Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 185 (2021) 119–126

Procedia Computer Science

www.elsevier.com/locate/procedia

Complex Adaptive Systems Conference Theme: Big Data, IoT, and AI for a Smarter Future
Malvern, Pennsylvania, June 16-18, 2021

Cyberinfrastructure for Social Good: Ensuring That No Homeless Individual Stays Behind

Charalampos Chelmis[a]*, Yogesh Kumar Angajala[a]

[a]*Department of Computer Science, University at Albany, Albany, NY 12222, USA*

Abstract

We present a prototype decentralized transactional platform designed to improve the transparency of homeless serving organizations and facilitate their accountability and oversight. In the proposed system, the complete history of transactions between organizations offering homelessness services (e.g., shelters, transitional housing) and individuals seeking such services is stored in a distributed ledger. Using smart contracts, the proposed tamper-proof framework can automate the exchange of information between clients, organizations and government agencies, and allow government agencies audit organizations without violating the privacy of homeless individuals. We begin by describing the goals and concepts, the stakeholders' requirements and the corresponding desirable system properties, and identified challenges. We continue with an in-depth description of the overall architecture of the proposed system designed to achieve these goals, and lessons learned towards transitioning this system to the real-world.

Keywords: social services; process traceability; accountability

* Corresponding author. Tel.: +3-518-437-4948.
E-mail address: cchelmis@albany.edu

10.1016/j.procs.2021.05.013

1. Introduction

Human service providers [1], i.e., entities whose primary goal is the provision of housing and services to homeless individuals and families at risk of homelessness, play a critical role in improving well-being in the United States. In 2001, the United States Congress directed the U.S. Department of Housing and Urban Development (HUD) to provide an annual report on the status of homelessness across the country. To meet this demand, HUD put forth the Homeless Management Information System (HMIS) [2]. HMIS records the characteristics, demographic information, and the number of people using federally funded homeless services. This includes all homelessness services programs under HUD, Health and Human Services (HHS), and Veterans Affairs (VA). However, organizations that do not receive HUD funding are not required to use HMIS. At the same time, current methods for obtaining data (e.g., using intake forms) are limited by human data entry. Despite their simplicity, existing methods often result in high levels of missing and/or poor-quality data, which can in turn potentially lead to little accountability or oversight.

This paper investigates the application of distributed ledger technologies to address some of the key challenges in the domain of homeless services. Specifically, this work explores the feasibility of a decentralized platform with the goal of improving the transparency of homeless services provision, while facilitating verifiability and auditability.

2. Background

2.1. Distributed Ledger Technologies

Blockchain [3], and more generally, distributed ledgers, has recently gained popularity, mainly due to the Bitcoin cryptocurrency and the associated platforms for decentralized asset management (e.g., [4, 5]). A blockchain is a chronological chain of records called blocks, each of which records a set of transactions and is linked to its preceding block. Combined with cryptographic hashes, the chain of blocks provides a permanent, immutable, and verifiable record of transactions stored in a decentralized network of peer nodes [7]. Each node hosts the same copy of a blockchain, and consensus mechanisms are used to ensure that all nodes are synchronized with each other and agree on which transactions are legitimate. The immutability feature (i.e., data recorded in a blockchain can neither be deleted nor altered) makes blockchain an ideal solution for verifiability and auditability purposes. Finally, a blockchain has the ability to automatically the execute "if condition X is met, then perform function Y" rules (i.e., "smart contracts") [8].

3. Related Work

Among the various domains where blockchain technologies have thus far been utilized, social good projects are among those that blockchain is believed to have a great impact [6]. Existing solutions for social good mainly focus on collecting and distributing money for charity, followed by projects whose main purpose is to improve the quality of the environment, as well as projects aimed at optimizing the usage and distribution of energy [6]. All such solutions exploit the characteristic features of blockchains, which include the quick and inexpensive transfer of cryptocurrency, the transparency of transactions, and trustworthiness due to decentralization [6].

