Blockchain for Digital Crime Prevention: The Case of Health Informatics

Completed Research Full Paper

Kane J. Smith  
Virginia Commonwealth University  
301 W. Main St., Richmond, VA 23284  
smithkj6@vcu.edu

Gurpreet Dhillon  
Virginia Commonwealth University  
301 W. Main St., Richmond, VA 23284  
gdhillon@vcu.edu

Abstract

Blockchain implementation in Health Informatics is a significant challenge in a rapidly evolving era of privacy and security concerns. Dealing with such concerns, healthcare institutions are presented with a serious problem in how to manage new technology and allocate finite resources to maximize value. It is important to understand how organizations address these concerns by exploring blockchain implementation management in the context of cybersecurity. The problem question is twofold: First, how can objectives that are important based on the strategic values of an organization with regard to the implementation of blockchain technology be used to ensure privacy and security of vulnerable patient data? Second, how can these objectives then be used to evaluate proposed solutions for blockchain implementation in electronic medical record systems? In this paper we utilize Keeney’s (1992) value focused thinking to demonstrate how the process can occur to maximize value-add within healthcare organizations.

Keywords

Blockchain, Decision Analytics, Value Focused Thinking, Health Informatics

Introduction

Years of heavy regulation and bureaucratic inefficiency have slowed innovation for electronic health records (EHRs) and organizations are now faced with critical need for such innovation (Azaria et al. 2016). With large amounts of patient data, privacy and security issues surrounding EHR susceptibility to cybercrime is on the rise (Peterson et al. 2016). Patient data contains a trove is highly valued data to cybercriminals (Peterson et al. 2016) and as such will become a prime target moving forward. Organizations must either adopt new security measures to address these threats or be subject to the fallout of failure to do so. Blockchain technology represents a new and useful means of securing and protecting vulnerable patient data, however as interest in a technology grows the selection of proposed offerings using this solution will only grow. Therefore, blockchain implementation in Health Informatics is a significant challenge in a rapidly evolving era of privacy and security concerns. It is important to note that health informatics is contextualized for the purposes of this paper to be, “a term describing the acquiring, storing, retrieving and using of healthcare information (www.nlm.nih.gov).” Hence, when dealing with such concerns, healthcare institutions are presented with a serious problem in how to manage security and privacy as well as where to allocate resources to maximize value in the application of technological solutions. It is important to understand how organizations address these concerns by exploring blockchain implementation so it can be managed in the context of cybersecurity. To do this, the problem question is twofold: First, how can objectives that are important based on the strategic values of an organization with regard to the implementation of blockchain technology be used to ensure privacy and security of vulnerable patient data? Second, how can these objectives then be used to evaluate proposed solutions for blockchain implementation in electronic medical record systems in healthcare organizations. The paper is organized into five sections: introduction, literature pertinent to blockchain and implementation in Healthcare, the theoretical and methodological aspects of this research, an
example application of this research to guide its use in the decision making process and finally a
discussion that also includes the limitations and future research directions.

**Literature Review**

When reviewing the available literature regarding blockchain and blockchain in health Informatics, it is
important to understand the context of blockchain technology and the proposition of using it as a means
of securing patient records in electronic health records. To do this, blockchain technology is provided a
brief description and then the prior work in academia regarding the use of blockchain to address privacy
and security concerns in healthcare. While the various literature addresses a particular and unique
concept of interest related to blockchain technology in healthcare it is important to note that these
selected works are not all-inclusive of the entire spectrum of blockchain research. However, current
research in the domain of blockchain technology and its application in health informatics is presented for
two purposes. First, to provide both background context for the purpose of this paper and secondly to
demonstrate that current research is concerned with the technological aspect of how to implement rather
than on how such a solution can address unique organizational concerns. Therefore, this review of current
blockchain research is intended to place focus on the gap in the literature that our research is intended to
fill.

**Blockchain**

While a large portion of the population is at least tangentially familiar with Bitcoin and the concept of a
decentralized digital currency, they may be much less familiar with the underlying technology that allows
Bitcoin to function, known as “blockchain.” The lack of awareness is understandable, as Bitcoin was the
first real implementation of blockchain technology, invented by a developer known as Satoshi Nakamoto,
the official creator of Bitcoin, and the underlying blockchain technology. “Satoshi Nakamoto” is a
pseudonym, as the true identity or identities behind it are still unknown to this day. In the seminal work
backbone of blockchain technology. It is described in the introduction as, “The network timestamps
transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that
cannot be changed without redoing the proof-of-work” (Nakamoto, 2008). The transactions are hashed
into a single block, and all blocks make up the chain, hence the name “blockchain.”

