

Using Blockchain and smart contracts for secure data provenance management

Aravind Ramachandran
The University of Texas At Dallas
800 W Campbell Rd
Richardson, Texas 75080
axr156530@utdallas.edu

Dr.Murat Kantarcioglu
The University of Texas At Dallas
800 W Campbell Rd
Richardson, Texas 75080
muratk@utdallas.edu

ABSTRACT

Blockchain technology has evolved from being an immutable ledger of transactions for cryptocurrencies to a programmable interactive environment for building distributed reliable applications. Although, blockchain technology has been used to address various challenges, to our knowledge none of the previous work focused on using blockchain to develop a secure and immutable scientific data provenance management framework that automatically verifies the provenance records. In this work, we leverage blockchain as a platform to facilitate trustworthy data provenance collection, verification and management. The developed system utilizes smart contracts and open provenance model (OPM) to record immutable data trails. We show that our proposed framework can efficiently and securely capture and validate provenance data, and prevent any malicious modification to the captured data as long as majority of the participants are honest.

KEYWORDS

Distributed systems, knowledge management, Data provenance, Block chain platform

1 INTRODUCTION

As the data used for scientific research increases exponentially, ensuring information quality and preventing data manipulation has emerged as an important factor in validating the research results. For example, an audit conducted by the Cancer and Leukemia Group B, one of the multi-center cancer clinical trial groups sponsored by the National Cancer Institute, found an incidence of fraud of 0.25 percentage of the trials conducted [10].

To **avoid data frauds** such as **data fabrication**, under-reporting of the results and **falsifying the results** to match research objectives in critical scientific research, the provenance of the data has to be maintained. In this context, **data provenance is defined as meta-data** that describes **where** the data of interest originated, **who owns** the data and **what were the transformations** that were done to the data. Data provenance facilitates the **integration of scientific data from diverse sources as well as providing verifiability of the sources**. Also, it acts as a yardstick for measuring how far the results of the experiments supports the actual objectives of the research and increases transparency and trustworthiness. For example, in [15], authors highlight the increase in transparency and trustworthiness of research results due to data provenance tracking. Therefore, to increase transparency and trustworthiness, provenance details of the data must be recorded from its generation to the transformations to the productions of results.¹

¹In section 6, we discuss two real-world settings where the provenance of data is crucial to prevent fraud.

Main challenges for a provenance system are the collection and immutable storage of provenance data, verifiability and preserving the privacy of the collected provenance data. Although tracking data provenance is important, but equally important is to ensure that security and privacy of the collected provenance data is maintained. Data used in any form of research may come from a myriad of sources and may contain sensitive information such as patient records. Any form of data provenance management system should ensure that the data is protected against unauthorized access. Also, a data provenance system should guarantee that the provenance details recorded in it are verifiable by the authorized personal without compromising the privacy and violating the ownership of the data.

Due this importance of collecting provenance information, systems such as Chimera[27] and myGrid[6] have been developed to store and process provenance information. Many of the existing provenance systems are based on a centralized storage model. The downside to the centralized system architecture is that if the central server is compromised, the whole data provenance trails could be compromised. In provenance systems based on distributed architecture, the security of the data provenance information is another area of contention. Any authorized users can corrupt the data stored in the provenance system. To our knowledge, the current provenance systems do not try to validate the changes before they are stored. Our proposed *DataProv* addresses these issues by using blockchain as a medium for storing provenance information and providing validations for each of the changes before logging the changes using smart contracts. The immutable nature of the blockchain environment ensure that the approved provenance changes cannot be modified by any users once they are stored. In *DataProv*, due to the distributed nature of the blockchain, the data provenance trails are replicated on every node of the blockchain ensuring high availability and fault tolerance.

1.1 Overview of Our Contributions

To address the above-mentioned challenges and requirements, in this work, we propose a system, *DataProv*, to securely capture scientific provenance data. *DataProv* combines the distributed immutable nature of the blockchain technology with cryptographic techniques to securely track data provenance without leaking privacy sensitive information. Furthermore, *DataProv* facilitates seamless generation of data provenance by authorized users and provides an automated method for verification of the generated provenance data. It also ensures the privacy of the data using public key encryption. The access control policies of the system restrict the access for the provenance data to authorized users.

The *DataProv* eliminates the need for a trusted third party storage and verification of the provenance data using smart contracts and randomized voting process. Furthermore, monetary punishment mechanism is enabled to discourage any malicious changes. These monetary payment penalties are guaranteed to be enforced as long as half of the participants are honest. Storage of the provenance data in *DataProv* is done using the log events of Smart Contracts [5] thereby saving further cost on storage. The *DataProv* system also provides customized verification scripts for authorized users to determine whether the changes submitted are valid or not.

We have implemented a *DataProv* system on top of Ethereum Blockchain [5] platform along with Meteor framework [23] for developing interfaces for the user's client module. The system was then evaluated in real world scenarios of clinical Drug trials and wheat production tracking system. The results show that *DataProv* system captures data provenance with fixed cost and moderate overheads.

The paper is structured as follows: Section2 describes the System model. Section 3 discusses the system architecture and walks through the provenance life cycle. In Section4 we take a detailed look at the various components of the system and their functionalities. Section5 describes the two different types of the voting process implemented for verification of changes trails. In section6 , we analyze the security and privacy parameters of the system. Section7 details the results obtained by implementing *DataProv* in two real-world environments. In section 8 we compare *DataProv* with other related blockchain based systems. Section9 we discuss the conclusions.

2 BACKGROUND

In this section, we discuss some of the tools used by our system and our threat model assumptions.

2.1 Ethereum

DataProv is built on top of the Ethereum, a distributed public blockchain network. Ethereum is a worldwide network of interconnected computers that execute and validate programs. Ethereum provides a decentralized Turing-complete platform called Ethereum virtual machines to run application codes called smart contracts. Ethereum also provides a currency called ether that is used to implement value exchange between nodes in the platform. Smart contracts are codes that reside within the Ethereum blockchain environment that executes when specific conditions are met. As the smart contracts reside on top of the ethereum blockchain, executions of the smart contract are also recorded in the blockchain. Smart contract can store and control ether. The functionality to control ether can be used to build applications that require deposit and payout of ethers such as online casino games, Identity managemets systems . In the Ethereum blockchain platform, each computational step has a cost associated with it [30] called gas.

2.2 Provenance Model

The *DataProv* system represents the data provenance trails using Open Provenance Model(OPM) [25]. In the OPM methodology, each action of the current system is represented using three parameters: 1) artifact (e.g., documents, files etc.) before and after change versions, 2) an agent which represents the initiator of the change and,

3) the process which is the process that changes the artifact from the previous version to the current version.

