can embed related information (e.g., the file name, the creator's name, and comments) and the hash of the digital data. The related information has the added benefit of being decrypted in plain text. The method creates transactions with N output addresses; therefore, one transaction can store at most N*20 bytes.

The reviewed work is closely aligned with the current research. The use of blockchain as an irrefutable secure storage of records and the result of the evaluation in terms of cost and effectiveness is what the current work aspires to establish.

A paper, published in the International Journal of Medical Informatics [13], deals with the long-term validation of the authenticity of electronic healthcare records (EHR). The authors' premise is that medical records should be preserved at least for the lifetime of a patient or even longer for research or other purposes. The challenge is that preserving electronic data for a lifetime is not a straightforward task, since ICTs are under intense development and are subject to continuous changes. The long-term preservation of EHR may be approached and analyzed from various perspectives, such as future data readability, storage media longevity and security.

The paper proposes a successive trust transition towards new entities, modern technologies, and

refreshed data to mitigate the key life-time problem. According to the paper, a future relying party will have to trust only the information provided by the last notary, in order to verify the validity of the initially signed EHR, thus eliminating any dependency on ceased entities, obsolete data, or weak old technologies.

3. The Proposed Solution

The proposed solution is a notarization, registration and verification system. We start by defining the functional and non-functional requirements of the system. Next, we describe a process for selecting a blockchain from a family of related chains based on system requirements. Finally, we construct an architecture and detail design of salient features of the notarization, registration and verification system. We arrived at this decision after a technology selection exercise. We made comparison of technologies we reviewed based on key attributes that a notary system should possess. The primary attributes for technology selection are the perceived effectiveness and efficiency of a notarization. We concluded that the proposed solution is a better fit to solve the problem at hand.

3.1 Functional Requirements

The prominent functional requirements are authenticate documents, authenticate and register copies of documents against their originals and register same, suspend document authentication and act in lieu of a Registry Authority. Figure 1 shows the proposed system functions.

3.2 Nonfunctional Requirements

The important quality attributes shape the structure and behavior of the overall system. We elucidate attributes, sourced from The Model Notary Act [14], that have relevance towards system building. These are technology neutrality, confidentiality, performance, integrity and nonrepudiation, capable of independent verification and digital signature source agnosticism.

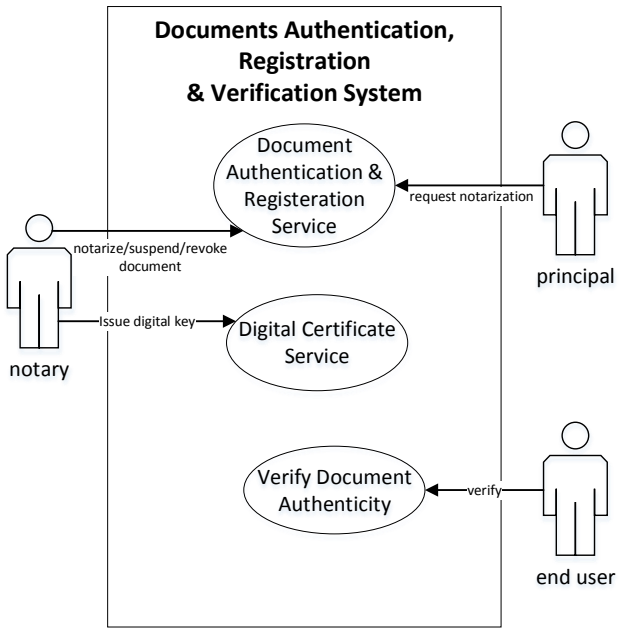

Figure 1: System Use Case

3.3 Blockchain Selection

"A major difficulty for architects designing applications based on blockchain is that the technology has many configurations and variants. We propose how to classify and compare blockchains and blockchain-based systems to assist with the design and assessment of their impact on software architectures" [15]. The selection process answers the following guiding questions: 1) Has trusted authority? 2) Can it be decentralized? 3) How to decentralize the authority? 4) Storage and computations on-chain vs. off-chain? 5) Need new blockchain? 6) What consensus protocol? 7) What incentive? Going through the guide, we selected A DARA controlled, decentralized by DARA branches and subordinated institutions, with optional off-chain document store, identity based consensus protocol (allowing only DARA and subordinates to write to the blockchain) dismissing the need for incentive.