Blockchain was created to prevent the problem of double-spending within cryptocurrency, its
implementation is essentially a distributed ledger system, wherein participants work to build blocks on
the chain by hashing individual transactions with the chain acting as the ledger. As a blockchain is a
decentralized distributed ledger, it means that multiple participants involved in building the blocks can
hold a copy of the ledger. In technical terms, every participant in the blockchain that holds a copy of the
ledger is known as a “node.” As all nodes hold a copy of the ledger, it means the ledger is decentralized
and does not exist in a single location, which prevents a central authority from altering the ledger in any
way as all nodes must “agree to” any additions to the ledger. Therefore the most important role the nodes
have is to add blocks to the chain, which is done by processing transactions (of which blocks are
composed) through a one-way cryptographic hash function that cannot be altered retroactively (Iansiti &
Lakhani 2017). This means that a blockchain then acts as an open and distributed ledger that records
transactions between various parties in an efficient, verifiable and permanent manner (Iansiti & Lakhani
2017). These types of secure transactions can be very appealing to any organization interested in
maintaining information in a secure, yet efficient manner such as medical or banking records.

**Blockchain in Health Informatics**

There are numerous contributions to the application of blockchain technology in health informatics
dealing with the applications of blockchain for solving privacy and security concerns in healthcare
organizations. One such example is that of Liu (2017) which discuss the major aspects of medical records,
blockchain and big data. The author details the advantages and disadvantages of using blockchain on
medical records storage and retrieval. Further, they detail various alternatives for using blockchain and
big data techniques as well as investigating different aspects of medical records that can be impacted by
this technology. Another work which delves into a more technical application of blockchain technology is
that of Peterson et al. (2016) at the Mayo Clinic which details how heterogeneous data structures in the EHR’s of various healthcare organizations may preclude compatibility of shared information resources as well as disparate use of healthcare terminology can limit data comprehension. Most critically, the authors state that even if structure and semantics could be agreed upon for data integration methods, both security and data consistency concerns abound. As EHRs are centralized data stores, authority providers are attractive targets for cyber-attacks and then establishing a consistent view of the patient record across a data sharing network is thusly problematic (Peterson et al. 2016). Therefore, a Blockchain-based approach to sharing patient data is presented in which the approach trades a single centralized source of trust in favor of network consensus, and predicates consensus on proof of structural and semantic interoperability (Peterson et al. 2016). Lastly, the work of Azaria et al. (2016) provides a proof of concept tool which implements blockchain technology in health informatics. In this paper, the authors propose MedRec: a decentralized record management system to handle EHRs that utilize blockchain technology. The system gives patients a comprehensive and immutable log which provides easy access to their medical information across providers and treatment sites (Azaria et al. 2016). By leveraging unique blockchain properties, their MedRec system manages authentication, confidentiality, accountability and data sharing which are important considerations when handling sensitive information (Azaria et al. 2016). These developments of blockchain technology application in health informatics is important as they highlight the need for a means by which healthcare organizations can evaluate what will eventually become a vast array of blockchain-centric solutions. This is what serves as the basis for the need to develop a model which healthcare organizations can use to determine which proposed solution from a set of alternatives best meets their needs.

**Methodology**

To ensure greater measures of protection from digital crime using blockchain technology, it is necessary to identify the fundamental objectives for implementing the technology in Health Informatics. This is where Keeney’s (1992; 1996) Value Focused Thinking (VFT) for decision analysis can help create an objective-based framework for healthcare and related organizations to model the necessary objectives for preventing digital crime using blockchain technology. This model can then be used to assess alternatives for implementation and demonstrate gaps in all proposed solution’s performance relative to the objective’s goals which acts as quantitative metrics for comparison (Merrick et al. 2005). This process occurs in five basic steps adapted from Keeney (1992) and Merrick et al. (2005) and derives its objectives either directly from literature or expert users of blockchain technology and health informatics can be interviewed to elicit the objectives as well as the necessary importance and swing weights to fully build out the proposed model. Before this can be done it is first necessary to discuss in detail the steps, which will be undertaken as the methodology for this research. It is important to note that this model will use fundamental objectives, which are defined by Keeney (1992; 1996) as “providing a structure for clarifying the values of interest in a given decision context and provide a basis for evaluating alternative,” while strategic objectives are “relevant to a wide range of decision contexts, to a long time period, and to many levels in an organization.” This proposed model must then use fundamental objectives for building a model aimed at assessing proposed solutions for blockchain technology implementation, but organizes them in the context of strategic objectives which meet the general goals of an organization embarking upon an IT project in the decision context.

