Phillip An
Grinnell College
ECN-378

Implementation of Blockchain Technology into Healthcare Information Systems

Introduction

Records of patient health contain information on patients' physical characteristics, as well as previous diagnoses and treatments. Secure and accurate storage of health information is critical for patients to receive the best possible care, but current systems of storage have introduced new problems for healthcare institutions and their patients. Today, Healthcare Information Technology (HIT) systems utilize Electronic Health Records (EHR), which house patient information on a computer-based storage. The rise of EHRs was catalyzed by advancements in medical technology (Haux, 2005) as paper-based storage systems could no longer keep up with the accompanying increase in data. In addition to the ability of storing significantly larger amounts of information, EHR implementations introduced multiple other benefits, such as decreases in documentation time (Poissant et al., 2005) and costs (Chaudhry et al., 2006), as well as providing data for clinical research (Haux, 2005). However, beyond the convenience of computer-based storage, the current system of EHRs can still be improved upon. The localization of information on EHRs have invited significant risks, where a single data breach may expose sensitive, confidential information. Additionally, it has been reported that over 50% of data breaches in healthcare information systems are due to internal factors, such as sending information to the wrong recipient (Jiang & Bai, 2018), highlighting the security risks of current EHRs. Furthermore, the current system limits patient agency over their information. According to the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, requesting and receiving your information can take up to 60 days, and institutions have the

option of denying you access to the information. Moreover, data stored on EHRs is fragmented, with different institutions housing different information on the same patient. This happens when patients relocate, or visit multiple institutions for varying treatments, since it is the patient's responsibility to update the institutions. To summarize, current EHRs are inefficient, imposing costs in both data security measures and patient agency, fragmenting patient information between institutions, and preventing patients from receiving the most accurate, effective treatment. Blockchain technology may be able to help.

The blockchain is a chain of blocks, each of which hold data, a unique identification called a "hash", as well as the hash of the previous block it is connected to. When new data is entered into the blockchain, it goes into a new block. A hash is calculated for that block, which then allows the new block to be added to the growing chain. Once the new block is added, data stored in the block is theoretically unchangeable (Yli-Huumo et al., 2016). This is because the hash is dependent on the data stored within the block, and even the tiniest of changes will necessitate the block to be re-hashed for the changes to be accepted. Furthermore, if changes are made to a block in the far past, all subsequent blocks become invalid as the hash of the tempered block is not recognizable anymore. In other words, subsequent blocks become unlinked from the blockchain. This means all subsequent blocks must be re-hashed for any changes to past data to be valid. Additionally, the blockchain exists as a distributed ledger, which means that each access point into the blockchain, called a "node", has a full copy of the data stored on the blockchain. The nodes are constantly in communication with each other, verifying and agreeing on the contents of the blockchain. Therefore, it is understood that you need at least 51% of the total computing power of all nodes in a blockchain to be able to manipulate the blockchain. Only then will a tempered block be accepted by other nodes. This phenomenon, called a "51% attack"

has been theorized to be impossible, due to the sheer amount of computing power necessary to execute it (Yli-Huumo et al., 2016). Thus, blockchain implementation into EHRs could provide increased security from data breaches. Furthermore, since the blockchain is programmable, patients who store their health information on the blockchain will obtain the ability to grant information access to institutions or individuals, significantly increasing patient agency. Additionally, storing patient health information on a single blockchain would allow inter-institutional sharing of data, directly increasing the potential of research, as well as creating holistic patient profiles which ensure that the most accurate diagnoses and treatments are being given to patients.

Similar to how EHRs replaced paper-based storage systems as a solution to a data-management problem, blockchain technology may replace EHRs as a solution to the issues of data security, fragmentation, and patient agency. Blockchain technology would also produce the benefits of increased research that translates into improved healthcare treatments. In this paper, it is argued that implementation of blockchain technology into current healthcare information systems will increase social efficiency. Through a modeling approach, it is shown that at the private level, institutions are not incentivized to implement the blockchain without government or third party subsidies into software development, and that only private institutions large and advanced enough to reap the benefits of research will be incentivized to implement blockchain technology. At the social level, it is shown that the socially efficient number of implementation is at least greater than one, and that there is a social demand for blockchain implementation. In the following sections, I will be reviewing the literature on EHRs and blockchain applications into healthcare, and subsequently introduce the model and its results.

