Information Security and Knowledge Sharing: A Blockchain Perspective

Kai-Ping Huang
Department of Business Administration, Fu Jen Catholic University, Taiwan, R.O.C

Correspondence Author: Kai-Ping Huang, Department of Business Administration, Fu Jen Catholic University, Taiwan, R.O.C
E-mail: 129741@mail.fju.edu.tw

Received date: 22 August 2020, Accepted date: 25 September 2020

Copyright: © 2020 Kai-Ping Huang. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

INTRODUCTION

Blockchain can be denoted as a new-age technology. Its principal function is to revolutionize the process of executing, controlling, monitoring, recording and managing financial transactions with maximum security, accountability and transparency. Blockchain has also been represented as the foundational technology supporting the establishment of bitcoin platforms [1]. It is further appreciated for being a suitable mechanism to efficiently organize and gather data in the most cost and time-effective manner, besides substantially reducing complexities involved in the transactions [2]. Nonetheless, even though the invention has improved at a rapid pace since it was first introduced, blockchain technology is still perceived as an emerging technology. Identifiably, a large and versatile number of global organizations have depicted their interests to invest significantly in the development processes to enhance blockchain-based applications as suitable to their long-run interests [3]. Correspondingly, as a distributed database, blockchain is expected to maintain an expanding list of records, which are technically referred to as ‘blocks’. These blocks are further designed in a manner to ensure security from possible tampering and alteration efforts. It is thus that each of the blocks designed in the chain is framed with a timestamp while being linked with the hash to the block developed before to create the chain [2].

According to many technology experts, blockchains are effective in reducing the risks of a data breach and by doing so, it contributes to data security. Notably, as the blockchain technology has been improving continuously with inclusions from various experts, the currently used blockchain is much different from its traditional version. Today, the blockchain contains a series of shared copies based on a similar pattern of the database, making it even more challenging to hamper or impede data security through a breach or a cyber-attack [4]. Along with various other techniques used in the blockchains today, the current version of the technology is certainly better in its fraud resistant...
features, further holding the potentials to transform the modern, digitally dependent, business sectors by making the processes smarter, more secured than earlier, and increasingly transparent [5].

Uses of blockchain have been recently gaining much criticism on the grounds of scalability, security, and sustainability at large [6-7]. However, even though the scholarly interests for the technology practice has increased substantially in the recent years, a comprehensive analysis regarding data security offered through blockchain applications has been severely lacking a systematic elaboration. The objectives of this study is, therefore focused on assessing the current level of security that blockchains can offer against a faulty system and data perspective for both public and private ledgers. In the explanation, thus, the CIA security triad model will be taken into consideration, which comprises Confidentiality, Integrity and Availability as the three key areas to assess the current maturity level of blockchain technology. Correspondingly, Authentication, Authorization and Audit (AAA), and Non-Repudiation related fundamental security aspects commonly associated with the blockchain technology will also be addressed as a measure to protect information as well as design/manage new systems for long-run efficiency.

LITERATURE REVIEW AND PROPOSITION DEVELOPMENT

Blockchain and Trusting Records

According to Yoo [8], blockchain can be defined as a ‘distributed ledger technique’, which allows its participating members to share information based on the transactions among each other in a more hustle free and convenient manner. Explaining further, Yoo [8] affirmed that a blockchain principally acts as a distributed database with a continuously expanding series of data records, which in turn tends to prevent the possibilities of alteration or tampering even by the operators. Similarly, Swan [2] had defined blockchain as a technology designed to maintain the public ledger for all the transactions using bitcoins. Being public by nature, the blockchain technique is growing at an incessant rate, as data miners have been contributing with the creation of new blocks at a frequency of one in every 10 minutes to record information about the most recent bitcoin transactions [2;7]. As the new blocks keep on adding to the linear and chronological blockchain, each full node gains access to a copy from the blockchain. It is then downloaded automatically as new miner contributes to the Bitcoin network, where on the other hand, the blockchain developed automatically stored information related to the addresses and the balances from even the initial blocks built [2].