The process for developing and quantifying an objective-based model involves the following steps (Keeney 1992, 1996; Merrick et al. 2005):

1. Critical analysis of academic literature or generation of values through a value forum or survey and interview type methods, which is conducted by the analysts, to identify the factors that are fundamentally important as well as elicitation of any omitted objectives from expert users. The analyst ensures that important objectives are not omitted.

2. The objectives are structured into a hierarchy that clarifies the differences between strategic and fundamental objectives and eliminates redundancies of objectives derived from the literature and expert users.
(3) Expert users define attributes for the objectives to clarify exactly what the objectives mean and to measure any possible consequences. The measurements also include importance and swing weighting for each objective in the model by the expert users (Kirkwood 1997).

(4) Construction of a Multi-Attribute Utility Model. The tradeoffs elicited in step 3 are then converted into weights for the attributes using standard multi-attribute utility techniques (Keeney & Raiffa 1976, Keeney 1990, Keeney 1996). For most decision context a multi-attribute utility model is only a simple weighted average of the constructed single-attribute utilities. However, researchers can perform additional tests to examine if a more complex multiplicative or multi-linear model is necessary (Keeney & Raiffa 1976), if they find the simple additive model to be questionable in application. Should a researcher choose a more complex model, additional tradeoff questions may be needed to elicit any additional parameters for the model. The multi-attribute utility model (also a value model, Keeney 1992; Akkermans & Van Helden 2002) is then used in combination with the expert evaluations to generate an overall model.

The best way to describe the utility of this type of value model is to consider the various fundamental objectives as being $O_1, ...O_n$ and $m_1$ as a measure for a fundamental objective $O_1$. It follows therefore that the vector $m = (m_1, m_2, ..., m_n)$ would provide a description of a particular path in which a fundamental objective is delivered. The accumulative value of $m$ would then serve as a measure (quantitative or qualitative) of the idiosyncratic resources and abilities that would fit the decision context (i.e. the prevention of digital crime in Health Informatics using blockchain technology). In the additive case (Keeney 1992), the overall utility $v$ for any alternative described by $m_1-m_n$ is:

$$v = \sum_{i=1}^{n} k_i v_i(m_i)$$

where $n$ is the number of attributes, where $k_i$ is the weight ascribed to the objective $O_i$ and $v_i$ is the relative desirability scaling.

(5) Assessing the value gaps of individual objectives based on the outcomes of the analysis. This identifies areas for improvement and allows a cost-benefit analysis to be performed to determine to most cost-effective areas to implement change and target finite organizational resources.

Once these steps have been completed it is necessary to test the proposed model and the newly developed fundamental objectives and demonstrate its usefulness in the context of an organizational analysis of proposed alternatives. This is done through the use of an analysis of various proposed solutions for blockchain implementation in the context of digital crime prevention. The experts will utilize the model and evaluate each of the objective criteria on their respective measurement scales, which are created for the model. Once that is completed a score will be created on a scale of 0 to 100 (0 being the worst and 100 the best) to address its relative success in addressing the fundamental objectives for blockchain implementation. Then a gap analysis of each objective and strategic context can be completed to demonstrate which objectives were most completely addressed by the selected alternative and which ones have room for improvement. This analysis demonstrates both the impact of the objective itself (its given contribution to the model), the degree to which it was addressed in the project and the gap or area for improvement. With this information the organization can employ a cost-benefit analysis to determine which objectives with the highest gaps in performance should be rectified. This is important as an organization may identify several areas to target improvement, but some may require additional costs, which may be untenable to the organization. Instead objectives elucidated by the model, which are the most impactful and cost effective to address should be those focused on by the organization. In the following sections an illustrative example will be sued to demonstrate how this process can be used by a healthcare organization to develop their own model for assessing proposed blockchain solutions and select the best alternative for driving a successful implementation.
Application Example

In this section an example of how the process for developing an objective framework for evaluating blockchain applications in Health Informatics is demonstrated. The purpose is to describe how a healthcare organization can develop a framework for assessing blockchain solutions for integration into their electronic health record system. It will begin with the development of fundamental objectives as well as a framework and finish with how solutions can be further analyzed with a gap analysis to determine points of possible improvement. The process for developing fundamental objectives can take two paths as both, traditional Value Focused Thinking (VFT) and the Value Forum Process (VFP), use the same general process described in this section and can be applied by any organization.