In our project, we represent the OPM model as a triple describing what the agents, artifacts, and process are and also number coded relationship edges between them. For example, the action of modifying a file can be represented in OPM as a tuple (user, file: old version, file: new version, process used for modifications).

2.3 Threat Model

The *DataProv* system can have two types of attackers: an external adversary and an internal adversary. An external adversary is a user who does not have access to the document/data in the system, but will actively try to corrupt the data provenance trails of a particular private document/data. The external adversary does not know the key to decrypt the document nor does he have access to the location in which the document is stored. The adversary only has knowledge of the document id and uses this information to mount an attack on the blockchain based data provenance trail system. We assume that the cloud storage is not trustworthy. To overcome this vulnerability, we store the files in encrypted form.

An internal adversary has access to the document/data granted by the owner in the *DataProv* system. The internal adversary is able to change the document and log the changes as provenance trails on the blockchain. An internal advisory cannot grant access to a document to another (we assume the adversary is not the owner of the particular document). The internal adversary may use the access rights to corrupt the provenance trails by logging in incorrect changes to the document trail. We assume that at least half of the users that can access the documents and associated provenance data are honest, and they can be trusted to verify the correctness of the changes done to the data. We believe that this assumption is reasonable since if most of the users are malicious, we cannot provide security guarantees [12].

3 SYSTEM OVERVIEW

We consider a scientific research setting where researchers keep their research records as a document stored in the cloud. The document (e.g., any data file) is encrypted by the owner of the document (e.g., the lead researcher). Access to the document is restricted using public key encryption. The owner of the research document provides access to the document to users by providing the key. For a user to log the provenance information in the *DataProv* system, the owner of a document needs grant access to the document to the user. In the *DataProv* system model, the changes to the documents are made through versioning. Each change related to a document is stored as a separate new version. The system assumes that only the latest version of the document/data file is used for modification. The system checks the condition that any document which contains changes not logged in the provenance data is ignored.

The system encourages truthful behavior by penalizing the users who submit wrong change provenance details. The voters are rewarded in the event they find a defective change submitted with a portion of the deposit amount for the change. The users log valid changes to the system using client applications running in each of the individual user's browser. Each of the client applications stores persistent data about the documents that the current user has access to using a back end database. For the current version of

DataProv, meteor JS [30] and MongoDB [24] are used to implement the client applications. The client applications communicate with the smart contract through a Geth node running at the client side. The smart contract system which stores the change records of the document is monitored for change events by the client. The smart contract stores access control policies along with details like the time of the last change of the particular document, signature of the last change and change logs etc.

3.1 Provenance Capture Life Cycle

An individual execution cycle of the *DataProv* system is shown in Figure 1. The steps involve: 1) A user, who wishes to add or change the result set, modifies the latest version of the data file and then uploads it to the cloud server. Different versions of the documents/data files are maintained in the cloud so as to revert back in the event a change is rejected. 2) The change requester then submits a change request to Vote Contract through the client module along with a *deposit amount*. The change request consists a digest comprising of: document Id, Encrypted form of hashes of the previous and current versions of the data file, Link to the location of the file in the cloud repository, timestamp at which the change was made and also the signature of the requester. 3) The client module submits the change and then initiates the voting period. During the voting period, authorized user clients verify the changes using the verifier script residing in the cloud storage. The scripts return true if the change is valid and false otherwise. 4) The clients cast their votes for/against the change based on the verification result, using the vote contract. The process is automated. 5) The vote contract records each of the votes cast by the users. At the end of the voting period, if the requisite amount of the users voted against the change, the change is rejected. The change initiator is penalized by the deposit amount and it is distributed among the voters. If after the voting period, the number of votes against the change is less than half of the voter, the change is accepted and the change requester is refunded the deposit amount. 6) In the event that a change is accepted after the voting process, the vote contract records the change in the document tracker contract. The log entries for each change consists of the following: author responsible for the change, the hash of the current document and the hash of the previous version of the document, high-level OPM representation of the current change and digital signature for future verification.

4 SYSTEM DETAILS

The basic setup of *DataProv* system consists of two components. The on-chain components which mainly consist of Ethereum Smart contracts for access control, generating and storing provenance trails and conducting voting process, and the off-chain modules which consist of client application module that interfaces with the smart contract to submit the changes and keeps timers for the voting process and the cloud based script for verification of each of the data file changes that are submitted.

4.1 On-chain module

The Ethereum blockchain platform provides executable programs that reside within the blockchain called Smart Contracts. The Smart contracts execute only when called and is capable of maintaining

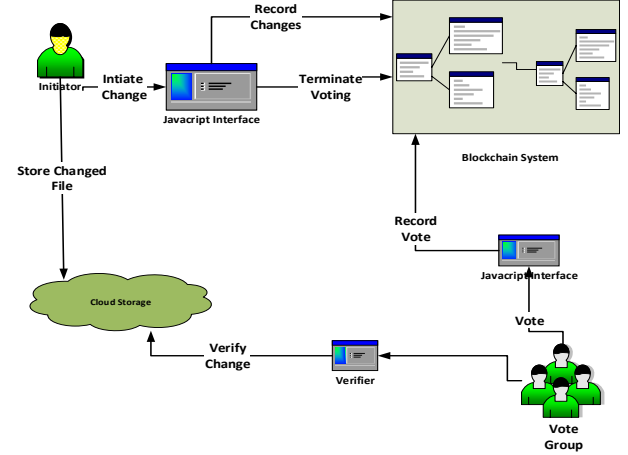


Figure 1: Provenance Life Cycle in *DataProv* System

state variables. *DataProv* on-chain module mainly consists of two smart contracts which we discuss in details below.

4.1.1 Document Tracker contract. The Document Tracker smart contract is used to keep track of all the changes to a given document. Document Tracker contract implements access control policies and maintains all the user access information to the documents. The contract also provides methods for provenance trail generation for a particular document. The generated document trails are stored as events in the event log of Document Track contract. Event log storage of data provenance trails is preferred due to cost per storage consideration in Ethereum blockchain environment [4]. The format of the change event is described in detail in Appendix A. Each change event also stores the digital signature of the initiator based on the message digest. The document tracker supports all the basic functionality of access control management such as create a document for tracking, grant users rights to add changes to a particular document provenance history, revoke users access rights to a particular document history and finally generating and storing provenance history of a particular document to the log. It is *important to note that*, *DataProv* does not store any sensitive information in plain text on the blockchain, because any information stored on the blockchain including the smart contract code is publicly accessible. In addition, due to storage costs and blockchain storage limits, actual data is stored off the blockchain, potentially in a cloud location.