Further elaborating on the definition of blockchain technology, Rennock et al. [10] asserted that there are two types of blockchain networks, which are private and public blockchains. On one hand, the private blockchain networks refer to proprietary networks, which are used by particular authenticated individuals to conduct the intended financial transactions. On the other hand, public blockchains act as similar to open source networks, which are accessible to everyone without the need to obtain any specific authentication, such as observed in the case of bitcoin users [10]. From a different perspective however, Brünnler et al. [11] described blockchain in purview of its association with the concept of bitcoin. According to Brünnler et al. [11], bitcoin can be denoted as a crypto-currency, fundamentally because of its use of peer-to-peer technology that in turn supports a direct transaction between the users, and therefore, does not need an intermediary (for example, banks and credit card companies) for the conduct. Brünnler et al. [11] further noted that this form of transactions may be subjected to double spending, which is frequently observed in systems those lack central control, but as bitcoin transactions are built to maintain a detailed and public record for the transactions, such a threat can be easily prevented through the blockchain technology.

Sultan et al. [12] were further of the view that a blockchain gains its secure and unchallengeable nature through the amalgamation of two key innovations. This include a cryptographic link connecting records of bitcoin transactions, making it increasingly challenging for the miners to make any deliberate change to the process or make alterations to the already recorded information. With due consideration to all these unique elements in the technology, Oh and Shong [13] offered a more inclusive list of elements to define blockchains as applicable in the current phenomenon. As affirmed by Oh and Shong [13], “blockchain is a technology to secure integrity and reliability of transaction records without trusted 3rd service provider, by having all the participants in the network create, record, store and verify transaction information jointly, and has the structure to realize various application services based on distributed network infrastructure using security technologies including Hash, Digital Signature and Cryptography”. Elaborating further on this statement, Bahga and Madisetti [14] argued that the fundamental motive to design the blockchain technology was to increase the security when dealing in bitcoins by issuing, circulating and managing the transactions of these digital currencies.
Preservation of Trustworthy Digital Records Using Blockchain Technology

As was specifically indicated by Atzori [15], blockchain has evolved as a core technology for bitcoin transactions, with a variety of applications, which were intended to transform the way interactions are recorded in business, politics and societal spheres. Sharing a similar perspective, Swan [2] asserted that blockchain principally was developed to act as a distributed database system, competent of recording and preserving transactional information. More comprehensively thus, Swan [2] explained blockchain as a data structure equipped with an advanced information technology design to record data in the form of blocks, intertwined as a series or a chain. Blockchain, therefore, acts as a fundamental technology to be able to support the execution of bitcoin transactions in the most reliable manner in different industries. Illustratively, Tian [16] recommends the use of blockchain technology in the process of managing data for the ‘agri-food supply chain traceability system’, which is principally based on the Radio-frequency identification (RFID) technology to monitor agricultural products accurately. Using the blockchain technology in this regard, according to Tian [16], will be not only reliable but also beneficial for the management, to successfully reduce the chances of fraudulence, tampering, corruption, and information falsification.

Supporting this claim, Iansiti and Lakhani [17] further argued that blockchain is beneficial to make the data management process more “secure, irreversible, distributed, transparent, and accurate” than the previous technologies used for bitcoin transactions. In doing so, the blockchain technology constructs a series of data structures referred to as the ‘blocks’, while also encrypting the information for safe mining and execution of bitcoin transactions [18]. This prevents the transmitters from making any alteration to the data, once it has been encrypted into blocks and have been constructed into blockchains and therefore, making the entire blockchain a tamper-proof procedure [19]. Drescher [20] further affirmed that these data blocks are designed through nodes using the preservation function. Drescher [20] also argued that because of the lack of a centralized management system to guide the applications for bitcoin transactions, the rights, as well as the obligations created through blockchain technology by default for any node, are denoted as equal. This form of data management can be expressed as suitable for data storing, especially when the information needs to be identified and verified to accomplish the desired usability objectives, besides enabling the respondents with the establishment of a decentralized consensus by sequentially structuring the events as well as the current transaction status [20].

The blockchain technology has therefore been widely recognized for its benefits for being a decentralized system of data management, which in itself has been a revolutionary idea to make information widespread from the very moment of its recordkeeping and by doing so, preventing possible breaches [19]. Stating precisely, Tian [16] asserted this fundamental feature based on which the blockchain technology was created that has allowed the users to autonomously exchange transactional data and maintain information security [16]. Furthermore, as was noted by Kosba et al. [21], execution of the cryptographic protocols within blockchain technology has certainly enriched trade-offs for the systems’ transparency, confidentiality, verifiability, and enforceability as a part of smart contracts. It is this particular feature, which differentiated between conventional and unconventional blockchain technologies that demand every node involved in the network to be able to process each transaction being added to the blockchain, making it a scaled and time efficiency process, without compromising with security in any form [22]. Therefore, Proposition 1: Blockchain technology is positively related to the preservation of trustworthy digital records.

