A combined Blockchain and zero-knowledge model for healthcare B2B and B2C data sharing

Journal Item

Arab Journal of Basic and Applied Sciences

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tabs20

A combined Blockchain and zero-knowledge model for healthcare B2B and B2C data sharing

Hesham Moosa, Mazen Ali, Hasan Alaswad, Wael Elmedany & Chitra Balakrishna

To cite this article: Hesham Moosa, Mazen Ali, Hasan Alaswad, Wael Elmedany & Chitra Balakrishna (2023) A combined Blockchain and zero-knowledge model for healthcare B2B and B2C data sharing, Arab Journal of Basic and Applied Sciences, 30:1, 179-196, DOI: 10.1080/25765299.2023.2188701

To link to this article: https://doi.org/10.1080/25765299.2023.2188701

Published online: 29 Mar 2023.

ARAB JOURNAL OF BASIC AND APPLIED SCIENCES
2023, VOL. 30, NO. 1, 179–196
https://doi.org/10.1080/25765299.2023.2188701

University of Bahrain
Taylor & Francis
Taylor & Francis Group

ORIGINAL ARTICLE

OPEN ACCESS Check for updates

A combined Blockchain and zero-knowledge model for healthcare B2B and B2C data sharing

Hesham Moosa[a], Mazen Ali[a], Hasan Alaswad[a], Wael Elmedany[a] and Chitra Balakrishna[b]

[a]College of Information Technology, University of Bahrain, Zallaq, Kingdom of Bahrain; [b]Mathematics School of Computing & Communications, The Open University, Milton Keynes, UK

ABSTRACT

The two main forms of healthcare data exchange among entities are business-to-business (B2B) and business-to-customer (B2C). The former uses the electronic data interchange (EDI) technology between healthcare institutions, while the latter is usually conducted by providing web-based interfaces for patients. This research argues that both forms have inherent security and privacy weaknesses. Furthermore, patients lack appropriate transparency and control over their own Personally Identifiable Information (PII). We explore the issues of medical record exchange, analyze them and suggest appropriate solutions in the form of a new model to mitigate them. The vulnerabilities, ranging from critical to minor, include the possibility of Man-in-The-Middle (MiTM) and supply chain attacks, weak cryptography, repudiable transactions, single points of failure (SPOF), and poor access controls. A novel model will be presented in this research for healthcare data sharing which applies the best security practices. The proposed unified model will counter the listed vulnerabilities. It automates the healthcare processes in decentralized architecture by utilizing the smart contracts for B2C transactions such as medicine purchase. The model is based on the Blockchain and zero-knowledge proofs. It is made with novel controls which represent the latest advancements in cybersecurity. It has the potential of setting a new cornerstone.

ARTICLE HISTORY
Received 24 December 2021
Revised 14 February 2023
Accepted 4 March 2023

KEYWORDS
Zero-knowledge; Blockchain; healthcare; business-to-business; electronic data interchange; business-to-customer; cybersecurity; smart cities

1. Introduction

Recent developments driving the transformation of cities to smart cities call for a rise in the importance of providing cybersecurity to the different data being collected. Although smart cities allow seamless connection among citizens and reduce the city's operating costs, they also create cyber risk. The risks to the data therein will affect all participating stakeholders of the smart infrastructure, which includes financial services, healthcare, transportation, and power (Bai, Hu, He, & Fan, 2022).

The Blockchain technology provides functions necessary for the sharing of trusted and verifiable data (Al-Jeshi, Tarfa, Al-Aswad, Elmedany, & Balakrishna, 2022). It allows the sharing of data across different parties in a secure and verifiable manner. The technology is being integrated into several digital services (Swan, 2015; Al-Aswad, El-Medany, Balakrishna, Ababneh, & Curran, 2021). Many countries have plans to invest in the Blockchain for the development of their digital services to improve process efficiency (Ølnes, Ubacht, & Janssen, 2017).

Many security and privacy concerns arise when data is being communicated using the traditional client-server model. Having a unified model which connects isolated steps within the supply chain together can mitigate risks and streamline processes; and the base for such a model is the Blockchain. This research presents the Blockchain, a decentralized technology for storing data shared by a network of peers, as a solution for the presented issues.

In the proposed model, the Blockchain does not replace EDI but replaces the way EDI messages are exchanged. Instead of the data being submitted to an EDI server, the data is submitted to a private Blockchain network. All transacting businesses are part of the network. The Blockchain network, in turn, will validate the transactions by the use of smart contracts and pass the transaction to the other party.

Some security advantages will be provided inherently by the Blockchain network, such as preventing data manipulation and avoiding SPOFs. The

CONTACT Wael Elmedany welmedany@uob.edu.bh College of Information Technology, University of Bahrain, UOB Sakhir Campus, Building S40, P.O. Box 32038, Zallaq, Kingdom of Bahrain

proposed model has the following features and advantages:

- Provide unique security and privacy features needed for B2B transactions.
- Mitigating the risk of MiTM attacks by delegating the certificate authority (CA) responsibility to members of the network.
- Reducing the possibility of supply chain attacks by codifying trading agreements and contracts into smart contracts.
- Avoiding the use of vulnerable protocols by mandating a novel unified EDI exchange mechanism through HTTPS based on the RESTful programming concept.
- Providing granular access control.

This research will address, among other issues, the security and privacy limitations of EDI. It will study the risks of sharing healthcare data and mitigate those risks. The main contribution of this paper is the development of a novel model combining the zero-knowledge proof with Blockchain to solve the security and privacy issues in the healthcare data sharing in both business-to-business or business-to-customer scenarios (Mozumdar, Aliasgari, Venkata, & Renduchintala, 2016; de Vasconcelos Barros, Schardong, & Custódio, 2022; Barros, Schardong, & Custódio, 2022). This combined model has the potential to unify the way data are shared in healthcare (Al-Aswad, Hasan, Elmedany, Ali, & Balakrishna, 2019; Al-Aswad et al., 2021).

The rest of the paper is organized as follows: Section 2 review the most recent related works, in Sections 3, we review EDI technology, its components, controls, security and privacy weaknesses, and their countermeasures; Section 4 discuss the Blockchain Technology as a Solution. In Section 5, we present the combined model which aims to address the discussed risks and offers suitable countermeasures. In Sections 6, we map the security and privacy countermeasures within our combined model. Next, in Section 7, we provide a statement on the reliability of the proposed model's data, and discusses the results and overview of the model's limitations. Section 8 is the conclusions and future works.

2. Related work

The Blockchain technology enables the sharing of trusted and verifiable data among different entities in healthcare sector (Al-Aswad et al., 2021), it can revolutionize inter-business processes, such as those seen in supply chains or healthcare data sharing (Al-Abbasi & El-Medany, 2019; Kumar et al., 2022; Truong, Sun, Lee, & Guo, 2020). The Blockchain is a distributed digital ledger where data transactions are visible to the participant or peers (Al-Jeshi et al., 2022). A dynamic consent protocol will allow users to grant, deny or revoke access to data for different reasons according to their preferences. Blockchain technology offers a different approach to storing information (Truong, Sun, & Guo, 2019). Transactions are the equivalents to records of the classic database. The Blockchain uses a block for each data to be stored, with each block having cryptographic information combined between that data in the block along with a link to the previous block. A chain of blocks is maintained to establish trust and verifiability. Therefore, if a block within the chain is valid, all blocks up to that block are valid.