The initial iteration of the provenance history is generated by the owner of a document when that document is added to the system. The contract enforces the constraint that granting access for adding provenance trails for a document is strictly controlled by the owner of the document. In the current implementation of *DataProv*, access rights to a particular document are nontransferable. In addition to the main methods, Document Tracker also consists of helper methods for checking the user access to a document and methods to update the owner of the document. The Document track contract also implements checks to prevent unauthorized calls to the functions. Every provenance change event *has to be approved through a voting process by the vote contract*. Access to the ChangeDocument

method (e.g., log the change to a document) is therefore restricted to only a call from vote contract.

We chose the *voting for verifying the submitted provenance information for two reasons*: 1) We want to efficiently prevent malicious changes that obviously violate data use constraints (e.g., not allowing the deletion of a patient record from the drug trial data). 2) We do not want the verification process to leak any sensitive information. Unfortunately, verification process could be very different in different settings. For example, for drug trials, main verification process could be to make sure that no patient is deleted (e.g., to boost the success rate of the drug) from the data set due to a fatal reaction. Also, if the verification is done in the contract, we need to do this in a way that discloses no information (e.g., using zero knowledge proofs [19] since contract source code and execution are publicly observable). To our knowledge, the existing zero knowledge techniques that are efficient are not general enough for all verification scenarios needed for our use case. At the same time, general zero knowledge verification techniques are not efficient enough to implement for provenance capturing [3]. Due to these reasons, we allow each participant client programs to run the verification code off-the-chain and use on-the-chain contract to vote for or against the change. Below, we discuss the details of the voting process.

4.1.2 Vote contract. The vote contract implements the voting protocol. The contract implements two types of voting: simple majority voting and threshold voting which are discussed in section 5. The initiator submits the change in an encrypted form along with his signature and document id to the vote contract. The vote contract receives the change and after verification generates a log event to initiate the voting phase for the change. The voting phase time interval for the set as t_1 (t_1 is set to one hour in our experiments) during which the participant can vote for/against the change. For each vote that is submitted, the vote contract verifies whether the vote is valid for the current voting period. At the end of the voting period, based on the type of voting process, the vote contract rejects/accepts the change based on the minimum number of votes for or against the change. If the total votes for the current voting period do not reach the minimum threshold of the number votes required, the vote contract restarts the voting phase. At the end of the voting phase, if the decision is to accept the change, Vote contract submits the change to the Document Track contract for generating the provenance event. The vote contract currently accepts only a single outstanding change for a particular document for ensuring the continuity of the data provenance chain and consistency. The protocol also contains the option of logging changes without voting process for documents whose total user-base is less than three.

4.2 Off-chain module

The off chain client JavaScript module runs on the browser of each of the client machine. The JavaScript module acts as an interface between the user and back-end smart contracts. The client module is responsible for communicating with the smart contract for the storage of the changes, retrieval of the changes and verifying the validity of the changes. In addition to the client modules in each of the clients, *DataProv* also has a verification script module running at the cloud storage location where the different versions of the

documents reside. The verification module verifies the validity of each change request of a particular document.

The client modules consist of different components as discussed below:

4.2.1 Client Interface module. The interface module mainly provides an interface for the user to interact with the smart contracts. The client module provides access methods for all the basic operations of the system such as adding a new document for tracking, providing grant and revoke information and also tracking change trails for the documents. The Interface module implicitly generates the digital signature for all the operations that the user performs through the module.

4.2.2 Event Watcher module. The event watcher module observes the change events generated by the Vote contract. The event watcher module reads any new change event logged into the contract, and checks if the current client is tracking the document for changes. If the current document change is relevant to the current user, the watcher contract decrypts the change event, verifies the signature of the change and then initiates a call to the verification script. It notifies the client about the verification results and if the verification result is valid, casts vote on behalf of the client. The voting process is automated such that the user need not be in the terminal. The watcher module uses a database to keep track of the details of documents that the current user is a stakeholder.

4.2.3 Timer module. The timer module is responsible for keeping track of the voting phases. When a change event to the document is generated, the timer module is called for initiating the voting interval for the change. The timer will trigger the termination of the voting process at the end of the voting interval.

4.2.4 Verification script: The verification script resides within the cloud storage of the system. The verification script validates the data file/document changes that are submitted to the *DataProv* system. The input to the verification script includes current and previous cryptographic hash of the document (from the changes submitted to *DataProv*) and the link to the latest version of the file. The verification script first verifies whether the hashes submitted to the files are valid. It then compares the current unconfirmed data file with the last stable version of the file. If any other changes to the file other than the ones mentioned in the change request is identified, the verification script notifies the user of a mismatch. If there are no invalid changes in the file, the verification script confirms the change as valid to the user. Once the changes are verified as valid, to prevent further manipulation of the document version, the verification script restricts the write access to only the owner of the original document. The verification script *can be customized according to the usage scenario* of the *DataProv* system and is developed as a plug-in module. In current implementation, we have developed the verification script based on Google appscript [13] to support Google Drive Storage.

5 VOTING PROCESS

The overall view of the voting process is described in figure 2. The voting process starts when the initiator submits a change to the Vote contract. The initiator client triggers a timer to initiate the voting phase of the newly submitted change. The vote contract

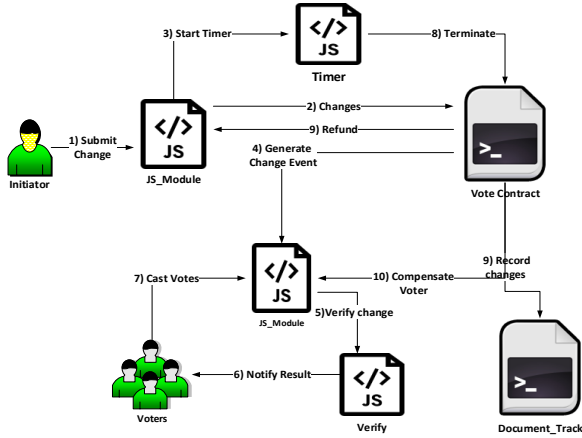


Figure 2: Voting procedure for a Document change.

generates an event which indicates the commencement of the voting phase for the submitted change. The Event listener module in the client applications reads the newly generated vote event. The client application verifies if it is a stakeholder in the current document change event. It then calls the verification script residing within the cloud along with the links to the current and previous versions of the file and the file hashes. The call to verification process occurs in every node based on the voting protocol policy. If the verification script returns as true then the client application notifies the user of the result. The client application then casts votes on the decision to accept or reject the changes. The vote contract on receiving the vote from a client records the user decision. The timer module will terminate the vote contract at the end of the voting period. The vote contract counts both for and against votes and rejects the change if the majority have voted against the change. If the change is accepted, the deposit by the initiator is refunded back. If the change is rejected then the deposit is divided among the participants of the voting phase. This way we incentivize truth telling by the participants and reward participants for catching errors.