Blockchain and Information Security

According to the findings obtained by Zyskind et al. [23], various attempts have been made to assess and amend privacy issues involved with the blockchain technology, from a legislative standpoint, and simultaneously from a technological standpoint. To argue further and rationalize the claim, Zyskind et al. [23] illustrated the competencies of the recently introduced Open Public Distribution System (PDS) framework, which is a modular representation for the independent deployment of a PDS. This mechanism functions on the formula to return data computations and therefore, offering answers rather than providing raw data to the analysts [10]. In the industrial context, major corporate entities have preferred the implementation of customized proprietary authentication software to suffice their organizational needs by making use of the OAuth protocol [24]. In addition to offering the benefits of customization to the organizational users, the blockchain technology also allows data anonymization that in turn offers security to personally identifiable information [23].

The technology designed for blockchain is principally aimed at enhancing its immutability from data breaches, while keeping the data recording process tamper-proof as well as democratic in nature [25]. In doing so, the three principal characteristics of blockchain technology can be duly considered, which are (1) Decentralization, (2) Cryptography,
and (3) Consensus [21; 26-27]. These characteristics indicate the degree of complex interplay correlating them, which adds to information security when recorded using the blockchain technology, while simultaneously reducing risks of any form of foul play [26]. Traditionally, ownership was deemed as one of the fundamental and most crucial aspects to store, process and subsequently effectively share information. Ownership in this regard is substantially dependent on the stages of creating, borrowing or transmitting the information through a permission process (if considered to be necessary), and subsequently, ensuring that the data is available on the open PDS network, which makes the changes public [2]. Fundamentally, this entitles the public in the role of a watchdog, where any change or addition made to the information recorded in the blockchain becomes immediately public. Therefore, any future discrepancy to the information becomes easily traceable and therefore, undermining the covert needs for any foul play in the system [22]. In other words, as the blockchain technology is based on the idea of decentralization, it requires changes in all the previously recorded blocks of information in order to make one specific chain in one specific block and thereby, conduct any fraudulency undetected. Not doing so can otherwise lead to easy identification of the breach [23].

A core principle of the blockchain technology is to maintain the highest standards of security in its information management process. In correspondence to this principle, a key objective of the technology has been to empower virtual transactions in a tamper-proof manner [28]. The rapid increase in the use of blockchain technology can be linked to its characteristics and the subsequent ability to ensure data security and transparency by monitoring and identifying an independent source of truth and agreement between the parties engaged into a transaction [28]. The percentage of blockchain applications has certainly been substantial among banking institutions and financial service providers, considering the benefits it offered against data security breaches through self-executing smart contracts, better fraud detection capacity, digital currencies, real-estate records, processing of the automated claim, data privacy, inventory management as well as product source tracking [28]. Throughout these verticals, the fundamental use of blockchain technology has been to enrich an environment of trust by offering better security for the information being shared amid partners and strategic decision-makers [28].

A vital advantage of blockchain in assuring information security at the greatest extent is that it maintains non-conditional adherence to increased levels of data protection and immutability when compared to the traditional technology-based alternatives available for the users [29]. As noted by Böhme et al. [29], data stored through the blockchain technology is distributed by computing networks containing multiple nodes and blocks that make it too difficult to tamper with the information being shared. Not only from hackers or fraudulent conducts, the technology also assures safety from possible technical glitches, which were common in the traditional information storing systems based on a single point network. In case the computer containing all the information failed, the data were supposedly lost owing to the lack of back-ups [30]. This particular feature in the blockchain technology thus allows more efficient and transparent transactions to take place in a time as well as cost-effective manner, besides allowing an organized framework for verification and discussions among the intermediary institutions. Arguably, bitcoin transactions are noted to take place in the blockchains, constantly being verified throughout the distributed network, which assures the interrelated parties regarding data security [29].

Illustratively, in the process of settling a sale of the securities, data stored in the blockchain can prove beneficial to make the entire decision-making procedure more time and cost-efficient by assuring that the data was stored and verified by a legally authenticated seller with the permission or in a permissionless manner for transfer [31]. In the process, therefore, the data recording and managing intermediaries can be referred to as guarantors for information reliability, which offers another perspective to the information security issues addressed through the revolutionizing technology [32]. It was thus affirmed by Kim and Just [21] that blockchain technology allows substantial reductions to the time and costs required for the data verification processes, as compared to the traditional mechanisms. This in turn, also increases the scope to conduct verifications in multiple phases, further assuring the authenticity of the data shared and the transactions conducted based on the information. Therefore.