Healthcare is currently offered by both government and private entities. Automation in healthcare has devices generating data that needs to be validated and associated with both users and providers (Alromaihi, Elmedany, & Balakrishna, 2018; Farouk, Alahmadi, Ghose, & Mashatan, 2020). Such data would require to be shared across multiple providers. There is a need for a trusted model for exchanging such *citizens medical data*, where the privacy and integrity of the data can be verified (Zyskind, Nathan, & Pentland, 2015; Rahulamathavan, Phan, Rajarajan, Misra, & Kondoz, 2017; Baizal, Tarwidi, & Wijaya, 2021; Ouaddah, Elkalam, & Ouahman, 2017; Ni, Huang, Zhang, & Yu, 2019; Srivastava, Parizi, & Dehghantanha, 2020).

There is a large scope for the use of the Blockchain in a smart city context, given the diversity of providers, devices, the velocity of data generation, and the need for its exchange (Ali, Anwar, Salem, & Dhuhlia, 2022; Aidos, Ezzahra, Kassab, Benamar, & Falah, 2022). The Blockchain can be used for health information administration, so any private organization could be allowed to access the health information (Abdallah & Nizamuddin, 2023; Gunasekaran, Shanmugam, Rajan, & Rontala, 2023; Matullo, Amato, & Burskii, 2023). There are a number of documents involved in process of exchanging patient information between healthcare institutions, such as prescriptions, medical history, and radiography results (Tripathi, Ahad, & Paiva, 2020; Alharam & El-Madany, 2017; Shen, Guo, & Yang, 2019; De Aguiar, Faiçal, Krishnamachari, & Ueyama, 2020; Su, Zhang, Xue, & Li, 2020; Fu, Wang, & Cai, 2020). Currently, electronic data interchange (EDI) is used in the process of exchanging those documents (Shahzad & Heindel, 2012). Bahrain will be used as an example to show the applicability of the Blockchain in the health care industry.

EDI refers to businesses electronically communicating data that relate to transactions across the

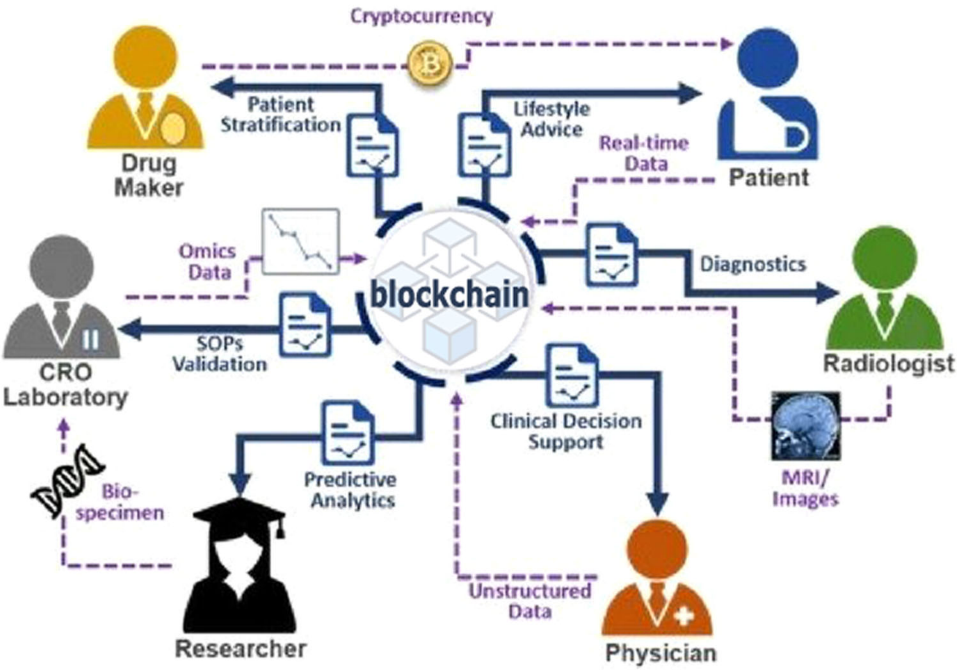


Figure 1. Blockchain as platform for healthcare.

supply chain (Lee & Whang, 2000). The main justification behind using such a technology is that it automates various parts of business processes (Lee, Ainin, Dezdar, & Mallasi, 2015). EDI allows two or more systems to directly communicate and transact medical information without the need for human data entry or involvement. It decreases costs and improves the speed and accuracy of medical data sharing (Gullkvist, 2002). EDI brought many improvements to the way data sharing was being conducted (Narayanan, Marucheck, & Handfield, 2009).

The technology employed in the most common EDI standards, such as X12 and EDIFACT, have some basic security capabilities, such as ensuring the transferred data cannot be read illegally by third parties and messages cannot be changed in transit. The EDI standards are responsible for their own security. Consequently, different ways of implementing security for each standard, all attempting to reach the same goal of ensuring confidentiality and integrity of transferred data, have evolved. The impact and the need for security was not evident until technology and automation reached regulated sectors such as healthcare (Blobel, Pharow, Engel, Spiegel, & Krohn, 1999) and banking (Dosdale, 1994). Mechanisms to provide security for EDI were retrofitted into EDI standards years after the standards were developed. A number of messaging security mechanisms such as X400 (email), X435 (email security) and X500 (directory services) are available to use as a security baseline for non-standard EDI (Abrams, Jajodia, & Podell, 1995).

There are numerous standard and non-standard EDI implementations each having varying limitations. The security and privacy limitations listed pertain to EDIFACT, an EDI standard implemented by the United Nations (UN) in 1987 (Graham, 1995). This research takes EDIFACT as an example of EDI because it is the only international standard available (Salminen, 1994). Other common standards, like X12 and TRADACOMS, are constrained to particular regions/countries or industries, and non-standard EDI are unconventional. As most EDI standards provide similar features, the same weaknesses may be found in standards other than EDIFACT.

In upcoming sections, this paper will discuss the weaknesses of EDI's security and privacy controls. A summary of the weaknesses is listed as follows:

- Man-in-the-middle (MiTM) attacks are possible due to lack of certificate verification by an authoritative third-party.
- Trust relationships among businesses render the systems vulnerable to supply chain attacks.
- Use of vulnerable cryptographic protocols.
- Transactions can be deleted after occurrence.
- Systems have a single point of failure (SPOF).
- Insufficient access controls.