On the other hand, a number of approaches has been proposed to achieve traceability in supply chain (e.g., [12, 13, 14]) that could address challenges associated with trust, fraud, corruption, tampering and even falsifying information [15]. However, such solutions have not been designed to handle privacy-sensitive data [16]. In addition, restrictions associated with the human services domain (e.g., the lack of technological expertise, as well as privacy rules, such as HIPAA [17], that make the sharing of data problematic) makes it difficult to meet the envisioned traceability, verifiability, and auditability requirements. The work most similar to ours is an Ethereum-based [19] electronic medical records management system [18]. Unlike existing blockchain-based social good solutions, our prototype uses Ethereum merely for its transactional convenience, and its support for smart contracts [20].

Finally, given the plethora of distributed ledger platforms, several processes for deciding which blockchain architecture is appropriate (if any) for a given use case are described in literature [9, 10]. Typically, if the identity of participants authorized to append the blockchain with new transactions does not need to be verified (i.e., no single authority grants permissions), a public blockchain, such as Bitcoin or Ethereum, can be used. Instead, when it is vital

for participants to acquire permission to execute transactions, a permissioned (private) blockchain, such as Hyperledger Fabric, is more appropriate. In our prototype implementation we use Ethereum for simplicity, and plan to explore Hyperledger in our future work.

4. Case Study, Challenges and Opportunities

To put the proposed decentralized transactional platform in context, we discuss next a scenario from our ongoing smart and connected community project, COMPASS [11], which focuses on efficiently and effectively connecting those in need with corresponding service providers. As part of COMPASS, we have developed a mobile app [11] that makes information about service providers openly accessible, easy to find, search and filter through, while at the same time facilitating digital service delivery. Focusing on the service delivery functionality of our mobile app, users can (i) request for services with the click of a button, (ii) track the status of their service requests, and (iii) even receive notifications of status changes (e.g., need for additional documentation). At the same time, we wish the complete history of service requests to be traceable for verifiability and audit purposes.

We assume three types of actors/stakeholders involved in our case study as following:

- Clients i.e., individuals seeking homeless services. We seek a design that allows clients to (i) make service requests (i.e., ask for emergency shelter) without having to provide any personally identifiable information, (ii) edit a service request as long as its status is "pending".
- Service providing organizations. Upon receipt of a request from a client, service providing organizations have the option to accept, decline, or make a referral. When a request is referred to another organization, clients are provided the option to either accept or decline the referral. We seek a design that provides reputational incentive for providers, where service transactions can be easily verified, and efficient providers are rewarded (e.g., in terms of positive reputation among agencies and donors, which in turn can lead to more funds been donated towards their mission).
- Government oversight agency, which we assume are mainly involved in monitoring activities and evaluation of outcomes. Thus, we seek a design that allows government agencies to receive as complete an accounting as possible based on stored service transactions.

These actors automatically create timestamped transactions that are added to the blockchain. For illustration purposes, Fig. 1 shows a hypothetical sequence of transactions between a client and two organizations.

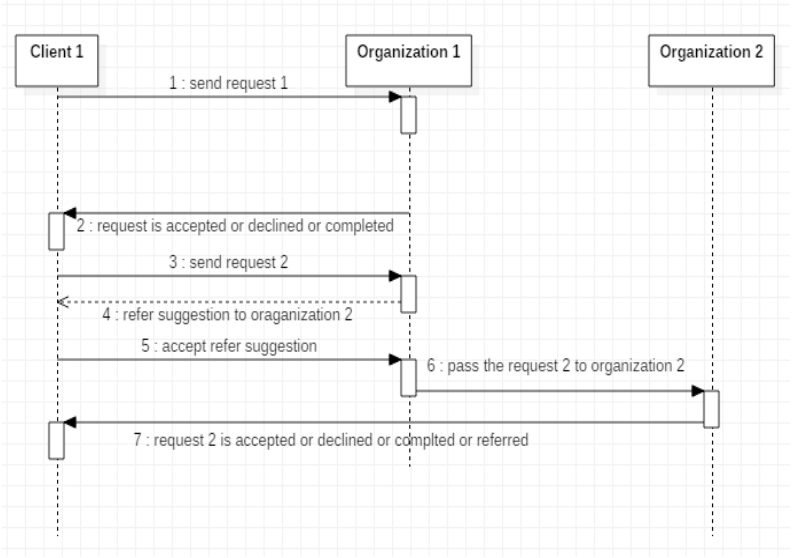

Fig. 1. Illustrative scenario of a sequence of transactions between a client and two organizations.