Literature Review

Due to the novel nature of blockchain technology, literature is lacking on empirical studies that attempt to quantify the benefits of implementation. As a starting point, we will review the literature on current healthcare information systems and then proceed into discussing current applications of blockchain technology in healthcare.

Previous studies have examined the effects of Electronic Health Records (EHRs) and Health Information Technology (HIT) on the quality and efficiency of healthcare. Haux (2005) analyzes the developmental process of health information systems. This review article summarizes the published literature on the transition from a paper- to computer-based information storage and further predicts the consequences HIT systems will produce in the future. Haux (2005) describes that along with the advancement of medical technology, care providers began to collect more data than they could handle, which prompted the introduction of computer-based data storage. This implementation significantly increased the level of data processing as well as the possibility of applying patient information to other fields, such as clinical research. Whereas patient information prior to computer-based systems merely functioned as historical records, it could now contribute to the improvement of health care and treatments through research. Haux (2005) claims that such extended benefits of computer-based information systems explain their dominance in utility today, but acknowledges the existence of the remaining aspects of paper-based systems that may be continued for legal reasons. He describes that the coexistence of paper- and computer-based systems is redundant, and can produce higher costs and effort in maintaining organization and accessibility. In turn, Haux (2005) envisions a future in which care providers completely shift over to computer-based

systems, as well as regional and global HITs, through which healthcare may advance via global access to health services and medical knowledge.

However, even if the theoretical benefits of computer-based HITs have been accepted by care providers, analysis must be conducted on their quantitative impact. Poissant et al. (2005) reviewed articles listed in MEDLINE, CINAHL, HEALTHSTAR, and Current Health databases that discussed the efficiency of EHRs. The 23 studies qualified for review had documented quantitative time differences, with health professionals as their subjects. To compare results across different studies, 95% confidence intervals were constructed for time differences in paper or computer documentation, and variability in sample sizes were accounted for by calculating weighted averages. Poissant et al. (2005) concluded that there was a lack of consensus between studies with wide ranges of both increases and decreases in documentation time being reported. However, general trends indicated that nurses were more likely to benefit from a computer-based system (reported a 2.1% - 45.1% decrease in documentation time) than physicians (reported 8.2% - 238.4% increase in documentation time), potentially due to the difference in work processes. It was also noted that the increase in physicians' documentation time may be due to physicians taking advantage of the multifunctionality of EHRs.

As indicated by Poissant et al. (2005), the complexity of quantifying the quality and efficiency benefits of EHR implementation seems to be a significant limitation of these studies. Due to this limitation, Buntin et al. (2011) chose to categorize 154 articles that discuss the effects of HIT implementation by overall positive and negative outcomes. Articles that were overall positive associated HIT implementation with a pareto improvement in one or more aspects of care. Buntin et al. (2011) indicated that 96 (62%) articles were positive and 142 (92%) were positive or mixed-positive, where there were at least one negative aspect but the outcome was

positive overall. It was additionally noted that studies that measured the care provider's or staff satisfaction of EHR implementation were less likely to be a positive outcome, while studies that utilized statistical hypothesis testing were 2.1 times more likely to produce a positive outcome. This suggests that the sentiments of care providers may impede implementation of new technology, such as the EHR, that may be a net-benefit for healthcare.