3.4 Notary Application

The notary application is designed for the notary to complete notarial acts. It manages the notary's digital signature, it accepts user document for the notary's review, helps it generate digital keys for the principal and the attorney-in-fact as well as securely print it for later use, digitally sign the document using the principal's and its combined digital private

keys, digitally sign the document with the attorney-in-fact's public key and finally send the notarized document to the blockchain. The system architecture is shown in Figure 2.

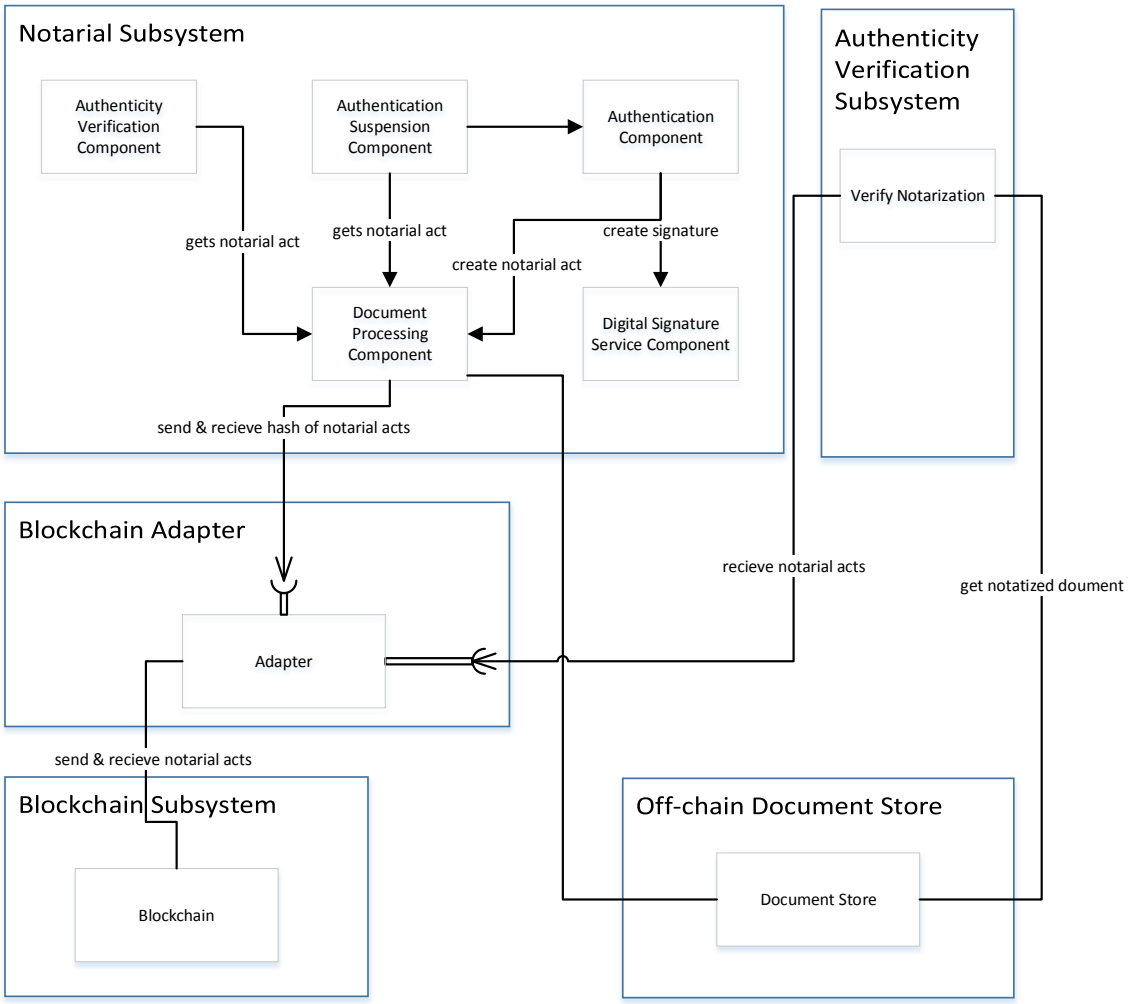

Figure 2: System Architecture

3.5 Verification Application

The verification application is designed for any interested party to independently verify a provided document from the off-chain document store that matches a hashed version in the blockchain. For this to happen, the attorney-in-fact needs to present the third party, a bank official for instance, with a raw document decrypted using his/her private key from the off-chain