We assert that a framework to automatically record and track the trail of service requests in this context has the potential to benefit both homeless serving organizations and government agencies. Specifically, by digitally collecting, storing, and verifying the complete history of transactions between organizations offering homeless services and individuals seeking such services, the need for time spent by staff to transcribe paper records would be minimized. On the other hand, government agencies overseeing homeless serving organizations can be assured that by automatically creating an immutable log of the complete history associated with a service request, no data can be altered or falsified, therefore improving the overall trust to reported data.

The associated requirements with such framework are summarized in Table 1. Note that the traceability requirement does not conflict with the confidentiality requirement. Instead, it is possible using smart contracts, and proper compartmentalization of data to facilitate traceability at the request of a government agency without providing direct access to the corresponding data. At the same time privacy and anonymity can be simultaneously realized with traceability using any given cryptographic protocol to encrypt raw data. The identified challenges associated with designing and developing a framework to record and track the trail of service requests are summarized in Table 2.

Table 1. Requirements.

Requirement	Description
Trust	Maintaining a trust relationship with government agencies is a key factor in homeless service providing organizations' ability to receive funding consistently.
Transparency	Depending on regulatory requirements, homeless service providing organizations may have to submit reports of provided services on a regular basis (e.g., annually).
Auditability	A digital bookkeeping system that records all transactions, including service requests and communication between service providers and clients, as well as among providers if necessary, creates rich opportunities for auditing operations (e.g., identify cases of discrimination).
Verifiability	A means of verifying claims without sacrificing the privacy and confidentiality of clients is currently lacking. Using existing solutions such as HMIS, data is available to service providing organizations, but remain opaque to government agencies.
Confidentiality	Clients' personal identifiable information of clients and sensitive data (e.g., disabilities) must be kept confidential.

Table 2. Challenges.

Challenge	Description
Infrastructure and Deployment	Homeless service providing organizations may lack the technical expertise to develop a technological solution based on distributed ledgers. Some stakeholders (e.g., clients) might only have access to the mobile app. Hence, any solution should be lightweight, with the ability to run on low-end mobile phones, and yet being capable of interacting with a blockchain network.
Training and Adoption	New technologies typically require stakeholders to be trained so as to ensure their adoption. To help stakeholders adopt the proposed solution without spending their time and resources for training, the architecture is currently being seamlessly integrated with the existing COMPASS system.
Privacy	Typical blockchain environments lack data privacy. Therefore, care must be taken to ensure client data remain private in accordance to HIPPA privacy rules.
Scalability and cost	The success of solutions based on distributed ledgers depends on the amount of resources comprising the network used to store records. The associated cost of establishing and maintaining such network may be overwhelming for resource constrained homeless service providers.

5. Proposed Solution

The overall architecture of the proposed decentralized transactional platform is shown in Fig. 2. Clients access information about service providing organizations and interact with them directly through a cloud-enabled mobile app [11]. This architecture enables clients and organizations to come to an agreement on a set of rules while allowing access to service transaction data dynamically and without supervision.

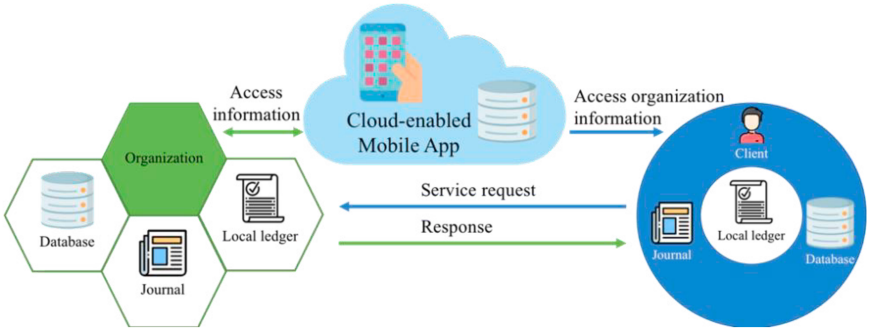

Fig. 2. System architecture.

Next, we outline the features of the proposed solution through examples typical for the stakeholders, rather than presenting a formal description of the corresponding smart contracts and functions.