Developing Fundamental Objectives

The following three-step process is used to identify and organize the values that an individual might have with respect to a specific decision context (Keeney 1992): First, interviews are conducted which elicit the values an individual might have within a decision context. For Second, individual values and statements are converted into a common value format, such as an objective oriented statement. Then similar objectives are grouped together in order to form clusters of objectives. Finally, the objectives are then classified as either fundamental to the decision context, resulting in a fundamental objective, or simply a means to achieve the fundamental objectives, which is known as a means objective.

Identifying values

To begin, interviews are conducted with the concerned peoples as a process of identifying values. At the beginning of each interview, the purpose is clarified and context and scope of the interview are established. The core objective in this interview is to understand the fundamental objectives for the desired decision context. To set the decision context, we emphasize that the scope for eliciting these values is limited to either individuals or organizations such as businesses or governments. After defining the scope of the interview, explanations are provided to the interviewee so that they can understand the decision context, in this case blockchain integration for healthcare organizations, which helps to establish a common understanding of all terminology. It should be made clear to respondents that the goal is to understand values that people might have with respect to the topic. To identify these values questions are posed about their personal values toward the decision context and all questions should be open-ended. As individuals can express values differently, an inherent difficulty exists with the quiescent nature of the values, so different probing techniques must be used to identify latent values. For Keeney (1992), probing techniques are suggested with words like trade-offs or consequences etc. as being useful in making such implicit values explicit.

Structuring values

Once the values are identified, a process of value structuring and objective development begins. Step one is that all statements are restated in a common form where duplicates are removed. Common form restatement is simply converting like ideas or values to similar wording to reduce duplicate ideas. Then, these common form values considered from these statements are converted into sub-objectives. According to Keeney (1999), an objective is constituted of the decision context, an object and a direction of preferences. With all values systematically reviewed and converted into sub-objectives, it may be found that a number of sub-objectives deal with a similar issues, making it necessary to determine if these overlapping clusters should be merged or stand alone. By carefully reviewing the content of each of these sub-objectives, clusters are developed that group similar ones together (thus removing any overlap) and then each cluster of sub-objectives is labeled by its overall theme, which then becomes the main objective of the cluster.

Organizing objectives
The list of sub-objectives and corresponding clusters initially include both means and fundamental objectives so we must differentiate the two. This is accomplished by repeatedly linking objectives through means–ends relationships then specifying the fundamental objectives. To identify fundamental objectives, the question is asked, ‘Why is this objective important in the decision context? (Keeney 1994).’ If the objective is an essential reason for interest in the decision context, then the objective is a candidate as a fundamental objective. If the objective is important due its implications with respect to some other objective, then it is a candidate as a means objective. This is termed by Keeney (1994) as the ‘WITI test.’

**Example of Fundamental Objectives for Blockchain Integration**

Here, each fundamental objective is categorized by strategic objective, derived from academic literature and expert users, which are general in nature and applicable at the strategic level across an organization. Objectives can come from academic literature as they are often derived from interviews that perform, generally, the essence of VFT, but require the additional vetting of experts to ensure they meet the standards for use as a fundamental objective. It is important to note that using these strategic objectives as categories allows the derivation of fundamental objectives that align with the strategic objectives of an organization at the granular level. Further, an expert in Health Informatics and blockchain technology should be used for defining the measurable scales, eliciting importance and swing weights and then evaluating a use case to demonstrate real-world application. As a framework (Figure 1) objectives were derived from literature using the CIA Triad (Samonas & Coss 2014) to develop security-centric strategic objectives to serve as categories, and also to derive basic fundamental objectives within them made from independent components of the CIA Triad.