document store. The precondition is that at the time of notarization, the document is pushed to the document store encrypted using the attorney-in-fact's public key for the purpose of privacy (a copy can be made using the principal's public key for his/her reference as well). The document needs to be accompanied by metadata describing the notary and principal's public keys and a document reference. From there, the verification application computes and compares the hash with the one in the blockchain referenced by the same document reference. Thus, the physical architecture depicted in Figure 3 ensues.

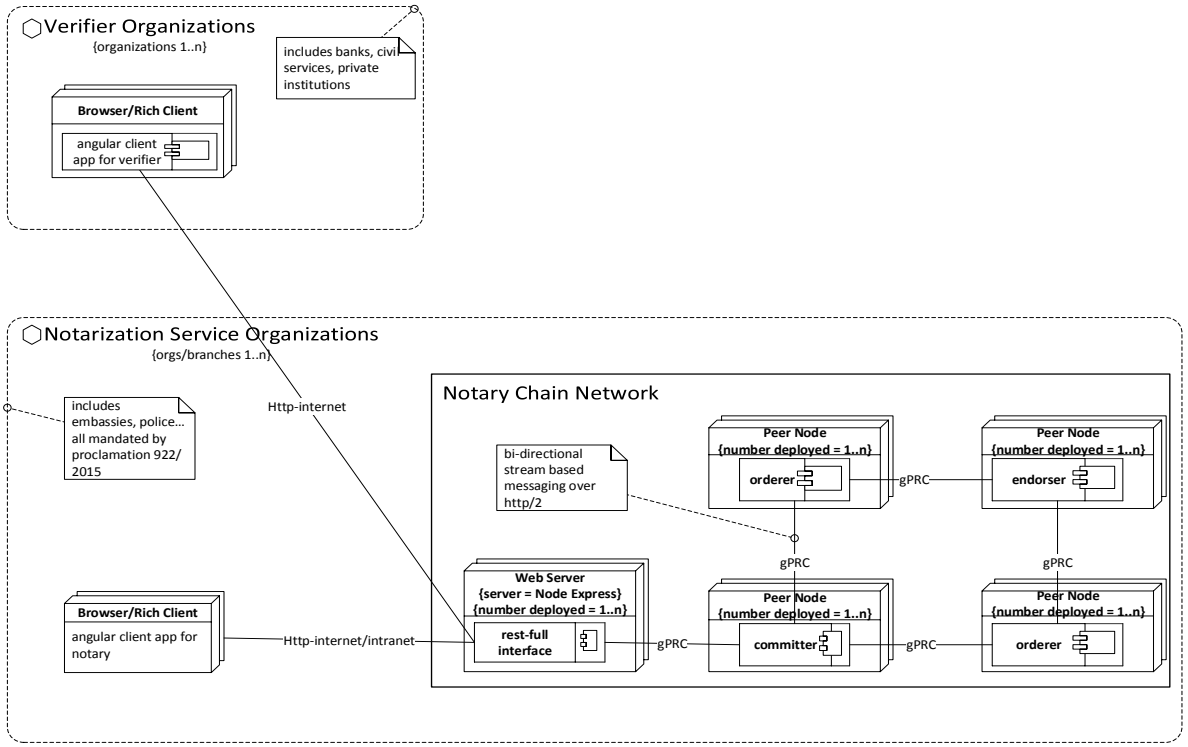

Figure 3: Physical Architecture

4. Conclusion and Future Work

We showed that recent development in distributed trust relationships with the advent of blockchain technology is a viable solution to a whole slew of problems - trusted third-party computation model, single point of failure and the related scalability and availability issues. We did so by designing a blockchain based solution to DARA.