There are many Blockchain architectures that have been implemented to provided services for the healthcare system. Figure 1 (Adapted from Shahzad and Heindel (2012)) represents a Blockchain combined with IoT technologies that enables the healthcare facilities to have efficient and accurate record management, which is critical. Figure 2 (Adapted from Tanwar, Parekh, and Evans (2020)) shows a "Blockchain-based electronic healthcare record system for healthcare applications", in this research, authors "propose an Access Control Policy Algorithm for improving data

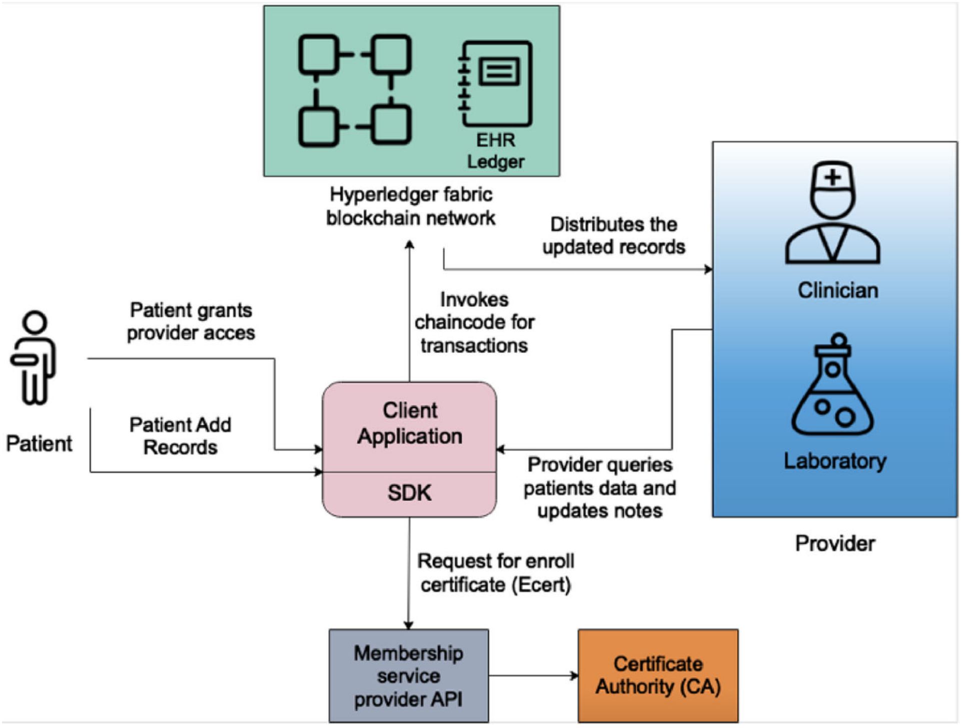


Figure 2. Blockchain-based electronic healthcare record system for healthcare applications.

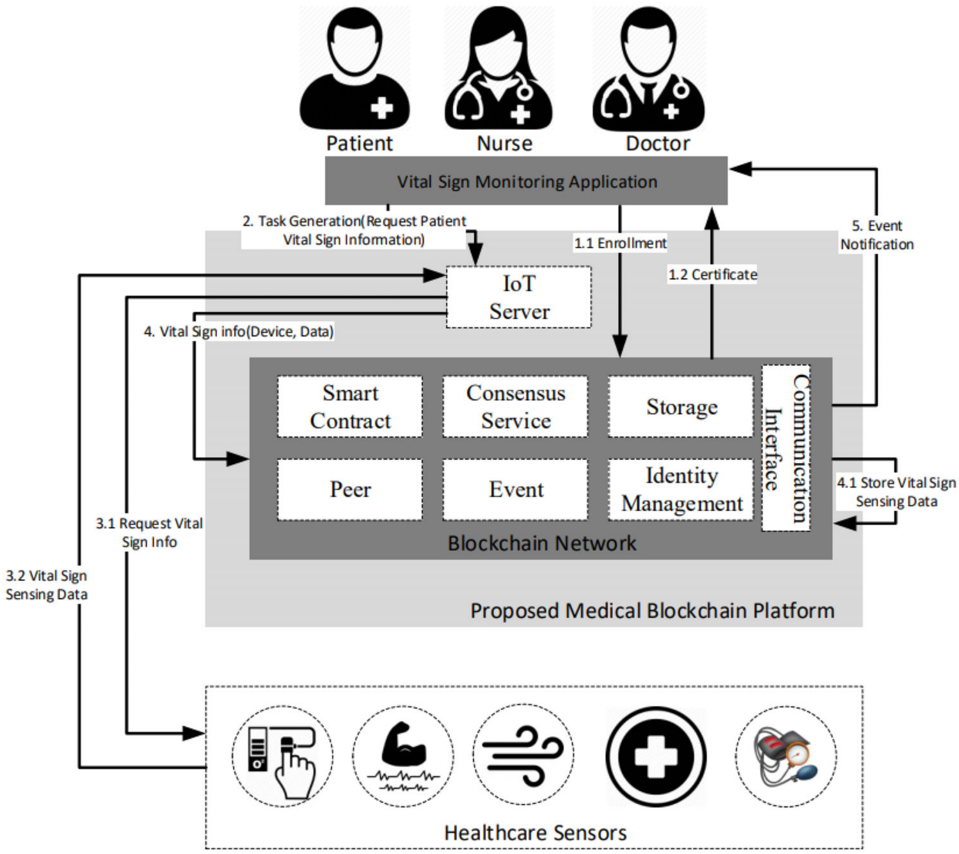


Figure 3. Healthcare IoT Blockchain platform.

accessibility between healthcare providers, assisting in the simulation of environments to implement the Hyper-ledger-based Electronic Healthcare Record (EHR) sharing system that uses the concept of a chain-code" (Kim, Yu, Lee, Park, & Park, 2020; Alzuabi, Ismail, & Elmedany, 2022; Attaran, 2022).

A novel platform for monitoring patient vital signs using smart contracts based on Blockchain is shown in Figure 3 (Adapted from Jamil, Ahmad, Iqbal, & Kim, 2020).

Using the Blockchain means that businesses not only can *exchange* data, but also *integrate* data according to Swan (2018). In their paper, the authors conceptualize how can accounting ledgers be linked together through the Ripple Blockchain-based network. They indicate that the current ways of transacting, EDI and paper-based included, creates accounting journal entries which have to be confirmed and posted by humans. This is prone to errors and fraud. In the Blockchain-powered supply chain process, the whole process is automated as smart contracts will take over the verification tasks of humans.

With the Blockchain, accounting can benefit from an emerging concept called "triple-entry bookkeeping", where one or more accounts are debited, one or more accounts are credited, and the transaction is confirmed in a distributed ledger.

The use of private Blockchains is explored in a publication by Banerjee (2018), it discusses how can Blockchain be used to improve upon B2B processes that are currently being conducted between enterprise resource planning (ERP) systems. The authors suggest that Blockchain networks will enhance the standardization, synchronization and security of business data while ensuring that the data remains immutable and less prone to attacks.

3. Electronic data interchange (EDI)

EDI is the communication of business data in a structured, computer-readable form through an electronic medium. Data exchanged using the technology does not need to be re-keyed as it occurs between business systems in different locations (Hill & Ferguson, 1989). The data may be transported using a variety of mediums. These ways include exchange of physical drives, use of intermediaries such as value-added networks, and using the internet (Shi et al., 2020).