Each actor holds a unique identifier (i.e., unique Ethereum address) and type (one of client, service providing organization, or government agency), both of which are assigned upon registration with the system. In our prototype, government agencies are authorized users with privileged credentials. User types are stored in a "vault" smart contract, along with all requests made by clients, and referrals initiated by service providing organizations. Finally, internal functions that can only be used by derived contracts (i.e., due to inheritance) are also stored in the vault.

A "user" smart contract is a derivative of a vault, and stores the details of clients and organizations, as well as corresponding functions that clients and organizations are allowed to perform. By design, such functions cannot access service requests and referrals data directly, but indirectly through internal vault functions. Table 3 summarizes the functions that clients and organizations are allowed to perform. Similarly, an "authorized user" smart contract, which is also a vault derivative, allows government agencies to seamlessly access statistical data about organizations. Table 4 summarizes the functions available to government agencies only.

Table 3. Functions associated with the "user" smart contract.

User type	Function	Description
Client	registerClient	Upon registering with the COMPASS system, a client is assigned an Ethereum address.
	sendRequest	A service request is issued to a service providing organization.
	modifyRequest	Changes/edits to an existing service request can be made as long as the status of the request is "pending".
	viewRequestClient	Allows a client to review referrals.
	acceptReferSuggestion	Allows a client to accept a referral made by an organization in response to her service request. A new request is automatically generated to the referred organization.
	declineReferSugestion	A client declines a referral made by an organization in response to her service request. No further action is taken.
Organization	registerOrganization	A service providing organization that is registered with the COMPASS system is assigned a unique Ethereum address.
	viewRequestOrganization	Allows an organization to review one of its received requests using the request counter value as key.
	acceptRequest/ declineRequest/ completeRequest	Allows an organization to change the status of a request it has received from "pending" to "accept", "decline", or "complete".
	sendReferSuggestion	Allows an organization to make a referral based on a service request it has received from a client. When activated, this function changes the status of the request from "pending" to "referred", and a referral suggestion is sent to the client.
	viewReferSuggestion	Allows an organization to view all referrals it has communicated to its clients.

Table 4. Functions associated with the "authorized user" (i.e., government agencies) smart contract.

Function	Description
organizationCount	Upon activation this function computes the total number of organizations in the system.
fetchOrganization	This function generates a report for a given organization.

This functionality is implemented using Solidity "smart contracts" [20] on Ethereum Virtual Machine [21] and deployed on a virtual testing environment with 10 default Ethereum addresses in Ganache [22]. Transactions are logged in the Ganache transaction logger, whereas the Ethereum consensus system executes autonomously. For illustration purposes, Fig. 3 shows a subset of transactions corresponding to the sequence presented in Fig. 1.

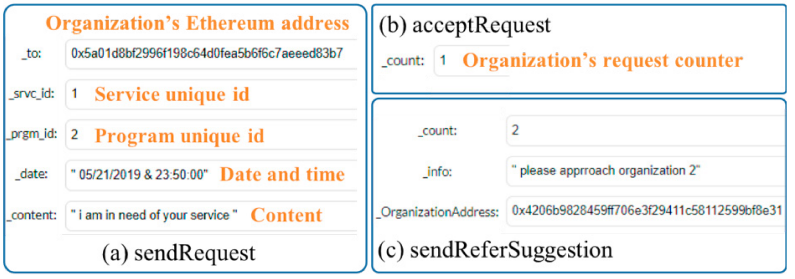

Fig. 3. Sample transactions corresponding to the sequence of requests in Fig. 1, as logged in the distributed ledger.

5.1. Registration, Identification and Authentication

Since our goal is to tie the proposed architecture to our cloud-enabled mobile app in the context of our COMPASS project [11], it is convenient to have all stakeholders' records linked to the existing infrastructure and generate their Ethereum address upon registration with the COMPASS system. This allows us to address the challenge of how stakeholders are to be registered with the system, and subsequently identified and authenticated. Transaction numbers are generated independently to the COMPASS system using the Ethereum infrastructure. This approach has both advantages and disadvantages. Specifically, generating and linking Ethereum addresses to user accounts become simple, convenient and streamlined, whereas, transaction ids are generated directly by the Ethereum infrastructure. At the same time, the reliance on the COMPASS system as a single source of trust may be disadvantageous. Although this aspect is not central to the contributions of this work, it should be further investigated in the future.