In our current implementation of *DataProv*, we have implemented two types voting protocols.

5.1 Majority voting

In majority voting, all the clients/users who have a stake in a document vote on a change to that document. The decision of accepting or rejecting the change is based on a simple majority. If the majority of the users votes against the change, the change is rejected, else the change is accepted. The disadvantage of this voting scheme is that it requires every user who has access to the document to vote. This policy is ideal if the number of users of a document is small (e.g., less than 5). For larger number of users, requiring all the stakeholders to vote for every change is expensive. *DataProv* implements simple majority voting when the number of stakeholders for the document is less than 5.

5.2 Randomized Threshold Voting

Every client voting for each and every change is not efficient for systems that contain a large number of changes and users. For such scenarios, we propose randomized threshold voting. In randomized threshold voting, the contract requires that a minimum percentage of votes to accept or reject the change. Suppose the document has n users, to accept or reject a change, the vote contract threshold is s . To ensure that each voting phase for a change receives s votes, the contract tries to get expectedly t votes for $t > s$. The threshold t ensures that the minimum amount of for or against votes s are received for each change.

To determine whether to take part in change voting phase, each client generates a random number based on the formula:

$$Ks = \text{Hash}(\text{Bno}, \text{ETxt}, \text{Diff}, \text{Glim}, \text{Addr}) \bmod n$$

In the formula, Ks is the random number generated by the client by hashing Bno - the current block number, Etxt - the encrypted text in the change event, Diff - the current gas limit and the Addr - the initiator's address. If the generated number is below the threshold number t set by the vote contract (i.e. $Ks < t$), the client votes based on the result of the verification script. Once a vote is submitted, the vote contract generates the random number for each vote in a similar manner and verifies that the submitted vote is legitimate.

In this technique, the voting for the change is based on secure pseudo-random numbers; and it is not feasible to know which clients vote on which changes since the inputs to the hash function differs for each vote almost in a random manner. At the end of a voting period, if the vote contract finds that the total number of votes is below the threshold s , the vote contract restart the voting process. The probability of a restart event can be bounded as discussed in Section 5.2.1. If after predefined maximum number of restarts, the required number of votes are not received, the change is rejected and the deposit is refunded to the initiator of the current change. As we discuss below, we can set the system parameters t and s in such a way that this is very unlikely.

5.2.1 Randomized Voting Analysis. In the randomized voting based verification, we randomly choose users to vote for or against the change. For security purposes, we may want to randomly choose at least s users out of n users available for voting. Since the process is random, we may set the probability that a user is randomly chosen as $\frac{t}{n}$ where $t > s$. Given this, we can analyze, the probability that a given voting phase fail to get at least s votes. Before we do our analysis, we use the following Chernoff-Hoeffding bound result.

THEOREM 5.1. [28] Let $X = \sum_{i=1}^n X_i$ where $X_i, i \in [0..n]$, are independently distributed in $[0, 1]$. Then $\Pr[X < E[X] - a] \leq e^{-\frac{2a^2}{n}}$

Now using the theorem 5.1, we can prove the following theorem:

THEOREM 5.2. Given n users that can vote for a submitted change, for a randomized voting process that chooses a user with probability $\frac{t}{n}$ where $t > s$, and the probability p_f that a chosen user does not vote due to a failure, the probability that total number of users voted V is less than s is bounded as:

$$\Pr[V < s] \leq e^{-\frac{2(t-s-n \cdot p_f)^2}{n}}$$

The proof of theorem 5.2 is given in the appendix 10.2. We would like to the stress that p_f value can be adjusted for scenarios where

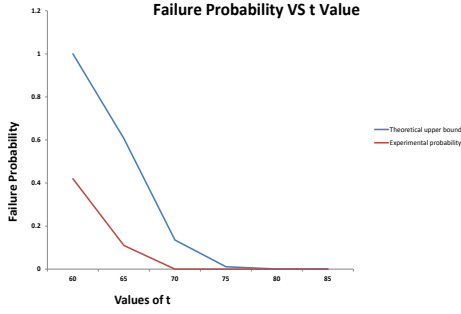


Figure 3: Failure Probability

some users are not online and/or do not want to vote for various reasons.

For varying t values, ($p_f = 0.0$) figure 3 reports the estimated versus theoretical probability of failure for the case where $n = 100$, and $s = 60$. To estimate the failure rate in smart contract voting, we run the voting protocol 100 times and count the number of cases where one round voting failed to get at least s votes. We use this count to estimate the probability of failure. As figure 3 shows when $t > 70$, we do not observe any failures even though the theoretical upper bound is non-zero.

Of course the next question is how can we set the t and s values in practice so that we do not get less than s votes for each voting period. To decide on the optimal values for t and s , we need to consider the total cost of voting at each round based on the failure probability (i.e., the probability that the total votes are less than s ($p_t = \Pr[V < s]$) for given failure probability p_f value). Below, we show the relationship between t, s, n and the expected cost of randomized voting process that continues until it gets at least s votes.

THEOREM 5.3. *Let failure probability be p_t where one round of voting gets less than s votes given that each of the existing n users votes with probability $\frac{t}{n}$. Then the expected cost of voting process $E[C_V]$ can be given as follows:*

$$E[C_V] = \frac{c \cdot t + c_1}{1 - p_t} \leq \frac{c \cdot t + c_1}{1 - e^{-\frac{2s(t-s)^2}{n}}}$$

for some system dependent constants c and c_1 .

Proof of the above theorem 5.3 is given in appendix 10.3. We can use the theorem 5.3 to find the optimal value for t given s and n based on the empirical constants c and c_1 .

6 SYSTEM ANALYSIS

In this section, we analyze the security and privacy aspects of our *DataProv* system. Specifically, we discuss how *DataProv* system handles attacks from the two type of adversaries discussed in section 2.3.

6.1 Security Analysis

An external adversary can try to attack the current system by submitting an invalid change request for a particular document ID. *DataProv* contract would stop any such attempts by enforcing access control policies on documents. The Document Track contract will accept only those change request from users who has been granted access by the owner of the document. All other change

requests are simply rejected by the contract. The Document track also penalizes the external adversary by withholding the deposit amount for the change for the attack attempt. An external adversary can mount a replay attack by using an earlier change request signature. Document track prevents this attack by keeping track of the latest change timestamp for a particular document. Any message carrying timestamp less than the latest timestamp for that document is ignored.