In order to implement EDI, an organization must have all the necessary infrastructure to run the technology or have them provided as a service. There are few main infrastructure elements as described by Hill and Ferguson (1989) which will be used within this paper:

- A common agreed-upon standard for representing business documents.
- Application to application intercommunication protocols.
- Translation software to convert internal business data into standard formats.
- Networking computer hardware and servers.
- A communication medium, such as Value Added Networks (VANs) or the internet.

3.1. Elements of EDI

A number of elements constitute an EDI system. The different elements are illustrated in Figure 4 (Adapted from Shahzad and Heindel (2012)). The contents of an EDI message are detailed in the next section.

The Figure depicts the transfer of EDI messages between a sender and a receiver. The messages are transferred in batches, where one or more messages are grouped together and then sent. A business calls other businesses who are involved with it in an EDI exchange its trading partners. Usually, a retailer, not the supplier, is the party who invokes an exchange.

Compliance checks also include conformance to the use of proper data element separators. The different element separators within a segment in EDIFACT.

Data transformation is the step where data is mapped to the data requirements of the receiver's

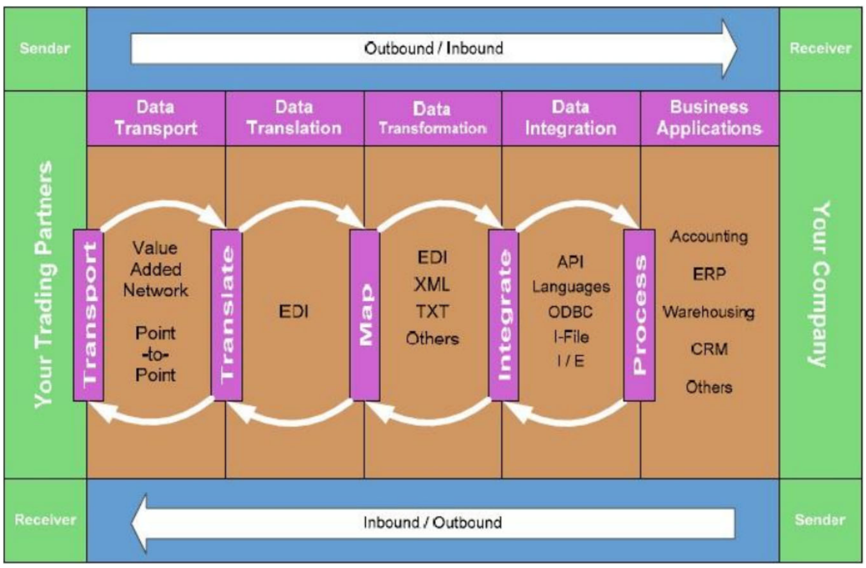


Figure 4. The elements of electronic commerce/EDI.

system. An inbound message has its data mapped according to a pre-specified map definition. The map definition determines the place of each piece of data within the internal system's database.

Every EDI messages is formatted in a special way and is combined with other EDI messages in a batch container. There is a special piece of transaction software which does the "behind the scenes" work to enable this grouping. Its concepts are discussed next.

3.2. Controls and message safety

The message safety standard, which guarantees that messages are resistant to various attacks, available for EDIFACT is formally known as the EDIFACT Security extension. This extension was designed to provide baseline protections where protocol-level security is insufficient. It is independent from the transport mechanism (Turi, 1993). We review the features of EDIFACT Security extension.

The EDIFACT message-level security solutions include AUTACK message, CIPHER message, Message Security Header and Trailer (which explains UNH and UNT message wrappers), and KEYMAN message (Thorud, 1994).

3.2.1. AUTACK message

Secure Authentication and Acknowledgement (AUTACK) message is used in two ways: (a) as an authentication message from the sender to the receiver, and (b) as an acknowledgement message from the receiver to the sender.

When used as an authentication message, the AUTACK message proves that the previous EDIFACT messages were sent from the actual sender and not a malicious third party, the messages' contents and sequence are valid, and messages cannot be repudiated by the sender.

When used as an acknowledgement message, the AUTACK message acts as a confirmation by the recipient that the messages were indeed received, messages' contents are intact, messages are complete and the receipt of messages cannot be repudiated.

3.2.2. CIPHER message

The CIPHER message, as its name suggests, provides confidentiality to EDIFACT messages and interchanges. It achieves this by acting as a wrapper of encrypted EDI content. CIPHER headers are added whenever the EDIFACT content is encrypted to enable it to be processed by the receiver. An overall view of a CIPHER message is shown in Figure 5.

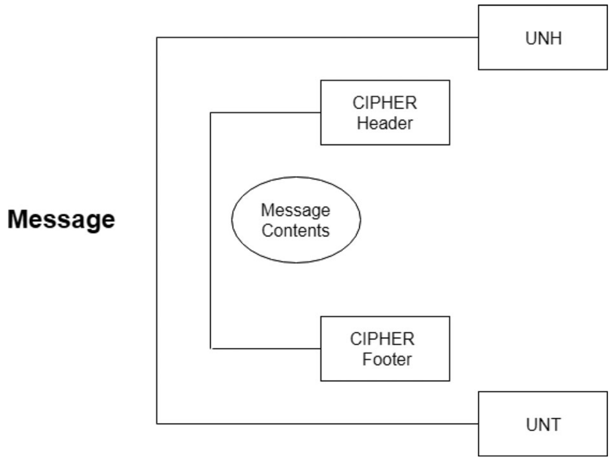


Figure 5. EDI segment wrappers of a CIPHER message.

If the receivers possess the correct decryption key, they will be able to decrypt and process the message contents like any other EDIFACT message.

3.2.3. Message security header and trailer

The security services can be either provided by a separate AUTACK message or built into the message by including special security headers and trailers. These two methods can provide all security services, such as integrity and non-repudiation, with the exception of confidentiality.

In order to provide security within a message, header and trailer segments groups are added after a UNH and before the UNT. UNH and UNT are security headers and trailers which provide security-related metadata. Each segment group corresponds to a particular security service. This way, security can be added to any message.

The role of a security header is to specify the security controls which were applied to the message and to provide the data needed to conduct message validation. It includes listing of used mechanisms and algorithms, including corresponding keys and certificates.

The role of a security trailer is to carry the results of security services specified in the header. Usually, it contains results of algorithm computations. For example, a header may specify that a message uses SHA1 hashing algorithm to achieve integrity, while the trailer will carry the actual SHA1 hash of the message.

3.2.4. KEYMAN message

Key management (KEYMAN) message allows parties in a communication to request and deliver keys, certificates and other cryptographic information. It can also be used to convey revocation of a certificate and a certificate's status.