The general positive outcome of EHR implementation indicated by Buntin et al. (2011) may provide some incentive for care providers to be welcoming of new technologies in healthcare data management, but a cost-benefit analysis is a more sure-fire way of convincing institutional stakeholders through financial incentives. In acknowledgement of the limitation of translating any realized benefits into monetary (quantitative) data, Chaudhry et al. (2006) conducted a systematic review of 257 articles on HIT implementation, focusing on its effects on quality, efficiency, and costs of health care. They conclude that HIT implementation resulted in an increased adherence to protocol-based care, as well as a 65% decrease in identification time and 14% increase in identification of hospital-acquired infections. Overall, HIT implementation increased care delivery by 12-20%, as well as a 12.7-25.4% decrease in cost, suggesting an increased efficiency in health care and treatments. Chaudhry et al. (2006) does note, however, that the total development and implementation costs could not be calculated with accuracy. Another important limitation of the study was identified as the prevalence of the outcomes of benchmark leaders— institutions that accounted for more than 5% of the 257 articles reviewed. Chaudhry et al. (2006) noticed that a disproportionate amount of benefits were realized by benchmark leaders who were comparatively more resourceful and experienced, having gradually prepared themselves to implement HIT systems. Thus, the results outlined by the study may not be generalizable to different implementation settings. In other words, even though the

implementations of HIT systems seem to increase the quality and efficiency of care, these results may not be replicable in other settings.

A significant difference between EHRs / HIT systems and blockchain technology is that whereas HIT systems are centralized to their respective institution's servers, blockchain technology installs nodes that connect to a decentralized server that is distributed across multiple nodes. Thus, implementing blockchain technology into HIT systems would effectively minimize the costs of back-end data processing as server maintenance is no longer an issue for all adopters. Additionally, the nature of the blockchain possesses characteristics that are desirable to HIT systems, such as accessibility, immutability, privacy, and interoperability, leading to the idea that blockchain implementation may overcome the shortcomings of and perhaps even replace current HIT systems, further improving healthcare for everyone.

Peterson et al. (2016) presents a blockchain-based approach to sharing patient data and discusses the advantages such a practice would entail. Peterson et al. (2016) argues that the patient should have full access of their data and that the benefits of sharing healthcare information in a data sharing network across institutional boundaries, such as the blockchain, will lead to increased data utility and healthcare. Although there are no quantitative evidences presented, the article introduces the theoretical benefits blockchain implementation would produce. These include patients having full stewardship of their data, greater amount of data accessible for utility (research, clinical trial information), decreased risk of cyber-attacks to a single centralized entity, and the elimination of data-driven competitive advantage between institutions that would encourage collaboration and ultimately lead to an improved quality of care. Additionally, sharing patient data across institutions also require homogeneity in data structure and formatting for interoperability, which current EHR and HIT systems cannot easily

adopt due to already existing practices. It is important to note that Peterson et al. (2016) does not fully account for a Proof of Work model, in which miners that verify blocks added on to the blockchain are somehow (mostly financially) compensated. Rather, an idealistic consensus model is proposed, where nodes are incentivized to provide proof of valid data (in terms of interoperability standards) in order to retain their status as a node in being connected to the blockchain.

As promising as blockchain implementation into HIT systems may seem to be according to Peterson et al. (2016), it is important to recognize the limitations of novel technology. Angraal et al. (2017) raises some concerns about implementing blockchain technology, stating that the sharing of private information on a public platform, no matter how encrypted, face potential risks of identification. Furthermore, implementation must comply with regulatory requirements, which require further costs to draft and execute. Finally, there is not enough data available to address whether blockchain implementation into HIT systems would be cost-effective in terms of hardware, implementation, support, and any other associated expenditures. Angraal et al. (2017) concludes by stating that the limitations enumerated above may serve as barriers of implementation and that although promising, blockchain technology may not live up to its expectations in healthcare.