An internal user can be the owner of the document or one of the users who has been granted access to the document by the owner. An internal adversary who is not the owner of the document can try and corrupt the data provenance trails by submitting defective changes. Since *DataProv* system requires each of the changes to be approved by a minimum number of users, this attack from the internal adversary succeeds only if he/she can control more than half of the total number of users allowed for the document. The randomized threshold voting further ensures that the adversary cannot know in advance which among all the voters can take part in the voting for a particular change, making it difficult to mount the attack. The internal adversary who is an owner can corrupt the system if he/she colludes with other stakeholders and votes for the change. The owner is the only user who can grant access, the system can be at a disadvantage if the owner selects a group of users who are loyal to him and corrupt the provenance trail. Although this type of attack may be successful, it still leaves a traceable trail on the blockchain that could be used to detect the attack.

6.2 Privacy Analysis

The privacy protection for the provenance data trail is achieved by the use of hashing and encryption. An external user can infer only the document id and the number of changes that are made to a particular document id by looking at the event logs. Each change event encrypts the payload of the event so that all an external adversary could get is the document id, the cipher text, and the signature. The link to the cloud location where the actual file is encrypted. The other information that an external user can deduce from watching the contract transaction trails are to see which users are associated with a particular document id. This information is deducible by observing iterations of the voting contract. The Ethereum platform provides anonymization of users through the use of random public addresses. The users of *DataProv* does not reveal their identity in the environment instead uses public addresses to perform operations in the system. In *DataProv*, only the file owner will have the knowledge of identity of user of the document. An adversary observing multiple voting iterations could at most deduce the public addresses associated with each document.

6.3 Concurrency

In *DataProv* system, each change is the document is represented as a separate record. In the current system, we take each changes as a standalone change and does not allow multiple outstanding changes for the same document. This can be restrictive in certain use cases. The system could be modified to accept non conflicting changes in different parts of the tracked document. The system could accept changes to the document as long as they are non -conflicting there by increasing the concurrency. The above modification may involve

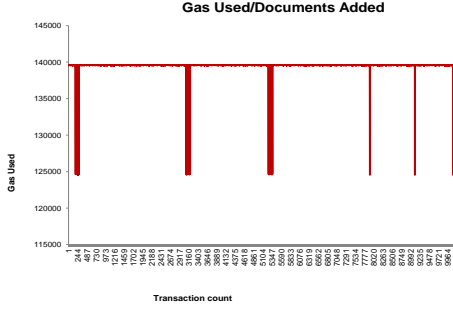


Figure 4: Cost distribution of adding documents.

adding an extra step to the verification script to check for non conflicting changes.

7 EXPERIMENTAL EVALUATION

To evaluate the *DataProv* system, we have tested it on two real life scenarios and calculated the average cost for each of the individual operations of the smart contract. In both of the scenarios, we have found that *DataProv* system performs at a constant cost for individual operations and within a reasonable overhead. We provide the details of these two cases below.

For both use cases, we have used the following evaluation setup: the client applications implemented using Meteor JS ran in a laptop(Core i7 2.4GHZ) and a desktop computer(Core i7 3.40GHZ) running Ubuntu 16.04.2 LTS. The smart contracts developed using Solidity language ran on Ethereum Ropsten Testnet. For both of the scenarios, we simulated the tests for a setting where we have 100 users for each of the document/data file. For the cloud based storage, we used Google Drive and the verification scripts were developed using Google AppScript.

7.1 Clinical Drug trial

In this use case, we consider the scenario of a clinical trial [9] of an experimental drug. In phase 3 of the drug trial process, the drug is tested with a patient count of 300 -1000 patients. The objective of the trial is to find the side effects of varying dosages on the patients. The drug trials may be conducted by various doctors in various locations and each of the results are recorded in a common document. Each of the experiment group updates the same document every month for a twelve month period. In the research setting, some of the patients may show adverse reaction to the drug. Researchers with a vested interest may try to remove those records that would show the side effects of the drug; and successive iterations of the same document will be missing records that would adversely affect the trustworthiness of the trails. To avoid the omission of records, the verification process for each of the change iterations of the document should ensure that the original patient set is maintained ².

7.1.1 Add Document. The Add Document function is used to add a document to the system for the purpose of maintaining its provenance. The owner of the document could be the head physician who initiates the whole process. The owner generates the

² In our experiments, we chose only this constraint for automatic verification process. Other constraints could be added for different scenarios.

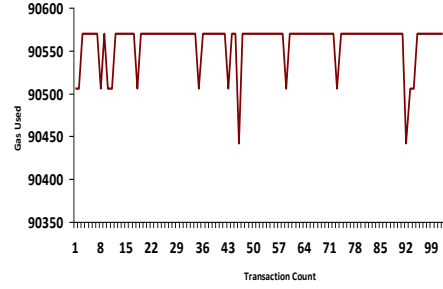


Figure 5: Gas Used for Each User Added.

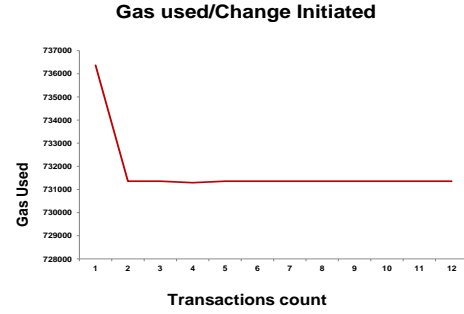


Figure 6: Gas Used to vote phase initiation.

initial form of the file that includes the entire initial set of patient details and initial drug dosage and adds it to the contract. The AddDocument functions generates a unique document id for each file added. Figure 4 shows the gas cost per file added for the contract. For the drug trials scenario, we need to add only a single file. The average gas cost per file added is 139552. Please note that in our setting, *DataProv* keeps *fixed size provenance records irrespective of the original data file size*.

7.1.2 Add User. The Add user function deals with the granting access to users for a document. The user who creates a particular document is recorded as the owner of the contract. Access to a particular contract can only be granted by the owner of that contract. Figure 5 gives the gas used per user added for one document where each transaction is the addition of a new user. The average gas used per transactions is 90559. The user details are stored as the hash of the user address. The spikes in the figure 5 represent the difference in the hashing requirements for the inputs.

7.1.3 Initiate Change. The initiate change function deals with triggering the voting process for logging a particular change. The initiate change requires the initiator of the change to deposit an amount with the contract while calling the contract. The initiate change function is called in the current scenario at the end of every month by the doctors to record the side effects(if any) of the current dosage. The average gas used for the changes is 731768. Figure 6 gives the gas distribution per initiation of voting phase for different transactions.

7.1.4 Voting phase. Once the change has been initiated, the client programs running in the voting quorum will verify the

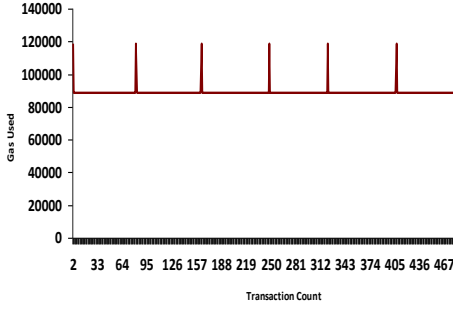


Figure 7: Cost distribution of voting process.