3.3. Security and privacy weaknesses

This research presented a high level view of the security and privacy issues associated with EDI and how they will be addressed. The following is a more detailed discussion of the issues:

- *Businesses must maintain a trading partner profile containing information* such as server addresses, bank account numbers, etc. When businesses exchange profiles, a certificate authority (CA) is required to verify that profiles exchanged are authentic. Value-added networks (VANs), a form of private data exchange networks which act as intermediaries between businesses, were used in the past to provide EDI solutions equipped with CA services but were expensive and soon replaced by the internet. With the global shift towards internet-based EDI, CA services for EDI almost ceased existence. The lack of internet-based CAs for EDI opened up EDI to man-in-the-middle (MiTM) attacks including DNS hijacking and packet injection. As opposed to internet websites which are verified by TLS certificates signed by known CAs, there are no known certificate providers for EDI and no established mechanisms for managing those certificates within the EDI protocols. Such mechanisms, if desired, would have to be retrofitted in protocol revisions.
- *Before any EDI communication commences, business documents such as trading agreements and contracts must be signed*. Those documents specify limitations on the nature of the business allowed to be done and the volume of transactions. Due to their complexity, those documents are either not codified or are weakly codified into the systems. Businesses may request a transaction through EDI which is out of the arrangement and get it accepted by their partner's system. In this scenario, the trust relationship (Ratnasingham, 1998) between businesses is exploited to affect the integrity of data contained in the system. These cases are a form of cyber-attacks called supply chain attacks (Miller, 2013).
- *Parties must agree on cryptographic protocols*. EDIFACT, like other standards, supports a wide range of connections such as FTP, HTTP and others, each offering different cryptographic capabilities. Since EDI is used by many legacy internet systems, the parties may be forced to communicate using deprecated and vulnerable protocols.
- *Transactions can be deleted by colluding vendors and suppliers*. A common reason for this is to commit tax fraud. There is no mechanism for third parties, such as auditors, to independently verify the occurrence of a transaction. The transactions can be deleted from the application's database.
- *EDI systems often have a single point of failure (SPOF)*. A business often has one internet-facing "gateway" server or an ERP system running AS2 or FTP. This risks the availability of the EDI service, especially if a malicious attacker attempts a denial of service (DoS) attack.
- *Any user in a business can view and conduct transactions that represent the business as a whole*. There is no granular level of access control. This leads to a potential loss of privacy.

Note that the presented weaknesses were determined based on observations of this research. They are the points this research will address and solve.

3.4. Possible countermeasures for vulnerabilities

This section will highlight the traditional countermeasures (Bendovschi, 2015) that can be utilized to prevent or mitigate the previously listed vulnerabilities (Ingham, Marchang, & Bhowmik, 2020). Note that the actual defenses employed in the proposed model may not match the traditional methods.

MiTM attacks on encrypted communications occur because the public keys of transacting parties are not verified by a trusted third party. Such attacks can be prevented using certificates (Amann, Sommer, Vallentin, & Hall, 2013). The certificates must come from a CA that all trading partners trust.

Supply chain attacks occur because the systems are not equipped with necessary data checks. They usually do the same checks on EDI data as the data inputted from a trusted employee within the organization. Such attacks are mitigated with more stringent checks and the codifications of the physical trading contracts and agreements (Boyson, 2014).

Deprecated and vulnerable cryptographic protocols should simply be replaced with more modern-proof protocols. The use of strong unbroken protocols must be mandated rather than suggested. Transaction deletion is difficult to prevent in case of colluding parties. It requires immutable ledgers, such as the Blockchain. DDoS attacks can also be avoided if the Blockchain was used, as the data is replicated among multiple nodes and there is no central server to attack. Granular access controls can be implemented into the ERP systems used by the employees, but require a network-level implementation to achieve proper protection against advanced persistent threats (APTs).

4. The Blockchain technology as a solution

The Blockchain is a recent technological advancement which has a disruptive potential. It is a

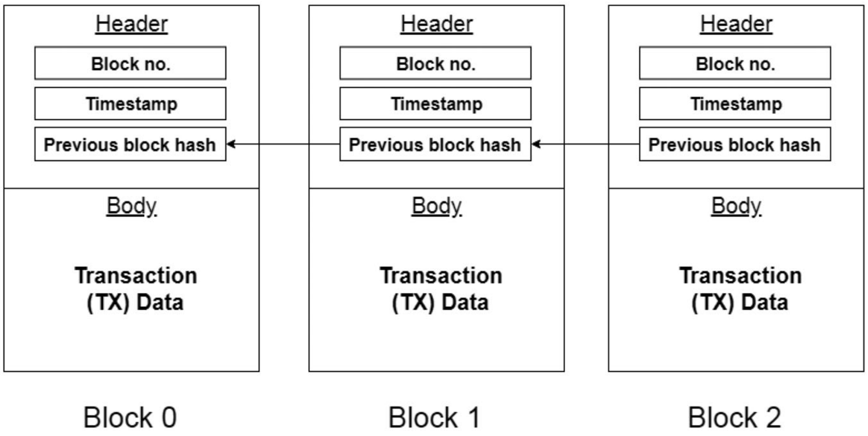


Figure 6. Example of a Blockchain.

distributed ledger of records, in which each party in the Blockchain network is having a copy of the latest version of the ledger. The ledger provided by the Blockchain is an append-only log used to record transaction data. Using a Blockchain network instead of a common database has numerous advantages: there is no central server to attack, the records cannot be modified by anyone, and the records (with the confidential information encrypted) can be made available to third parties, and so on. All the participants trust the transactions as even if one Blockchain server gets hacked, the records will not change and no damage can be done.

4.1. Introduction to the Blockchain

The idea of the Blockchain was first envisioned in paper by Nakamoto (2008). It was originally intended to become a distributed ledger which hosted Bitcoin, a cryptocurrency (electronic currency based on cryptography). Bitcoin is popular because it is the first digital currency to solve the double-spending problem in a practical way using processing power. Double-spending is flaw within digital cash schemes where money could be spent more than once.

As people realized that the potential of the Blockchain is much beyond digital currencies, the concept took off as an independent technology. The Blockchain refers to list of records that are related to each other by cryptography (Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). Each record (block) contains the hash of the record before it, creating a sequence (chain) of records. This is illustrated in Figure 6. The Blockchain records form a ledger which is distributed across many servers which synchronize the records with each other.

The inherent nature of the technology makes it especially suitable for applications having multiple parties who not trust each other (Daneshgar et al., 2019). This is because every party can contribute to adding records to the Blockchain and each can independently verify the information contained within it.

4.2. The Blockchain architecture

It is important to understand the contents of a block and how is it cryptographically linked to other blocks. Furthermore, any reader must also know the process in which a new block is added and how do the network peers agree to add it to their ledgers.

With reference to Figure 6, block 0 is the first block in the Blockchain, thus it is known as the *genesis block*. Block 1 is the *child block* of block 0. Block 0 is the *parent block* of block 1. A genesis block has no parent.

4.2.1. Block

A block consists of a header and a body. The header usually contains (Zheng, Xie, Dai, Chen, & Wang, 2017):

- Block ID: A number used to identify the block's sequence number.
- Timestamp: Indicates the time this block was created.
- Previous block hash: A cryptographic digest of the entire block preceding the current block.
- (Optional) Merkle tree root hash: A cryptographic digest of all the transactions in the current block.
- (Optional) Block version: The version number of the software used to build the block.
- (Optional) Difficulty goal: Relates to a proof-of-work consensus concept where the block hash must be less than a certain value.
- (Optional) Nonce: A number used once to indicate that significant processing has occurred. It is put in context in Section 4.2.