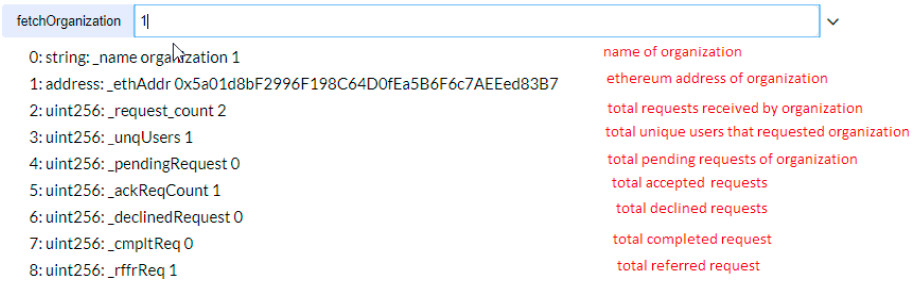

Fig. 4. Sample report for Organization 1.

5.2. Queries by Government Agencies

We envision the following common scenarios for government agencies: (i) audit an organization to verify claims made by that organization (e.g., verify annual reports), (ii) generate independent statistical analysis reports for a given

timeframe, such as, number of requests received, requests pending, accepted, declined or referred, and requests completed. Fig. 4 shows sample data automatically retrieved by an authorized user using the proposed solution.

6. Analysis

We next analyze our prototype decentralized transactional platform with respect to security and privacy, and cost.

6.1. Privacy and Security Considerations

Our primary focus for protection is client data and corresponding service records, which constitute sensitive data. At the same time, we wish to ensure that government agencies will maintain trust to the system and reports generated by the transactional data store into it. We consider the following threats as essential to the robustness of our decentralized transactional platform, and discuss how these are addressed by our design:

- Unauthorized users cannot access personally identifiable information and/or run reports on service providing organizations; smart contracts ensure that access to data is limited only to authorized users. For instance, a government agency is not allowed to access the raw data associated with a service request but can verify the status of a given request. The registration, authorization and access processes through our existing COMPASS infrastructure enable both clients, services providers and actors claiming to act on behalf of government agencies to be vetted by the COMPASS administrator. Similarly, an organization cannot access data of service requests made to a different organization, or clients that have not been served by that organization. An organization can also not run a report on another organization. This functionality is reserved only for government agencies. Finally, since all transactions are distributed and encrypted on the Ethereum network, there is no central place for a malevolent agent to hack and gain access to.
- An adversary may remove or change a transaction: The threat of tampering with any transaction is addressed by the inherent integrity properties of the blockchain. Specifically, each block consists of the signed root of the previous block, which makes the chain self-certifiable. Additionally, permissions ensure that each user type has limited access as needed. For instance, service providing organizations only have read access to client records to which they have been associated. Similarly, government agencies have access only to statistics about transactions involving organizations and clients and not the actual data that may compromise the privacy and confidentiality of clients. By limiting the access to data and functions different actors have, we enforce the overall security of the proposed solution.
- A service providing organization cannot claim a request has been met unless it is accepted and subsequently completed. Declined or pending requests persist in the blockchain and cannot be treated as completed. Referrals also do not account as completed when a report is generated.
- "Rogue" organizations could resort in fabricating client accounts and using such accounts to issue fake service requests. Such activity would require significant time investment from such organizations to manage multiple accounts and requests. We consider this threat to be moderately likely and mitigate this threat by requiring registration through the COMPASS system. At the same time, when generating reports, government agencies may review the distribution of response times (i.e., difference between the time a request is made and its completion) to identify discrepancies such as "instantaneously fulfilled" requests.

6.2. Cost

The deployment of each smart contract and each function call in Ethereum requires certain computational power, which is measured in gas paid in the form of Ether ETH. In addition, the security of the network is directly linked to the amount of gas miners can earn [19, 20]. For this reason, the higher the proposed gas price for a transaction, the higher the chances the transaction will be included in the next block. The default gas price for a single function call is 20 GWEI, which as of June 2019 would amount to $0,005. Since not all functions cost the same, we computed the amortized execution price for each transaction (which could involve multiple function invocations) at ~$0,053.