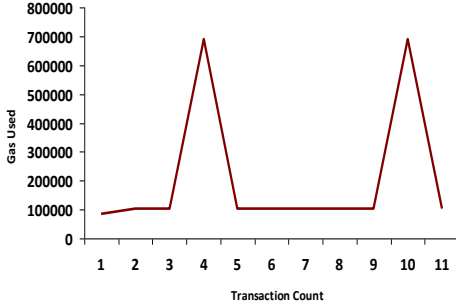


Figure 8: Cost distribution of a Termination operation.

changes and cast their votes. The vote of each of the participant is recorded by the smart contract and tallied up as for and against votes. The average gas used during this process is 89176. The gas consumption for each votes is given in figure 7. In the graph, we see that there are spikes at the beginning of each of the voting period. This is due to the initialization that occurs during the start of the voting intervals.

7.1.5 Termination: The result of the voting process determines whether to accept or reject the changes. If the majority of the people vote against the change, then the change is rejected. On rejection of a change, the voters who verified and voted are awarded the deposit amount of the initiator. On acceptance of the change, the change is recorded in the event log of the Document track contract and the deposit is refunded to the initiator of the change. In figure 8, we can see that there are two large spikes. These are the case in which the changes are rejected after the voting process. The gas used for these are more because all the voters are awarded a part of the deposit in the case of a rejection. The average gas used for termination is 249812.

7.1.6 Verification Script: In the drug trial scenario, the verification script verifies if the same set of patients given in the original trials are maintained across the various iterations of the data collection phase. The client initiates the verification script by providing it with the link of the current file version and hashes submitted with the change. The verification script generates its own hashes and compares with the submitted hashes. The script then compares patient identification columns with the previous files to ensure that none of the original patients have been omitted from the currently submitted version. The verification script then notifies the client of

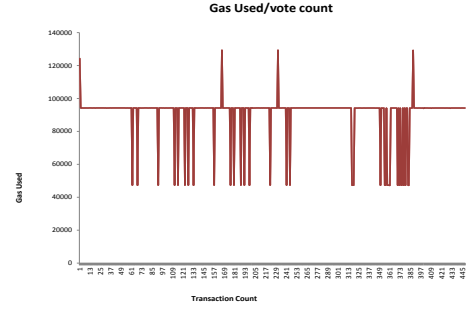


Figure 9: Cost distribution of vote phase.

the result. In the drug trials scenario, the verification script checks if all the patients records are retained in subsequent iterations. The run times of the verification script which depends on the data file size and the verification complexity, for data files that contain 1000 to 5000 patients, the verification run time vary between 7 secs to 31 secs.

7.2 Tracking Wheat Production

The second provenance relevant scenario that the system was adopted to is for the farming industry. The industry keeps track of the annual crop production of a given country. We implemented and tested our system based on the annual wheat production data system [29]. The Wheat production data file is updated quarterly and contains the quantitative details such as total production, total disappearance, and imports.

Our provenance system implements randomized threshold voting to confirm each change to the file. The Add User, initiate vote, initiate change functions of the system use the same amount of gas as with the drug trial scenario so we do not report here. The voting phase and the termination phase saw a slight increase in the gas amount used.

7.2.1 Initiate vote phase: During this phase a change to a document is submitted to the Vote Contract. The vote contract verifies the current user's access to the document and initiates the voting protocol. The average gas used is 778979.5.

7.2.2 Vote phase: We implemented the threshold voting method in the system. The participating nodes generate the random number and votes if the random number falls within the defined threshold. The vote contract checks if the vote is valid before recording the vote. We simulated an internal adversary who votes out of turn. The adversary controlled nodes vote even if the random number generated does not fall within the threshold. The contract rejects these votes. The gas used for such rejections are lower than the valid votes. The average gas used is 90862. The cost distribution per votes registered is illustrated in figure 9.

7.2.3 Termination: The timer module terminates voting phase after a fixed time interval. In the threshold voting, the voting process is restarted if the threshold amount of votes are not received for a particular change. The average rate of restarts for a particular change has been found out to be 3. Our results show that restarting consumes less gas (Same amount of gas as that of submitting change) than termination of the change phase. The cost for

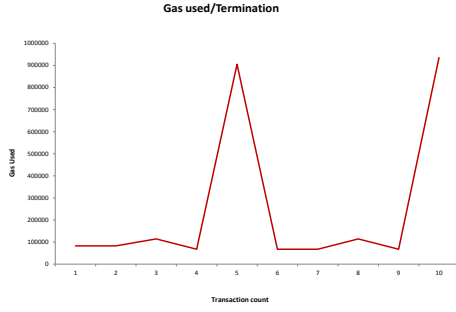


Figure 10: Cost distribution of termination.

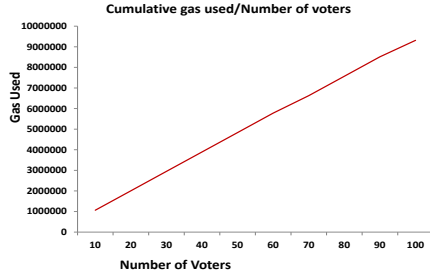


Figure 11: Cumulative gas consumption for the voting process

the termination operation is similar to the ones obtained in the clinical trials experiment and not reported here. The cost distribution per votes registered is illustrated in figure 10.

7.2.4 Verification Script: The verification script of the system compares the current files year on year data with that of the verified data. In Wheat Tracking use case, for data files that contain 1KB to 5KB patients, the verification run time vary between 10 secs to 45 secs.

7.3 Operation Cost

By observing the system contract executions in the above scenarios, we see that for an individual functions such as add user or add document, the gas used per transaction remains almost constant. The cumulative gas used for any individual function is a near linear function (e.g., as shown in figure 11 for vote function).

The gas usage is calculated at an average of 0.00000002 ethers per gas used. At the time of experimentation, a single ether cost is 90 US dollars. The table 1 shows the average gas used for various operations of the *DataProv* system. As the results indicate most operations can be executed with relatively little cost.

7.4 Contract Execution Duration

The time taken to perform each of the operations in the system is represented in the table 2. We can see that all the operations take near constant time to perform. The time taken for each operation is taken as the average time taken per thousand operations. The execution time of each of the above operations depends on the network speed and the speed of mining of the blocks, but in long

Operation	Avg gas spent	cost(USD)
Add Document	139552	0.2511936
Add User	90559	0.1630062
Initiate Change	731351.5	1.3164327
Vote	89176.33	0.160517394
Record Change	249812	0.4496616

Table 1: Cost of operations in the *DataProv* System

Operation	Time Taken(ms)
Add Document	926
Add User	877
Initiate Change	858
Vote	829
Record Change	950

Table 2: Time for operations in the *DataProv* System

run these times remain near constant and take less than a second in all of the usage scenarios.