The body of a block contains transactions. They may be the change of ownership of an asset, increase in the balance of an account, etc.

4.2.2. Consensus mechanisms

The main reason a consensus mechanism is used is to avoid the Byzantine Generals (BG) Problem. The

Table 1. Comparison among types of Blockchain networks.

Feature	Public Blockchain	Consortium Blockchain	Private Blockchain
Agreement	All nodes	Chosen set of organizations	One organization
Joining terms	Allow All	Authorized	Authorized
Viewing transactions	Public	Public or restricted	Public or restricted
Speed	Low	High	High
Central	No	Partial	Yes

Table 2. Taxonomy of vulnerabilities in the Blockchain.

Vulnerability	Cause
51% vulnerability	Consensus mechanism
Private key security	Public-key encryption scheme
Criminal activity	Cryptocurrency application
Double spending	Transaction verification mechanism
Transaction privacy leakage	Transaction design flaw

problem mainly questions the course of action to take in case not all peers agree to the same results (Baliga, 2017). It helps the network prevent attacks from malicious nodes. Proof-of-work (PoW) and proof-of-stake (PoS) are famous consensus mechanisms. The model in this research uses Practical byzantine fault tolerance (PBFT), which is another consensus mechanism where 2/3 of the nodes must vote to select the node that builds the next block. Although PBFT is the used in this research, the next section will describe PoW to highlight the most common method of building blocks and later sections will describe how PBFT is a more appropriate selection for the context of this research, how it works and the way it will be utilized.

4.3. Taxonomy of the Blockchain networks

There are three types of the Blockchain networks: public, consortium and private. The public Blockchain is open to anyone in the world. Users can check the transactions and participate in the consensus process. A consortium Blockchain consists of a group of organizations, usually based on business partnerships, and is regarded as partially decentralized because only a subset of the members can participate in consensus and the selection of organizations who will participate in the subset is bound to respective business arrangements. A private Blockchain is owned by a single organization only. It is operated mostly to achieve better auditability and availability (Zheng, Xie, Dai, Chen, & Wang, 2018). The different types are compared in Table 1.

4.4. Security of the Blockchain

Li, Jiang, Chen, Luo, and Wen (2017) conducted a systematic study for security risks and weakness of the Blockchain different technologies and discussed total of 17 risks in the Blockchain and the causes, 12 of which were in the smart contracts. The vulnerabilities in the Blockchain are summarized in Table 2.

Since Proof of Work (PoW) is a consensus protocol confirms that the participating nodes with most of the processing power are the ones who can create the block, the 51% attack was designed to exploit the core of this concept. The attack states that if an attacker could possess more than or equal to 51% of the combined processing power of all nodes in the pool, new blocks can be added by the attacker and the remaining nodes will recognize the update as legitimate. A similar attack can be waged against Blockchains that utilize the Proof of Stake (PoS) consensus protocol by controlling more than or equal to 51% of the total coins balance in circulation.

5. The proposed Blockchain model

A Blockchain-based EDI has the potential to solve the security and privacy concerns of the old technologies, especially in those involving supply chains (Saberi, Kouhizadeh, Sarkis, & Shen, 2019). When the Blockchain is used, the identities of EDI trading partners can be posted on the network to become constantly up-to-date and immutable (the secure standards used for posting profiles are based upon initiating a high-level trust when first joining the Blockchain only and are not a secure choice when routinely adding new partners to the legacy point-to-point EDI). This way, the risk of MiTM attacks when transmitting partner information updates is mitigated as there is no need for direct communication (which often uses legacy security standards and self-signed certificates). Businesses do not have to maintain partner profiles because the information is available on the network. When posting data to the network, the utilized cryptographic protocols can be standardized and only the most secure ones can be adopted. Note that trusting a Blockchain once is more secure than building trust every time when a trading partner is added because it is less likely that a single secure handshake would be intercepted and spoofed as opposed with multiple handshakes. The keys needed for joining a Blockchain network can also be practically transferred physically as only a one-time setup is needed, which is not the case for continually adding point-to-point trading partners.

Figure 7 depicts a sample Blockchain network with two organizations and one ordering organization between them.

All transactions in the Blockchain network are secure and auditable. The transactions cannot be deleted and the network is resistant to failures. In addition, the uniquely developed smart contracts tackle

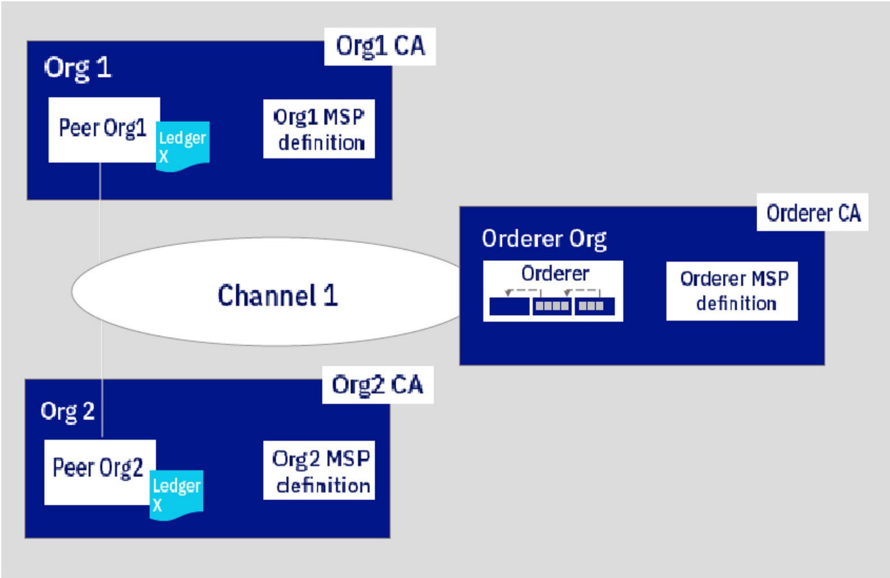


Figure 7. Sample Blockchain network.

the issue of trusting the contents of transactions. Privacy is enhanced as stricter and more granular access controls can be applied to users between transacting businesses and even within a business. Businesses can enforce access controls on each other. Furthermore, Blockchain allows for the creation of private channels for confidential deals and can permit the public or the government to access part of the data, such as for transparency or taxation purposes.

5.1. Justifying the use of Blockchain to counter existing vulnerabilities

There are two questions to be answered in this section: (a) Is Blockchain applicable to B2B transactions, and (b) Will using Blockchain lead to better mitigation of EDI's risks.

It is evident that B2B transaction processing is an excellent use case of Blockchain, as there are multiple institutions involved who by nature do not trust each other. The institutions already can directly communicate with each other without an intermediary, but it is unreliable due to poor controls on the data and on the infrastructure.