Proposition 2: Blockchain technology is positively related to information security.

Blockchain and Inter-Firms’ Knowledge Sharing

In the modern world, inter-organizational networks have been well-established even though the concept lacks a comprehensive and self-explanatory definition in the various fields where the practices conducted. Under such circumstances, the application of this sharing process has been based on a common understanding that inter-organizational networks are built on the virtues of social interactions, relationships, collaboration, connectedness, collective action, trustworthiness, as well as cooperation [33]. The network also mandates organizations or parties to
develop a strategic alliance among them prior to sharing the knowledge, especially those regarded with a high degree of confidentiality and categorized as sensitive [34]. The nature of the information or the knowledge being shared among the parties also has a crucial role to play in the network, owing to the influences of ambiguity, tacitness, and/or complexity [35]. Arguably further, the degree of ambiguity found inherent to knowledge can be directly and negatively related to the transfer process.

Arguing further in this context, Wang et al. [36] denoted that trust or transparency acts at the fundamental levels of inter-organizational networks, which raises collaboration and cooperation among the involved parties. The establishment of the blockchain technology has been revolutionary in this regard, as it contributed to the development of safer and more secured environments [37]. It has certainly forced reconsideration to the conventional inter-organizational ties based on governance transparency and reliability at large. It is thus that blockchain systems have often been considered to facilitate inter-organizational networks through effective reduction or possible elimination of dependency over control agents in situations with high risks of data breach [37]. This further redefines and establishes a more trusted relationship as compared to those of the past. As was noted by Seebacher and Schüritz [38], even if the blockchain technology is regarded as beneficial in adding value to the inter-organizational service systems with its features of immutability, integrity and transparency, the mechanism can be subjected to limitations, especially in the form of its high degree of complexities. This implies that the blockchain technology must be periodically scrutinized and enhanced for better efficiency to allow trustworthy knowledge transfer through the inter-organizational networks [39].

Knowledge Sharing within Firms through Blockchain

According to Beck et al. [37], the incentive system inherent to the blockchain economy (often referred to the economic system based on the blockchain technology) functions in three levels, which comprise (i) “digital processes in peer-to-peer exchanges for value creation of blockchain-based digital goods”, (ii) “incentives to create private goods, club goods, and public goods”, and (iv) “new network-based processes that incentivize the peer-to-peer nodes to reach consensus”. When emphasizing the role of blockchains in the knowledge sharing process using the inter-organizational networks, Xu et al. [40] asserted that inter-organizational systems, which have been based on permissioned blockchain, may perhaps be more virtuous as compared to a permissionless alternative. The authors have also been of the view that rather than recording entire data sets on the blockchains, a proportion of data should be recorded off-chain to gain privacy. Therefore, incentives of using blockchains can be identified in terms of reputation, security deposits and/or rating mechanisms. Okada et al. [41] have accordingly distinguished the blockchain systems for knowledge sharing purposes into two categories, which are market-based blockchain technology incentives and non-market-based incentives. While market-based incentives of using blockchains to share information through the engaged and interested parties are closely intertwined to crypto-currencies, often denoted in terms of bitcoins, the non-market based blockchain systems can be denoted as more strategic and rhetoric in nature [39]. Elaborating further, Okada et al. [41] denoted ‘consortium blockchain systems’ as an example of non-market-based incentives, which does not need specific participants to be engaged into the process of data mining or retrieval.

Illustratively, in accounting, blockchains are believed to hold the competencies and potentials to improve the overall quality of the information being shared, either by enhancing the degree of trustworthiness or by increasing the time and cost efficiency of the entire knowledge sharing process [42]. Similarly, the reliability coherent to the application of blockchain technology to share information in a transparent manner is also believed to facilitate better information sharing throughout the inter-organizational network, such as supply chains, by addressing automated governance necessities [43]. From a distinguished perspective further, Tian [16] asserted that using blockchains for knowledge sharing purposes in the inter-firm platforms can contribute to the trust of the customers by allowing them the means of track comprehensive information about product characteristics through smart contracts. Contextually, smart contracts, can be referred as a set of written rules recorded in the blockchain, which is most effective in determining the interactions between the network actors. Smart contracts are therefore quite likely to influence data sharing patterns through the network, most commonly observed in the information sharing processes used for supply chains to drive continuous improvements [16]. Stating precisely, it was argued by Saberi et al. [41] that governance systems built on the premises of smart contracts comprise the characteristics of a blockchain-based supply chain to further authorize actor certification as well as approval, which further aligns with the security principles of the technology at large. Therefore,