8 RELATED WORK

Recently there have been several research studies that leverage blockchain as a platform for building trusted systems. Below, we summarize this work and discuss its relationship to our work.

Access control: In [17], authors explain the use of blockchain as a trans-organizational authentication system. The medrec system proposed in [1] implements access control for medical records across medical institutions through the usage of the public blockchain. Fairaccess system discussed in [26] is a decentralized access control system for the Internet of things devices using blockchain technology. In our *DataProv* system, we also implement access control policies, our focus is in the capturing of provenance data.

Trusted Authority system: The legal aspect of using blockchain as a verifiable trusted source was further expanded upon by common accords group [2] and in [11]. These work describe leveraging data stored in a public blockchain as a verifiable evidence in a court of law. Namecoin[7] system uses the blockchain technology as a trusted source for the Domain Name System (DNS). Our *DataProv* system eliminates the need for storing data on transactions by using the event logs of the smart contract to store the provenance trails. The smart contracts on top of the Ethereum platform acts as a decentralized trusted authority regarding all provenance trails stored. The provenance trails generated is also trustworthy as the decision to accept or reject a change depends on the voting protocol. *DataProv* therefore acts as a decentralized trust based system for data provenance.

Privacy preserving blockchain systems: The DECENT system discussed in [21] uses the blockchain along with the smart contracts to implement key management services. It implements the idea of secret sharing to securely share keys in a public environment. The Hawk system proposed in [18] implements the concept of zero

knowledge proofs combined with encryption to implement privacy preserving blockchain systems. The Hawk system uses two components: an on-chain component which uses smart contracts and zero-knowledge proofs to facilitates betting protocols and the off-chain components which generates zero knowledge proofs for the system. The Hawk system show how secure computations can be implemented on top of a public system such as the blockchain. . The use of secret sharing techniques for protecting sensitive information is further discussed in [16]. Compared to these works, the *DataProv* system utilizes encryption and hashing to preserve the privacy of the data stored in the public ethereum blockchain and secure communication channels between the smart contract and client machines to preserve the privacy. For efficiency and generalizable reasons, verification of the captured provenance data is done off-the-chain.

Security in smart contracts: The common security vulnerabilities in the smart contracts are discussed in [18]. This work illustrates a number of security issues in smart contracts such as call stack bug, block hash bug, and miners withholding the addition of blocks to gain an unfair advantage. This work further discusses how to avoid these pitfalls by including additional access verification and cryptographic primitives like encryption and hashing. Compared to these works, *DataProv* implements digital signatures to avoid malicious logging of provenance data. It uses an encrypted form of the provenance trails to avoid revealing details such as the location of the files and the user access information. *DataProv* further restricts the access to methods based on checks implemented on the user address.

Data Provenance: Leveraging the blockchain as a data provenance tracker was first discussed by the Project Provenance [22]. In this work, blockchain transactions are used to store provenance details of food products from production to the consumer. In addition, in [14], the use of blockchain as provenance platform is presented as one of the four breakout cases of the blockchain platform. The use of bitcoin as a data provenance system for research scenario was further explored in [8]. The author suggested the idea of storing the research objectives as an encoded file in the data fields of bitcoin transactions. Compared to these works, the *DataProv* system adopts the immutability of the blockchain environment and implements a full stack privacy preserving, verified data provenance store with access control policies. The provenance chains that are generated by the *DataProv* system are stored as event logs there by saving costs on storage. The system facilitates the verification of these provenance events by any authorized users. *DataProv* provides a platform to implement custom verification scripts suited for the application area. The system ensures privacy by using public key encryption and preserves integrity by the use of digital signatures. The ProvChain [20] system provides a data provenance system based on blockchain technology. The ProvChain system uses monitor programs called 'hooks' to track the changes that occur in the cloud storage system and records each and generates events corresponding to the actions of the users. The user events thus recorded are then stored on the blockchain as transactions. The verification process is achieved by an external entity known as auditor. The auditor generates transaction receipts using Tieron API [22]. The Provchain system verifies the changes after the information is

logged on to the blockchain. The *DataProv* differs from Provchain by implementing automated verification scripts and rejecting the invalid changes. The change hash-chain generated by the *DataProv* records only the changes that are verified by the verification script. This guarantees that the changed document is always valid and prevents any chance of collusion between the auditor and the stakeholders. Another major difference of compared to Provchain is that *DataProv* implements incentivized voting using smart contracts to penalize the users who tries to log invalid changes to the system. The use of randomized voting reduces the centralization of the verification process. Therefore, there is no need for a physical verifier as the verification script verifies the changes before voting on the changes. The advantage of developing verification script is that a verification script for a scenario could be reused by similar applications there by reducing the cost of development.

9 CONCLUSION

The *DataProv* is a blockchain based system that provides access control based privacy-preserving data provenance trails. In *DataProv* system, an authorized user can verify the changes that are made to any data file. It also provides a proof of change with the use of digital signatures and timestamping. The system ensures that the change logs in the blockchain environment are only accessed by the authorized users with appropriate keys. The *DataProv* system further enhances trustworthiness of the data trails by implementing randomized voting for the change trails recorded/captured and any deviation is punished by a monetary penalty using smart contracts. The evaluation of the system based on two real life scenarios has shown that individual operations of the system runs with acceptable cost and near constant time.

10 APPENDIX

10.1 Change Log Event Format

change(docid,agent, $E_K(\text{docid},H(X_o),H(X_n),\text{link},\text{ts}),\text{OPM},\text{sign}_k)$

where

docid = unique identifier of the Document.

agent = address of change initiator

E_K = Encrypted Text

$H(X_o)$ = Hash of previous file version

$H(X_n)$ = Hash of new file version

link = link to cloud storage location

opm = High level representation of the OPM model

ts = latest timestamp

sign_k = signature of initiator based on Encrypted text

10.2 Proof of Theorem 5.2

PROOF. Let V_i be the indicator variable that gets the value 1 if i^{th} user is selected by the randomized voting process. By definition, we can write $V = \sum_{i=1}^n V_i$. Therefore, expected value of V can be written as:

$$E(V) = E\left(\sum_{i=1}^n V_i\right) = n * E(V_1) = n * \left(\frac{t}{n} - p_f\right) = t - n.p_f$$

Now we can use the theorem 5.1, and set $a = (t - n.p_f - s)$ and $E[V] = t - n.p_f$. This concludes the proof. \square