Referring back to Section 3.3, this research has identified six vulnerabilities affecting the security and privacy of EDI. The distributed immutable nature of Blockchain inherently mitigates vulnerabilities relating repudiation of transactions (related nonavailability of known CAs described in Section 3.3) and SPOFs. Other vulnerabilities such as MiTM susceptibility, supply chain attacks, vulnerable protocols and improper access controls will be dealt with by deploying appropriate controls in the proposed model. The countermeasures will be discussed more in the upcoming chapters.

5.2. Requirements

The proposed model will be replacing the network-level protocols currently in use for EDI with a Representational State Transfer (REST) application programming interface (API) connection to a Blockchain network. The REST API is an architecture for creating web services. It is a replacement for remote procedure call (RPC). It will be utilized in the PoC because it has greater flexibility in defining security policies and higher performance than RPC Feng, Shen, and Fan (2009).

Once connected to the REST API, the user will use the HTTP methods: GET, PUT, POST and DELETE to query the Blockchain. The connection will use HTTP over TLS/SSL (HTTPS). The user will communicate with the Blockchain network by invoking chaincode-based functions using HTTP requests. Note that the server hosting the REST API is also a peer in the Blockchain network. The communication between the client and peer is modeled in Figure 8.

In order to protect against the vulnerabilities mentioned in Section 3.3, the model will provide CA services inside the Blockchain. There will be multiple CAs within the network, each run by zero or more organizations.

Chaincode will minimize the likelihood of supply chain attacks. Users will not be able to do any modifications to the Blockchain without the use of a chaincode function. Real-world agreements and contracts must be codified in chaincode. Refer to Section 4.2 to understand how codifying contracts in chaincode are different than other methods.

Security policies will be created in the REST API (Serme, de Oliveira, Massiera, & Roudier, 2012) to mandate strong cryptography between the user and the peer. Hyperledger Fabric will be modified to mandate strong cryptography among the peers who

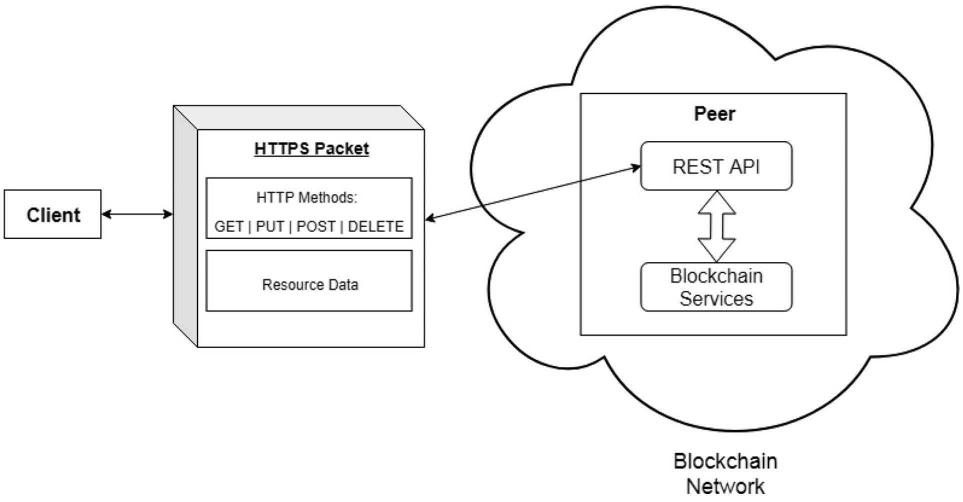
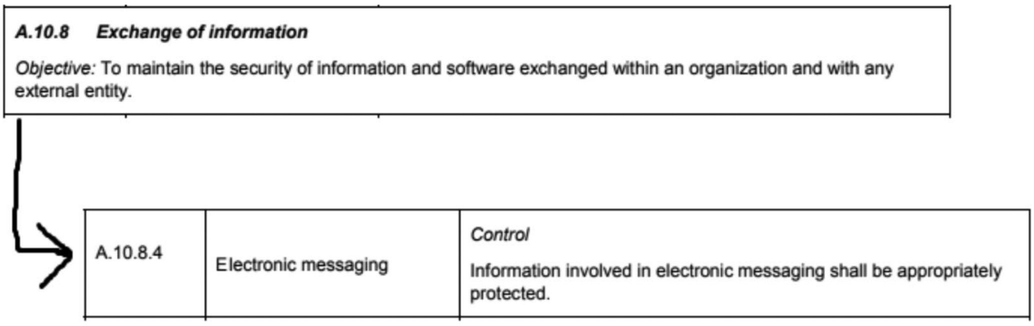


Figure 8. Client and peer communication using REST API.



A.10.8 Exchange of information *Objective:* To maintain the security of information and software exchanged within an organization and with any external entity.		

A.10.8.4	Electronic messaging	*Control* Information involved in electronic messaging shall be appropriately protected.

Figure 9. EDI security control in ISO27001 standard.

are members of the Blockchain network. Any connections using suboptimal cryptography will be immediately dropped.

Access controls will be built into the REST API. It will provide control authorizations on the user level, rather than the organization level which is currently used EDI. A mechanism will be provided for organizations to define allowable actions for their individual employees. No employee will be allowed to conduct EDI transactions of which they are not authorized.

The Blockchain will inherently provide immutability and availability of data. Organizations cannot collude to hide transactions from tax collectors and attacker's DoS attacks will not succeed since the ledgers are copied to multiple servers.

5.3. Security and privacy standards

The model will be designed to satisfy the requirements and best practices mandated in ISO27001 and ISO27002 (Calder, 2013; Vasudevan, 2008) international security standards. Specifically, the model will conform to electronic messaging rules. Figure 9 show the rules pertaining to achieving proper EDI from the standards. Note that ISO27001 discusses a policy-level managerial perspective of standards implementation, whereas ISO27002 explains how to achieve a good implementation of the controls in ISO27001.

The implementation guidance will be followed in the model and in the PoC. The advantage is that it will give a better standing to the work done in this research. Moreover, it proves that the model is a viable extension to EDI rather than an incompletely-studied deviation from the norm.

5.4. Network-level view

A core part of the proposed model is the consortium Blockchain network. Such type of network was chosen in particular because it was built for housing multiple organizations where the data exchange could be partially confidential. It allows organizations belonging to same industries to exchange data either in public or in private channels where only certain member organizations can access the data.

Before reaching the network, the message data passes through a number of steps. Data is manipulated and processed all the way to a Blockchain. The actual Blockchain is abstracted away from the user by APIs and smart contracts.

Figure 10 illustrates the proposed model from an action point of view of a single organization. An employee in an organization uses a business application, such as an ERP system, to send an EDI message.

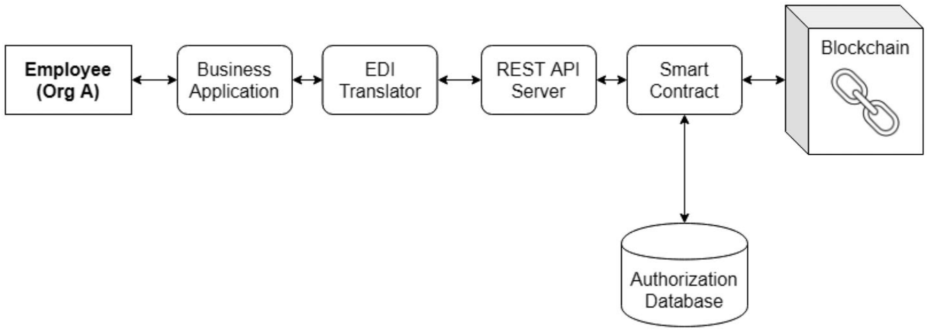


Figure 10. Action steps of the proposed model.