Then, in order to minimize the limitations mentioned by Angraal et al. (2017), perhaps current applications of blockchain technology as HIT systems can be analyzed and reviewed for potential advantages and disadvantages. Ekblaw et al. (2016) introduces MedRec, "a prototype for electronic health records and medical research data" that exists on the blockchain. Ekblaw et al. (2016) recognizes the fragmented structure of current EHRs, where institutions fail to possess complete health records unless updates are requested by the patient themselves. This lack of

cohesive data presents a societal cost in which data utility is greatly reduced and the opportunity for potential advancements in healthcare research and treatments are missed. With MedRec, patients are able to upload and update their information on the blockchain, as well as retain complete agency over their information across institutional boundaries. Additionally, with the use of "smart contracts", programmable code that runs on the blockchain, patients would be able to grant other parties access to their information upon appropriate verification. And since the decentralized nature of the blockchain eliminates a central target for cyber-attacks, the risk of data leaks are minimized. Furthermore, as the amount of data increases, data processing and analysis techniques could be used to identify certain patterns of health characteristics that inform both care providers and patients of patient conditions. Ekblaw et al. (2016) also mentions the integration of information from other facets of health data, such as information collected by wearables (Fitbit, Apple Watch) and other sources (23andMe). Thus, a holistic profile of the patient can be created and maintained on the blockchain. In contrast to Peterson et al. (2016) which suggests an ideal consensus model, Ekblaw et al. (2016) recognizes the financial incentives that must exist for the blockchain to continue its operations. A data reward for mining is suggested, where miners are able to receive a "bounty query" for verifying a block. A "bounty query" is described as aggregated, anonymized medical data that could be used in data analysis. In terms of feasibility, Ekblaw et al. (2016) states that implementation of MedRec is designed to occur on top of EHRs, promising a smooth transition. Currently, MedRec is being tested at the Beth Israel Deaconess Medical Center at Harvard Medical School to obtain data on the costs and benefits of implementation. Their findings will serve as a starting point for blockchain implementation into HIT systems and perhaps incentivize other institutions to adopt the technology as well.

With a growing interest in blockchain technology implementation into the field of healthcare information management, it is crucial to address whether such adaptions would be cost-effective. Similar to the rise of EHRs and their climb over paper-based information systems, blockchain technology is expected to soon replace current EHRs with promises of complete patient agency over healthcare information, improved data utility, and interoperability. Previous studies, to the best of my knowledge, have not attempted to model the cost-benefit analysis of blockchain implementation into healthcare information systems. In doing so, this paper will hopefully provide financial insight into blockchain technology and introduce a greater incentive to potential implementors than speculative benefits. Below, I present a theoretical model which analyzes the efficiency behind blockchain technology implementation into HIT systems.

The Model

As research into blockchain technology begins to identify potential applications (Zhao et al., 2016; Zibin et al., 2018), cases of implementation have begun to rise. The health care industry is one of such potential implementation fields, where blockchain technology may increase the cost efficiency of data organization and management compared to current infrastructure that manage patient records, such as Electronic Health Record (EHR) and Health Information Technology (HIT) systems. This paper utilizes a simple model to examine whether such an implementation would be beneficial, and attempts to identify the specific conditions that would incentivize patient-record keeping institutions to adopt blockchain technology.

In order to simplify the model, it is assumed that benefits are in the form of utility that are converted into quantifiable, financial measures. It is also assumed that institutions are equal in size, which implies that the number of intra-institution implementations and the resulting costs

are equal across institutions at the private level. Further assumptions will be described when necessary.

The model begins by defining the constituents of costs and benefits at the private level. Private cost (C_P) is a sum of the cost of maintenance (C_M), transferring existing records on to the blockchain (C_T), designing software (C_D), and implementation (C_I).

$$\boldsymbol{Eq.1} \quad C_P = C_M + C_T + C_I + C_D$$

At the private level, it is assumed that $C_D \gg (C_M + C_T + C_I)$ due to the novelty of blockchain technology and the expertise necessary for software design as well as data architecture. Thus as the private level, cost is dictated by C_D.

$$\boldsymbol{Eq.2} \quad C_P \approx C_D$$

Since it is assumed that the costs of implementation are equal across institutions, social cost (C_S) is assumed to increase linearly with the number of institutions that undergo implementation (X), described by:

$$\boldsymbol{Eq.3} \quad C_S = X * C_P$$

However, at the social level, it is assumed that the first institution to implement the software has paid for the cost of software design, and so $C_D \approx 0$ at the social level. Therefore, social cost is the sum of maintenance, transfer, and implementation costs multiplied by the number of institutions.