Proposition 3: Blockchain technology is positively related to inter-firms’ knowledge sharing.
DISCUSSION

Transactions practiced in the modern phenomenon are often defined with the features of involving more than one independent party, while also being centralized and dominated by third party organizations. This accentuates the requirement for a dependable and transparent way of recording, transmitting as well as managing information in its raw form. However, the modern era requisites negotiate currency transfer processes, which are subjected to the approval of a banking institution or a credit card company, acting as an intermediary or a middle man to execute the transaction and bring a closure to the engaged parties. In most occasions, the process is not only viewed as cost consuming but also as time consuming, besides being subjected to high risks of breach and foul play. A similar process is applicable in other fields of information sharing and storage that pertains various domains from gaming to business and software innovation among others. The involvement of an intermediary here makes the entire transaction system a centralized phenomenon, where the information is controlled by independent third-party organizations, which may or may not act out in the favour of the interests of the primarily involved parties.

It was with concern over these issues impeding the effectiveness of the transaction systems in the 21st century context that the idea of blockchain technology was established. As the fundamental objective of this technology is to make significant contributions to the process of developing a decentralized environment, with limited role for the third party to influence a transaction, it is also designed to consider the transparency, validity and security concerns of the modern era with greater efficacy. Blockchain has been much appreciated for its competencies to act as a distributed database solution, since its establishment, owing to the ability of maintaining an increasing series of data records, confirmed by the nodes. Blockchain technology also functions on a model similar to the public ledger, capable of including information from almost every transaction to have ever taken place without the involvement of any manual effort. It is thus that blockchain has been defined by experts around the world as a decentralized solution, which disregards any necessity for the third party organizations to get involved in the process, as the information created is immediately and autonomously stored in the blockchain for further sharing and availability through other nodes of the computer networking systems. It is owing to these qualities that the blockchain technologies become more transparent when compared to the security assurances offered by the centralized transactions connecting a third party in the process.

As already mentioned in the literatures reviewed in the previous section, the nodes used in the computer networks to share information through the blockchain are featured as anonymous by nature, making it even safe and more secured. Nonetheless, even though the blockchain technology can be observed as a suitable solution to conduct transactions using bitcoins or other forms of crypto-currencies, the underlying technical challenges, as well as limitations, cannot be ignored in the long-run perspective. It is in this regard that through continuous monitoring a high degree of transactional integrity and security needs to be mandatorily maintained, in addition to privacy to prevent the risks of a breach and similar attempts to perturb transactions conducted using the blockchain technology. According to Swan [2], some of the noteworthy challenges and limitations inherent to the process of blockchain technology are identifiable in terms of its throughput issues using the bitcoin network, besides being identified in terms of its latency and size as well as bandwidth requirements. This implies that even though the technology holds the competency to drive a significant change in the modern phenomenon concerned with the storage, protection and sharing of information, future amendments will be needed to ensure that blockchains are developed and maintained in an up-to-date manner.

CONCLUSIONS

Blockchain technology is principally denoted as a decentralized mechanism to empower security within transactions, especially concerned with crypto-currencies as similar to the bitcoins. Since the blockchain technology was introduced in the year 2009 by Nakamoto, it has propelled significant innovations in the modern phenomenon, especially in the context of computer science and crypto-currency. In doing so, the technology has imposed a long-run influence on the economic dimensions of the modern world, by implementing changes to the conservative dimensions of bitcoin, which has been categorized as critical to consensus among the engaged parties. This implies that bitcoin transactions are affected by the various issues related to internet protocols. To manage these concerns thus, the blockchain technology functions through a decentralized mechanism, where information is stored in the form of blocks created in an autonomous manner as soon as the chain identifies a new input. These blocks are non-editable and therefore, cannot be influenced by third parties. Even if it is changed, or is intended to be changed, the third party will need to change all the blocks in the series, which is not only complex but quite demanding. It is through this simple measure that the blockchain technology attempts to prevent data security breaches and therefore, increases the authenticity of the information shared through its networks.
Acknowledgement

This study is supported by The Ministry of Science and Technology, Taiwan, R.O.C. (Grant Number: MOST 107-2410-H-030-077 –SSS).

REFERENCES