10.3 Proof of Theorem 5.3

PROOF. For a given one round voting failure probability p_t and the cost of one round voting C_t , we can compute the expected cost of voting phase (i.e., voting continues till we have a round where at least s users voted) as follows:

$$\begin{aligned} E[C_V] &= (1 - p_t) \cdot C_t + p_t(E[C_V] + C_t) \\ &= C_t + p_t \cdot E[C_V] \\ &= \frac{C_t}{1 - p_t} \end{aligned}$$

In the above equation we use the fact that the expected cost is C_t if there is no failure. If there is failure, we pay the cost of one round of voting and then restart the voting from scratch. Solving this recursive equation gives us the required result. Furthermore, our empirical analysis show that total cost of one round voting C_t is a linear function of t , and can be represented as a linear function $c \cdot t + c_1$ for some constants c and c_1 . So replacing $C_t = c \cdot t + c_1$ and using the theorem 5.2 to bound $p_t \leq e^{-\frac{2s(t-s)^2}{n}}$ concludes our proof. \square

REFERENCES

- [1] Thiago Vieira, Andrew Lippman, Ariel Ekblaw, Asaf Azaria. 2016. MedRec: Medical Data Management on the Blockchain. (2016). version: 57e013615dbf3f3300152554.
- [2] David Bollier. 2015. Reinventing Law for the Commons. (2015). <http://www.commonaccord.org/>
- [3] Zvika Brakerski, Jonathan Katz, Gil Segev, and Arkady Yerukhimovich. 2011. Limits on the Power of Zero-Knowledge Proofs in Cryptographic Constructions. In *Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings*. 559–578. https://doi.org/10.1007/978-3-642-19571-6_34
- [4] Jonathan Brown. 2015. Storing compressed text in Ethereum transaction logs. (2015). <http://jonathanpatrick.me/blog/ethereum-compressed-text>
- [5] Vitalik Buterin. 2015. A Next-Generation Smart Contract and Decentralized Application Platform. (2015). September.
- [6] Tim Clark, Paolo Ciccarese, and Carole A. Goble. 2013. Micropublications: a Semantic Model for Claims, Evidence, Arguments and Annotations in Biomedical Communications. *CoRR* abs/1305.3506 (2013). <http://arxiv.org/abs/1305.3506>
- [7] Vincent Durham. 2010. NAMECOIN. <https://namecoin.org/>.
- [8] The Economist. 2016. Better with bitcoin. (2016). <http://www.economist.com/news/science-and-technology/21699099-blockchain-technology-could-improve-reliability-medical-trials-better>.
- [9] US Food and Drug Administration. 2017. *Clinical Research*. <https://www.fda.gov/ForPatients/Approvals/Drugs/ucm405622.htm>.
- [10] Buyse M, George SL. 2015. Data fraud in clinical trials. *PMC* 5, 2 (2015), 161–173. <https://doi.org/10.4155/cli>
- [11] Bela Gipp, Jagrut Kosti, and Corinna Breiter. 2016. Securing Video Integrity Using Decentralized Trusted Timestamping on the Blockchain. In *Proceedings of the 10th Mediterranean Conference on Information Systems (MCIS)*. Paphos, Cyprus.
- [12] Oded Goldreich. 2004. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, New York, NY, USA.
- [13] Google. 2017. *Google Appscript*. <https://developers.google.com/apps-script/>.
- [14] Gideon Greenspan. 2016. Four Genuine Blockchain Use Cases. (May 2016). <http://www.coindesk.com/four-genuine-blockchain-use-cases/>
- [15] R. R. Downs R. Duerr J. C. Goldstein M. A. Parsons Hills, D. J. and H. K. Ramapriyan. 2015. The importance of data set provenance for science. (2015). version: doi:10.1029/2015EO040557.
- [16] Roman Jagomardis, Peeter Laud, and Alisa Pankova. 2015. Preprocessing-Based Verification of Multiparty Protocols with Honest Majority. Cryptology ePrint Archive, Report 2015/674. (2015). <http://eprint.iacr.org/2015/674>.
- [17] Cruz Jason, Paul and Kaji Yuichi. 2015. The Bitcoin Network as Platform for Trans-Organizational Attribute Authentication. *IPSJ SIG Notes* 2015, 12 (feb 2015), 1–6. <http://ci.nii.ac.jp/naid/110009877764/en/>
- [18] Ahmed Kosba, Andrew Miller, Kevin Delmolino, Mitchell Arnett and Elaine Shi. 2015. Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. Cryptology ePrint Archive, Report 2015/460. (2015). <http://eprint.iacr.org/2015/460>.
- [19] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. 2015. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. Cryptology ePrint Archive, Report 2015/675. (2015). <http://eprint.iacr.org/2015/675>.
- [20] Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. 2017. ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid '17)*. IEEE Press, Piscataway, NJ, USA, 468–477. <https://doi.org/10.1109/CCGRID.2017.8>
- [21] Peter Linder. 2016. DEcryption Contract ENforcement Tool (DECENT): A Practical Alternative to Government Decryption Backdoors. Cryptology ePrint Archive, Report 2016/245. (2016). <http://eprint.iacr.org/2016/245>.
- [22] Project Provenance Ltd. 2015. Blockchain: the solution for transparency in product supply chains. (2015). <https://www.provenance.org/whitepaper>
- [23] MeteorJS. 2016. (May 2016). <https://www.meteor.com/>
- [24] MongoDB. 2017. MongoDB. (Jan. 2017). <https://www.mongodb.com/>
- [25] Open Provenance model 2007. *Open Provenance Model*. Open Provenance model. <http://openprovenance.org/>.
- [26] Aafaf Ouaddah, Anas Abou El Kalam, and Abdellah Ait Ouahman. 2016. FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and Communication Networks* 9, 18 (2016), 5943–5964. <https://doi.org/10.1002/sec.1748>
- [27] Eric F. Pettersen, Thomas D. Goddard, Conrad C. Huang, Gregory S. Couch, Daniel M. Greenblatt, Elaine C. Meng, and Thomas E. Ferrin. 2004. UCSF Chimera - A visualization system for exploratory research and analysis. *Journal of Computational Chemistry* 25, 13 (2004), 1605–1612. <https://doi.org/10.1002/jcc.20084>
- [28] Jeff M. Phillips. 2012. Chernoff-Hoeffding Inequality and Applications. *CoRR* abs/1209.6396 (2012). <http://arxiv.org/abs/1209.6396>
- [29] USDA. 2017. Annual Wheat production data, USA. (2017). <https://www.ers.usda.gov/data-products/wheat-data/>
- [30] Gavin Wood. 2017. ETHEREUM: A secure decentralized generalized transaction ledger. (2017). <http://gavwood.com/paper.pdf>