$$\boldsymbol{Eq.4} \quad C_S = X * (C_M + C_T + C_I)$$

As for the benefits of blockchain implementation, private benefit (B_P) can be described as the benefits of security, research, and reduced misdiagnosis:

$$\boldsymbol{Eq.5} \quad B_P = (1 - \beta_P) * B_{sec} + \gamma * \delta * (B_{res}) - (1 - \alpha) * C_{mis}$$

Where (β_P) is the probability of a security breach at the private level, and (B_{sec}) is the benefit of the immutability of records. The benefits of research (B_{res}) is multiplied by the probability of research being successful (γ) and the proportion of access into other institutions' data (δ). At the private level, it is assumed that $(\delta) < 1$. (C_{mis}) is the cost of misdiagnosing patients and is multiplied by $(1 - \alpha)$, (α) being the proportion of how whole and complete patient records are. α is a function of δ, $\alpha(\delta)$, where $\frac{d\alpha}{d\delta} > 0$, since the greater number of institutional data available, the more complete patient records will be.

At the social level, social benefit (B_S) is also a linear function of the number of implementations (X), but is also described by the utility patients receive from the increased agency over their records (B_A). As (X) increases, (B_A)'s contribution to social benefit also increases due to the increased number of institutions patients can transfer, retrieve, and grant permission to their data. Thus, (B_A) describes both the patient's agency over their data as well as the convenience they receive by storing their data on the blockchain.

$$\boldsymbol{Eq.6} \quad B_S = X * [B_P + B_A(N)]$$

In this equation, (N) is the number of people with health records in a given society, and it is assumed that each individual gets the same amount of utility over having greater agency over their records. Writing out the full equation of social benefit, we get:

$$\boldsymbol{Eq.7} \quad B_S = X * [(1 - \beta_S) * B_{sec} + \gamma * \delta * (B_{res}) - (1 - \alpha) * C_{mis} + B_A(N)]$$

Since greater access to a larger number of institutions' data will be granted at the social level, it will be assumed that $(\delta) = 1$. The probability of a security breach at the social level is less than that at the private level, $\beta_S < \beta_P$, due to an increased connectivity of a greater amount of data requiring a significantly greater amount of energy and effort to conduct a 51% attack that can violate the immutability of the blockchain (Yli-Huumo et al., 2016). It will also be assumed that

α is greater at the social level (α_S) than the private level (α_P) as patient data becomes more holistic with greater number of implementations across distinct institutions.

Following the conventional logic behind economic incentives, we expect private institutions to only undergo implementation of blockchain technology if the derived benefits outweigh the costs. At the private level, the following condition must be satisfied $C_P < B_P$:

$$\boldsymbol{Eq.8} \quad C_D < (1-\beta_P) * B_{sec} + \gamma * \delta * (B_{res}) - (1-\alpha) * C_{mis}$$

To satisfy the condition, and for the right side of the expression to be a positive number, we see that $(1-\beta_P) * B_{sec} + \gamma * \delta * (B_{res}) > (1-\alpha) * C_{mis}$. In other words, the benefits derived from the increased security and research must be greater than the total costs of misdiagnosis. Additionally, let us assume that $(1-\beta_P) * B_{sec} << \gamma * \delta * (B_{res})$. This is driven by the notion that institutions that house patient records, such as hospitals, derive greater benefit from research than from having a secure database. This is supported by the fact that successful research can be translated into treatment procedures that profit the institution, while increased security measures simply exist to prevent data breaches. These assumptions show that private benefit (B_P) is mostly driven by the benefits of research. Thus, the conditions for private implementation becomes:

$$\boldsymbol{Eq.9} \quad C_D + (1-\alpha) * C_{mis} < \gamma * \delta * (B_{res})$$

Rearranging the expression shows that the expected benefit of research, $\gamma * \delta * (B_{res})$, requires a minimum of $B_{res} > \frac{C_D}{\gamma * \delta}$, when $(C_{mis} = 0)$. As both γ and δ are parameters with values between 0 and 1, this expression indicates that institutions that may not be large or advanced enough to reap significant benefits of research would not be financially incentivized to implement blockchain technology at the private level.