7. Conclusion

This paper summarizes how a privacy-centric transactional platform can be designed and developed to promote the accountability and oversight of homeless serving organizations. In the proposed system, the complete history of transactions between organizations offering homelessness services and individuals seeking such services is stored in a distributed ledger, and smart contracts are used to automate the exchange of information and facilitate tamper proof reporting capabilities without violating the privacy of homeless individuals. We believe that the proposed platform is the first step towards the trusted solution that non-profit organizations required to collect, analyze, and even share, sensitive data involving vulnerable populations desperately need.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. ECCS—1737443.

References

[1] Hasenfeld, Y. (2009) *Human services as complex organizations*. Sage Publications.

[2] Culhane, D. P. (2004) Homeless management information systems (HMIS); data and technical standards final notice.

[3] Nakamoto, S. (2019) "Bitcoin: A peer-to-peer electronic cash system." Manubot.

[4] Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., and Weinhardt, C. (2018) "A blockchain-based smart grid: towards sustainable local energy markets." *Computer Science-Research and Development*, **33(1-2)**, 207-214.

[5] Konstantinidis, I., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V., and Decker, S. (2018). "Blockchain for business applications: A systematic literature review." *In International Conference on Business Information Systems*, 384-399, Springer, Cham.

[6] Bartoletti, M., Cimoli, T., Pompianu, L., and Serusi, S. (2018) "Blockchain for social good: a quantitative analysis." *Proceedings of the 4th EAI International Conference on Smart Objects and Technologies for Social Good*, 37-42.

[7] Tapscott, D., and Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.

[8] Kosba, A., Miller, A., Shi, E., Wen, Z., and Papamanthou, C. (2016) "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." *2016 IEEE symposium on security and privacy*, SP, 839-858, IEEE.

[9] Koens, T., and Poll, E. (2018) "What blockchain alternative do you need?" *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, 113-129, Springer, Cham.

[10] Wüst, K., and Gervais, A. (2018) "Do you need a blockchain?" *2018 Crypto Valley Conference on Blockchain Technology* (CVCBT), 45-54, IEEE.

[11] Chelmis, C., and Yao, M. (2019) "Creating Public Value by Democratizing the Ecosystem of Human Service Providers." *Companion Proceedings of The 2019 World Wide Web Conference*, 231-236.

[12] Tian, F. (2017) "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things." *2017 International conference on service systems and service management*, 1-6, IEEE.

[13] Biswas, K., Muthukkumarasamy, V., and Tan, W. L. (2017) "Blockchain based wine supply chain traceability system."

[14] Lu, Q., and Xu, X. (2017) "Adaptable blockchain-based systems: A case study for product traceability." IEEE Software, **34(6)**, 21-27.

[15] Kim, H. M., and Laskowski, M. (2018) "Toward an ontology-driven blockchain design for supply-chain provenance." *Intelligent Systems in Accounting, Finance and Management*, **25(1)**, 18-27.

[16] Maouchi, M. E., Ersoy, O., and Erkin, Z. (2019) "DECOUPLES: a decentralized, unlinkable and privacy-preserving traceability system for the supply chain." *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 364-373.

[17] Act, A. (1996) Health insurance portability and accountability act of 1996. Public law, 104, 191.

[18] Ekblaw, A., Azaria, A., Halamka, J. D., and Lippman, A. (2016) "A Case Study for Blockchain in Healthcare: 'MedRec' prototype for electronic health records and medical research data." *Proceedings of IEEE open & big data conference*, vol. 13, 13.

[19] Wood, G. (2014) "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper, 151, 1-32.

[20] Antonopoulos, A. M., and Wood, G. (2018) *Mastering ethereum: building smart contracts and dapps*. O'reilly Media.

[21] Dannen, C. (2017) *Introducing Ethereum and solidity*, vol. 1, Berkeley: Apress.

[22] Lee, W. M. (2019) "Testing Smart Contracts Using Ganache." *Beginning Ethereum Smart Contracts Programming*, 147-167. Apress, Berkeley, CA.