The proposed solution promises instantaneous and independent verification and immediate dissemination of authentication revocation, closing potential security gap. It also affords service providers prompt reply to customers enhancing their brands and satisfaction for the customer.

Perhaps, the biggest hindrance to the practical implementation of a blockchain based notarization system is the absence of a conducive legal framework that enables the notary and individuals to execute digital signatures in leu of hand signatures and for these signatures to be legally binding. The foundation for this, The Ethiopian Electronic Signature Act (ESA), is already laid out but is still a draft under consideration. The speedy adoption of the act can enable the materialization of notarization and related domains to flourish using the blockchain as a secure distributed applications platform.

Most notarial acts need human intervention. They are performed in person and out of band - meaning they are not amicable for automation. However, other tasks like keeping specimen of signature, ascertaining the legality of documents; ascertaining the capacity, right and authority of persons, ascertaining title certificates and ascertaining legitimacy of documents source can be aided and become components of the blockchain system. This requires that other government institutions - land management and citizens management - also can be brought onboard the blockchain system. Property certificates and citizens' identity information are inputs for the notary to ascertain legality of documents; ascertaining the capacity, right and authority of persons, ascertaining title certificates and ascertain legitimacy of documents source. We believe this extension is a fruitful research arena to explore.

References

[1] "Definition/notarization," Oxford University Press, 2017, https://en.oxforddictionaries.com/

definition/notarization, Last accessed on 20/03/2017.

[2] Federal House of Peoples' Representative, Proclamation No. 922/2015, Authentication and Registration of Document, Addis Ababa: Federal Negarit Gazette, 2016.

[3] D. J. Greenwood, "Electronic Notarization," National Notary Association, Chatsworth, California, 2006.

[4] M. L. Closen, "Notaries Public - Lost in Cyberspace, or Key Business Professionals of the Future?," Journal of Computer & Information, Vol. 15, No. 4, pp. 703-758, 1997.

[5] J. H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems," Proceedings of the IEEE, Vol. 63, No. 9, pp. 1278-1308, 1975.

[6] M. Bishop, "Security and Usability: Designing Secure Systems that People Can Use", L. F. Cranor and S. Garfinkel, Eds., Sebastopol, CA: O'Reilly Media, Inc., 2005.

[7] Hyperledger, "About - Hyperledger," The Linux Foundation, https://www.hyperledger.org/about, Last accessed on 24/9/2017.

[8] Hyperledger, "Hyper Ledger Composer," https://github.com/hyperledger/composer, Last. accessed on 24/9/2017.

[9] S. Nakahara, "Electronic Notary System and its Certification Mechanism," in ECIS 2000 Proceedings, Vienna, 2000.

[10] M. Vigil, C. Moecke, R. F. Custódio, and M. Volkamer, "The Notary Based PKI: A Lightweight PKI for Long-Term Signatures on Documents," in Public Key Infrastructures, Services and Applications: 9th European Workshop, EuroPKI 2012, Pisa, Italy, 2013.

[11] M. Ruhi, M. Bern, and D. Goldberg, "Secure Notarization of Paper Text Documents," in SODA '01 Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms, Washington D.C., 2001.

[12] Y. Gao and H. Nobuhara, "A Decentralized Trusted Timestamping Based on Blockchain," IEEE Journal of Industry Applications, Vol. 6, No. 4, pp. 252-257, 2017.

[13] D. Lekkas and D. Gritzalis, "Long-term Verifiability of Healthcare Records Authenticity," International Journal of Medical Informatics, Vol. 76, No. 5-6, pp. 442-448, 2007.

[14] National Notary Association, "The Model Notary Act," 2010. https://www.nationalnotary.org/file%20library/nna/reference-library/2010_model_notary_act.pdf., Last accessed on 2/5/2017.

[15] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, "A Taxonomy of Blockchain-Based Systems for Architecture Design," in IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 2017.