At the social level, the socially efficient number of implementation can be found by the point at which marginal benefit equals marginal cost. A derivation of social cost (C_S) and social

benefit (B_S) with respect to the number of implementations (X) give the following equations of marginal cost (MC_S) and marginal benefit (MB_S).

$$\boldsymbol{Eq.10} \quad MC_S = \frac{dC_S}{dX} = C_M + C_T + C_I$$

$$\boldsymbol{Eq.11} \quad MB_S = \frac{dB_S}{dX} = (1-\beta) * B_{sec} + \gamma * \delta * (B_{res}) - (1-\alpha) * C_{mis} + B_A(N)$$

Setting the marginal cost equal to marginal benefit and rearranging the terms by separating costs and benefit variables, we get:

$$\boldsymbol{Eq.12} \quad C_M + C_T + C_I + (1-\alpha) * C_{mis} = (1-\beta) * B_{sec} + \gamma * \delta * (B_{res}) + B_A(N)$$

At the private level, it was established that $C_D \gg (C_M + C_T + C_I)$ and private institutions would only be incentivized to implement blockchain technology if the benefits derived from research is greater than the sum of the cost of software design and misdiagnosis (Eq. 9). Therefore, substituting C_D for $(C_M + C_T + C_I)$ would show:

$$\boldsymbol{Eq.12} \quad C_D + (1-\alpha) * C_{mis} > (1-\beta) * B_{sec} + \gamma * \delta * (B_{res}) + B_A(N)$$

However, keep in mind that the completeness of patient data (α) is greater, the probability of security breach at the social level (β_S) is less, and the proportion of access to other institutions' data $\delta = 1$ at the social level. Additionally, with the summation of benefits including the benefits of patient agency $B_A(N)$, these changes in the parameters of social benefit (B_S) may be enough to offset the difference between marginal cost (MC_S) and marginal benefit (MB_S). Thus, a new expression is derived:

$$\boldsymbol{Eq.13} \quad C_D + (1-\alpha) * C_{mis} \leq (1-\beta) * B_{sec} + \gamma * \delta * (B_{res}) + B_A(N)$$

Eq. 13 indicates that the increased access of interinstitutional data and patient agency as well as the decreased possibility of security breach, at the social level, satisfies the conditions of implementation at the private level (Eq. 9), suggesting that the socially efficient number of

implementation is at least greater than the number of implementations that will take place at the private level. In other words, the socially efficient number of implementations is greater than one. Accordingly, considering the cost-benefit analysis of a private institution under the assumption that the software has been built ($C_D = 0$), it can be seen that the benefits are more likely to outweigh the costs (Eq. 9), and institutions would be more incentivized to implement blockchain technology.

The model shows that at the private level, only large institutions that can derive enough benefits of research (B_{res}) to outweigh at least the cost of software design (C_D) would be incentivized to implement the blockchain (Eq. 9). This suggests that implementation at the private level may be sub-optimum without government subsidy or other 3rd party investments that can significantly lower (C_D). These results indicate a first mover disadvantage into blockchain implementation as the sole bearer of the costs of software design. At the social level, however, the model shows that the socially efficient level of implementation is at least greater than one (Eq. 13). Thus, to meet the social demand for blockchain implementation, governments should subsidize the cost of software development.

Sensitivity to Assumptions

At the private level it was assumed that the cost of software design (C_D) outweighs other costs of implementation due to blockchain being a novel technology. It may as well be that due to this novelty, other costs such as maintenance (C_M), data transfer (C_T), and implementation (C_I) are much more significant than expected, which would worsen the disparity between private cost and benefit and further disincentivize even large institutions from implementing blockchain technology. If the listed costs are indeed considerable in size, the socially ideal condition (Eq.