![Figure 1. Example of Objective Framework](image)

**Defining the Scales Using Experts**

In the next phase after experts have refined the fundamental objectives, which were derived from the literature, they use their expertise to clarify exactly what the objectives mean and to determine if any additional objectives of importance should be added. Additionally, experts determine the criteria used to measure these objectives in order to ensure a consistent model with which blockchain solutions can be evaluated by an organization. Therefore, the output of this phase (Figure 2) in the development of the evaluation model requires: all necessary objectives for evaluation, consistent definitions to ensure uniform understanding of the objectives and scales by which the objectives can be measure by the model. Some evaluation measure will require constructed scales as not all objectives may have easily quantifiable metrics by which they can be measured, however they are still important to the decision context and should be included.
Objective | Definition | Scale
--- | --- | ---
Trust | Perception of a system’s ability to meet the set of requirements for which it is trusted to perform those specific tasks | Constructed Scale (1-5):
1: Poor 2: Somewhat Poor
3: Average 4: Above Average
5: Best

Table 1. Example of Objective definition and measurement scale

Setting Importance and Swing Weights

Once the measurement scales and definitions are completed, importance and swing weighting for each objective in the model is elicited from the expert (Kirkwood 1997). In order to do this importance scales are constructed for each objective based on the proposed measurement scale. The importance weights are from 0 to 100 with 0 being the worst and 100 being the best. The experts weight points on the measurement scale with the importance weight, which allows for the construction of single-attribute value functions (Figure 2) (Keeney 1992, 1996; Merrick et al. 2005). Importance weights are intended to demonstrate an actual measure of difference between, for example, a rank of 1 and a rank of 5 for an objective. The goal is that if a 5 rating is the best and weighted 100 then a 4, which is weighted as a 85, is essentially 85% as good. This distinction is important, because without importance weights we are unable to discern how much worse a 4 is to a 5 as perceived by the rater of a proposed solution.

![Figure 2. Example of Single Attribute Utility Function for Trust](image)

After importance weights have been assigned, swing weights are elicited for each objective relative to the others as well as by category (See Table 2). This allows the framework to create a holistic evaluation (multi-attribute value function) of a proposed blockchain solution and define the overall impact of each objective relative to an organization’s strategic goals. The solution uses scaled weights (Kirkwood 1997) to derive global weights for the objectives themselves as well as for the strategic objectives. Similar to importance weights, we need a metric to define the impact of an objective in the overall context of the decision. Participants should be asked to review ‘all good’ and ‘all bad’ scenarios for each objective and rank the magnitude of change or ‘swing’ between these scenarios for each objective from largest to smallest by strategic category (each category has its objectives ranked separately). This means participants are then asked to assign a weight that indicates the relative magnitude of a given ‘swing’ with respect to the scenario they rated as having the largest degree of change between the ‘good’ and ‘bad’ scenario. To do this the objective that ‘swings’ the most in each category should be given a swing of 100 and each rank given a lower number going as low as 0, relative to the one above it in the ranking. The objective weights are then scaled by taking each weight and dividing it by the total of all weights. Global weights, which are necessary for categorical comparisons, are created by weighting each category and
then scaling those weights and multiplying each objective’s scaled weight by their respective category’s scaled weight.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Weight</th>
<th>Global Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>.37</td>
<td>.37</td>
</tr>
<tr>
<td>Trust</td>
<td>.18</td>
<td>.066</td>
</tr>
<tr>
<td>Identity Management</td>
<td>.19</td>
<td>.07</td>
</tr>
<tr>
<td>Integrity</td>
<td>.33</td>
<td>.33</td>
</tr>
<tr>
<td>Ethicality</td>
<td>.08</td>
<td>.026</td>
</tr>
<tr>
<td>Responsibility</td>
<td>.08</td>
<td>.026</td>
</tr>
<tr>
<td>Authenticity</td>
<td>.09</td>
<td>.03</td>
</tr>
<tr>
<td>Non-Repudiation</td>
<td>.08</td>
<td>.026</td>
</tr>
<tr>
<td>Availability</td>
<td>.3</td>
<td>.3</td>
</tr>
<tr>
<td>Correctness of Specification</td>
<td>.3</td>
<td>.09</td>
</tr>
</tbody>
</table>

Table 2. Example of scaled Objective swing weights

**Fundamental Objective Gap Analysis**

This will allow an organization to perform a gap analysis (Figure 3) by objective and category and develop processes improvements to overcome any deficiencies in proposed solutions if available alternatives cannot fully meet all organizational needs (Merrick et al. 2005). This is based on the objective’s single-attribute utility function and can be measured at the categorical level or in a more granular fashion at the objective level. If the developed functions demonstrate a maximum allowed utility of 30, but the proposed solution only provides 26, then a gap is demonstrated. However, this gap would be relatively small and may not have a value proposition for correcting this deficiency, while another with a gap of 15 out of a maximum of 36, would be an ideal candidate for reviewing for possible process improvements to rectify this gap.