12) would also be affected and the changes in parameters at the social level (Eq. 13) may not be enough to set the ideal number of implementations greater than 1. The changes in parameters at the social level are also theoretical in nature, and may not induce the outcome shown in Eq. 13. For the outcome to remain unchanged under the condition that social parameters do not satisfy Eq. 13, a greater amount of government subsidy is needed for blockchain implementation to occur.

Additionally, at the private level it was assumed that the benefit of research (B_{res}) is much greater than the benefit of data security (B_{sec}), which may not hold true for all institutions that hold patient records, such as insurance companies that may not conduct scientific research at all ($B_{res} = 0$). For such scenarios private benefit would be mostly determined by B_{sec}:

$$\boldsymbol{Eq.14} \quad C_D + (1-\alpha) * C_{mis} < (1-\beta_P) * B_{sec}$$

This suggests that private institutions that do not conduct research would only be incentivized to implement blockchain technology if the derived benefit in security is greater than the cost. For such institutions, a greater government subsidy will be necessary to hold Eq. 14 true, as it is assumed that the benefits of increased research greatly outweighs the benefits of increased security, in general. As granting a larger subsidy to a non-research institution is riskier, especially since non-research institutions are unlikely to be as advanced as research institutions, it would be recommended for the government to grant subsidies to research institutions as the first site of implementation. Such a policy would meet the social demand of implementation with minimal cost.

Finally, as the model takes place when blockchain technology is still relatively new and costly to implement, it was assumed that costs are mostly driven by the technological factors. As blockchain technology becomes normalized into society and the costs of development drops,

costs may be significantly determined by the costs of misdiagnosis (C_{mis}) in the cost-benefit analysis. Such circumstances would increase the likelihood of benefits outweighing costs at the private level (Eq. 9). If this assumption holds true, private institutions may be incentivized to implement the blockchain without subsidization, and government subsidies should not be allocated as they would only incur costs and lower social efficiency.

Alternative specifications or applications of the model

The model assumes that social cost and benefit are linearly dependent on private cost and benefit, respectively. Therefore, taking the derivative functions of marginal social cost and benefit eliminates the number of implementations (X) as a variable, preventing the model from specifying the social ideal number of implementations. Thus, in order to include the number of implementations (X) in the marginal cost or benefit functions, at least one variable must also be a function of 'X'. Due to the nature of the 51% attack, a case could be made for the benefits of increased security being a function of the number of implementations. As the number of implementations increases, it would be more difficult to execute the attack (Yli-Huumo et al., 2016). Additionally, the benefits of increased research could also be a function of 'X', as more patient information would be entered into the blockchain. Altering these variables to be a function of 'X', indicated by B_{sec2} and B_{res2}, may simulate the cost-benefit analysis of blockchain implementation for institutions under a new assumption: the first implementation has already occurred. Thus, even at the private level, the private benefit function alters:

$$\boldsymbol{Eq.15} \quad B_P = (1-\beta_P) * B_{sec2}(X) + \gamma * \delta * [B_{res2}(X)] - (1-\alpha) * C_{mis}$$

This new expression of private benefit captures the nature of the blockchain, in which the received benefits increase when more institutional implementations have already taken place.

Through this logic, it can be argued that the benefits of increased security and research are greater for the second institution, and even greater for the third institution that undergoes blockchain implementation. Thus, under the private level cost-benefit analysis shown in Eq. 9, institutions are more likely to be incentivized to undergo implementation when they are not the first to do so. This result agrees with our previous finding of a first mover disadvantage in implementation.