![Figure 3. Example of Gap Analysis for proposed solution](image)

Hence, this is an important part for the evaluation of proposed blockchain solutions. It demonstrates to an organization both where a solution is lacking and if more than one area requires improvement, which is the most impactful. This enables an organization to more prudently address areas of need with the highest value per dollar, as it is unlikely, unless the organization selects a completely custom option for implementation that all objectives will be adequately addressed by any given solution.
Discussion

Blockchain technology is being proposed as a useful solution to the problem of security and privacy in the context of Health Informatics. For this reason this type of research is important as organizations are now faced with the daunting task of implementing a number of variations of this solution to address their organizational concerns. However, they will likely do so successfully without a mechanism by which they can fully evaluate a proposed solution in the context of their own organizational needs. Therefore, an objective-based framework will enable an organization to model their own strategic and fundamental objectives for enacting a blockchain solution in their organization aimed at the prevention of digital crimes. This methodology will provide a mechanism for quantitatively evaluating those objectives and return a set of tools which they can further use to address any shortcomings in the proposed solutions based on possible alternatives. Additionally, the VFT-based objective framework proposed in this paper allows an organization to collectively create this model, starting at the strategic level (think c-suite) and incorporate additional input from experts in order to develop a truly holistic organizational model. This can come in the form of objectives, which can be added and weighted into the model as well as in the form of the weights which can be collectively derived using a group-based forum.

This paper is not without limitations, as the demonstrated model in this paper is only an example. It serves only as a proof of concept and will require an actual use-case to stand up a working model. Further, sensitivity analyses should be performed to test how much the value gaps changed with variations in these weights (Merrick et al. 2005). As different organizations and experts can assign differing weights to the varying objectives, it is important to understand how value gaps can change based on differences in weights in order to ensure the gap analysis is robust to these possible changes. Lastly, this type of model and methodology uses cardinal utility functions, known as value functions and does not account for any uncertainty within the decision context. Therefore, development of an actual model should consider uncertainty and conduct a lottery to assess risk attitudes within an organization and overlaid onto the value function. This will create a utility function, which can then be compared to the value function and determine if the incorporation of uncertainty changes or alters the choice of alternatives.

The next phase of this research will extend the methodology for application on an actual use case in the field of Health Informatics. A healthcare organization has been selected which will serve as the basis for developing a full model for blockchain implementation aimed at the prevention of digital crime, ensuring privacy and security of Electronic Health Records (EHR). The selected organization is a large healthcare organization with multiple hospitals running a single EHR and integrates a large number of independent physicians into this system providing multiple vectors for attack. Therefore it is imperative, with concerns for patient privacy and security, to enhance the security controls protecting sensitive data contained in the EHR. The C-suite of the organization will be used to set the strategic goals for blockchain implementation and experts will be elicited with blockchain technology expertise to ensure all necessary fundamental objectives are included. Once the framework is derived, weighted and measured, an analysis will be conducted on 3 separate blockchain solutions to determine which proposal will best meet the needs of the organization.

Conclusion

The research presented in this paper seeks to examine the relatively under-developed area of blockchain in the field of Health Informatics aimed at the prevention of digital crime. This investigation mixes qualitative and quantitative methods, which uses value-focused thinking and multi-attribute utility modeling. It revealed that an objective-based framework can be utilized to create the necessary model by which an organization, pressed with finite resources and heavy demands to provide privacy and security controls for sensitive patient data, can evaluate how to secure their EHR using blockchain technology. Therefore, this is a significant contribution as previous research in this falls short of being able to propose tangible methods by which the numerous proposed solutions and implementations of blockchain technology can be evaluated by organizations. Results clearly indicate that a feasible model can be built using decision analytic techniques like value-focused thinking to create useful models for organizations faced with this difficult task. This research will further extend the process and provide a multi-attribute utility model that incorporates the values of blockchain experts and strategic level decision makers in
order to provide a flexible model for the evaluation of proposed solutions at an organizational level that maximizes the solution's value-add.

REFERENCES


Keeney, R. L. 2013. Foundations for Group Decision Analysis. Decision Analysis, 10(2), 103-120.