At the social level, adjustments to the changes described above produce a different expression in the marginal cost-benefit analysis:

$$\boldsymbol{Eq.16}\quad MC_S = C_M + C_T + C_I + (1-\alpha) * C_{mis} = (1-\beta) * B_{sec2}(X) + \gamma * \delta * [B_{res2}(X)] + B_A(N) = MB_S$$

Once the function for security and research benefits can be defined in terms of 'X', the socially ideal number of implementations can be determined. If we assume that the functions are linearly dependent on 'X', where $B_{sec2}(X) = B_{sec} * X$ and $B_{res2}(X) = B_{res} * X$, and B_{sec} and B_{res} are the respective average benefits derived by private institutions that join the blockchain, we see that the socially ideal number of implementations becomes:

$$\boldsymbol{Eq.17}\quad X = \frac{C_M + C_T + C_I + (1-\alpha) * C_{mis} - B_A(N)}{[(1-\beta) * B_{sec} + \gamma * \delta * B_{res}]}$$

As indicated, this result is subjected to change according to how the functions of security and research benefits are defined with regards to the number of implementations. However, although Eq. 17 was formulated through an extremely simple assumption, it shows that the model itself is adaptable and able to specify the socially ideal number of implementations.

Conclusion

As blockchain technology rises in popularity, numerous potential applications have been theorized. The nature of the blockchain has been proposed to improve security and functionality of computer-based data storages, and to introduce such benefits to healthcare information systems (Ekblaw et al., 2016). This paper utilizes a modeling approach to assess whether implementation of blockchain technology into current healthcare information systems would increase social efficiency. Results show that there is a social demand for blockchain implementation, but institutions may not be financially incentivized at the private level, as they are subjected to a first-mover-disadvantage. It is also shown that only large and advanced research institutions will be incentivized to undergo implementation. However, after the first implementation, subsequent institutions will face a lower barrier to implementation due to decreases in costs as well as increases in benefits. These results support the hypothesis that blockchain implementation increases social efficiency, but some policy changes may need to occur for such social demand to be met. To lower the barrier to private implementation, we recommend governments to grant subsidies into blockchain software development, specifically for research-centered institutions. As for extensions of the study, future works should focus on accurately defining the relationship between private and social cost and benefit, as well as the relationship between the number of implementations and the security and research benefits derived from implementation.

References

Angraal, S., Krumholz, H.M., Schulz, W.L. (2017). Blockchain technology: applications in health care. *Circulation: Cardiovascular Quality and Outcomes*. doi: 10.1161/CIRCOUTCOMES.117.003800. [Online]. Available:https://www.ahajournals.org/doi/full/10.1161/CIRCOUTCOMES.117.003800?url_ver=Z39.88-2003&rfr_id=ori:rid:crossref.org&rfr_dat=cr_pub%3dpubmed

Chaudhry, B., Wang, J., Wu, S., Maglione, M., Mojica, W., Roth, E., Morton, S.C., Shekelle, P.G. (2006). *Annals of Internal Medicine*, *144(10)*, 742-752.

Ekblaw, A., Azaria, A., Halamka, J.D., Lippman, A. (2016). A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. *MIT Media Lab*, *Beth Israel Deaconess Medical Cetner*. [Online]. Available: https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf

Haux, R. (2005). Health information systems – past, present, future. *International Journal of Medical Informatics*, *75(3-4)*, 268-281.

Jiang, J., Bai, G. (2018). Evaluation of causes of protected health information breaches. *JAMA Internal Medicine*. [Online]. Available: https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/2715158

Peterson, K., Deeduvanu, R., Kanjamala, P., and Boles, K. (2016). A Blockchain-Based Approach to Health Information Exchange Networks. [Online]. Available: https://www.healthit.gov/sites/default/ files/12-55-blockchain-based-approach-final.pdf

Poissant, L., Pereira, J., Tamblyn, R., Kawasumi, Y. (2005). The impact of electronic health records on time efficiency of physicians and nurses: a systematic review. *Journal of the American Medical Informatics Association*, *12(5)*, 505-516.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLOS ONE 11(10)*: e0163477.https://doi.org/10.1371/journal.pone.0163477

Zhao, J.L., Fan, S.K., Yan, J.Q. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, *2:28.* https://doi.org/10.1186/s40854-016-0049-2

Zibin, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2018). Blockchain challenges and opportunities: a survey. *Int. J. Web and Grid Services*, *14(4)*, 352-375.