The message passes through an EDI translator which maps the message to REST API representational data and methods. It turns EDI messages into smart contract calls encoded in REST API instructions. The REST API then queries peers and orderers (nodes who order transactions in a block) in the network that executes and posts the transactions.

In the figure, peers and orderers are simply represented as smart contract. The smart contract will query an authorization database. It will send the user's transaction signature and transaction channel ID to the database and get back the authorizations of the users on the particular channel and if the user can run the particular smart contract. If the user is authorized and the transaction information is valid, the transaction will be posted to the Blockchain and propagated to other nodes.

In this proposed model, querying the Blockchain without any updates also require the request pass through a smart contract. Reasons are mostly to check authorizations and to prevent users with insufficient privileges from accessing the organization data. Note that private channel data are not shared with nodes that are not members of the channel, so a user from an organization cannot view data shared by completely different organizations who are transacting with each other.

There are more details to the interaction of the smart contracts with the Blockchain. Other diagrams will show the topology and components of the model, and how the interaction works.

5.4.1. Consensus

The consensus mechanism used in the proposed model is PBFT. Different organizations may have different sizes and different capitals amounts. Resource-related consensus mechanisms such as PoW or PoS if used will enable a hacker who gains access to the servers of a large organization to control the processing of the entire network. This is possible because organizations will have varying processing capabilities and funds to stake. Another consequence manifests in a larger organization delaying the processing of transactions submitted by other organizations that it considers its competitors. PBFT treats all organizations equally. One organization will have one vote in the network, thus preventing monopolies.

PBFT, in the proposed model, is configured with 1/3 fault tolerance. This means that at least 2/3 of the organization in a network must vote for the validity of transaction before it can be posted. Although this is not practical in a public Blockchain networks, the case is different for consortium Blockchain networks where the number of users is in the hundreds or thousands, not millions.

5.4.2. Certificate authority

CAs are a common component of private and consortium Blockchain networks. They are responsible for signing certificates of the nodes in a network. The X.509 certificates signed by the CA identify nodes which belong to a particular organization. Best practices indicate that each organization must only have one CA (Morkel & Eloff, 2004).

The certificates can be used to sign transactions. When a peer wants to endorse a transaction, it signs it using its key which the CA has verified. Signing a transaction allows it to be traced back to the organization and the peer that signed it. Signing is also a requirement so that transactions will be posted to the ledger.

Another type of CA is the TLS CA. It is different from the common CA in that it handles the encryption of communications between nodes in a network. The key generation and storage functions of a CA may be delegated to a PKCS11 encryption based hardware security module (HSM) for better security.

5.4.3. Membership service provider

A membership service provider (MSP) is one of components added to the network of the proposed model. Using a MSP allows the identification of nodes in an organization as members of the organization. It is basically a set of information identifying the organization which is signed by the CA. It maps the certificate generated by a CA to an organization.

Whenever a node (peer or orderer) is added to the network, it must receive a certificate from the CA which also includes information pointing to which MSP it belongs.

5.4.4. Peers

A peer is a type of node in a Blockchain network. It is responsible for maintaining copies of the Blockchain ledger, and committing new blocks. In the proposed model, an organization may own one or more peers.

With reference to Figure 10, a peer runs smart contracts which interact with the ledger. That is, requests from REST API are forwarded to the peers' smart contracts for subsequent execution and return of results. This is the case for smart contracts that only query the Blockchain but do not change its state.

Results of execution are returned from smart contracts that alter the state of the ledger, but are not committed to the database. The result also includes a signed endorsement. The endorsements acknowledge that the peer has approved the transaction, there was no reply attack, the user's signature was verified against the MSP, and the user is authorized to conduct the transaction.

In the case of a ledger update, a peer does not receive commit commands from the REST API, but does receive them from orderer nodes. The peers receive blocks from the orderer nodes for direct import into the ledger.

5.4.5. Endorsement policy

This model advocates the importance of private channels in a network. Such channels allow two or more organizations to have a permissioned ledger where they can post transactions and those transactions remain private.

To achieve even greater privacy, this model mandates that the data contained in private channels to be within the nodes of the organizations who are member of the channels only. But how will the parties agree on the verification of transactions before posting them to the ledger?

The answer is to add a set of rules that define what each member can do on a channel. Members may view the ledger, post new records, validate transactions, add new members to the channel, etc. depending on privileges assigned to them when they are first added the channel. In addition, an endorsement policy is added. It defines which members or how many members need to validate transactions so that it can be posted on a channel.

Endorsement policies can require that one of two trading partners in a channel validate a transaction. They can also require that all trading partners validate the transactions or more than half the trading partners validate the transactions. The policy will depend on the application and the relationship among the involved organizations.

Note that endorsement is different than consensus in this model. Here, endorsement is for peers, while consensus is for orderers. PBFT will still be used for orderers as they need to have an agreed upon order of transactions always, but the peers endorsement depends on the level of trust among organizations and do not affect transaction validation.

5.4.6. Ordering service

Channels are added to orderers. The orderers are the nodes responsible for receiving endorsed transaction requests from the REST API and creating a block with ordered transactions. The orderers order transactions on first-come-first-service basis. All the orderer nodes use deterministic algorithms to reach the same order. The details of the algorithms will not be discussed as they are standardized (Sousa, Bessani, & Vukolic, 2018) and beyond the scope of this research.

The consensus policy adopted in this model from Section 5.4.1 applies to the ordering nodes, not the peers. The ordering service, which refers to a collection of ordering nodes, uses the PBFT model. This means that the network can tolerate up to 1/3 of the ordering nodes going down.

5.4.7. Network structure

The structure of the network components of the proposed model is depicted in Figure 11. It shows a network consisting of two organizations, however there may be more in a real-life network. Each organization has its own CA and MSP. The MSP is the entity that records information about the identity of the organization and ties nodes to the organization. Each one also has three peers and one orderer. Note that the Figure may imply a SPOF for REST API, CA and MSP, and orderer, but in real-world implementations, those components must be more than one to avoid a SPOF. A single component for each was illustrated in the figure for demonstration purposes only. The REST API, as shown in the previously discussed action model, receives input from an EDI translation software.

The REST API will communicate directly with the peers and orderers. The smart contracts (Chaincode) will run inside the peers of the network. More specifically, the REST API will communicate with the peers and invoke Chaincode within the peers based on arguments it receives from the EDI translator. Each peer maintains a copy of the ledger.

In this model, we separate the Blockchain ledger and the peer chaincode for efficiency reasons. This is because the peers are usually computationally intensive, while the ledger is storage intensive.

The REST API communicates with the orderer only after it receives signed endorsements from the peers.

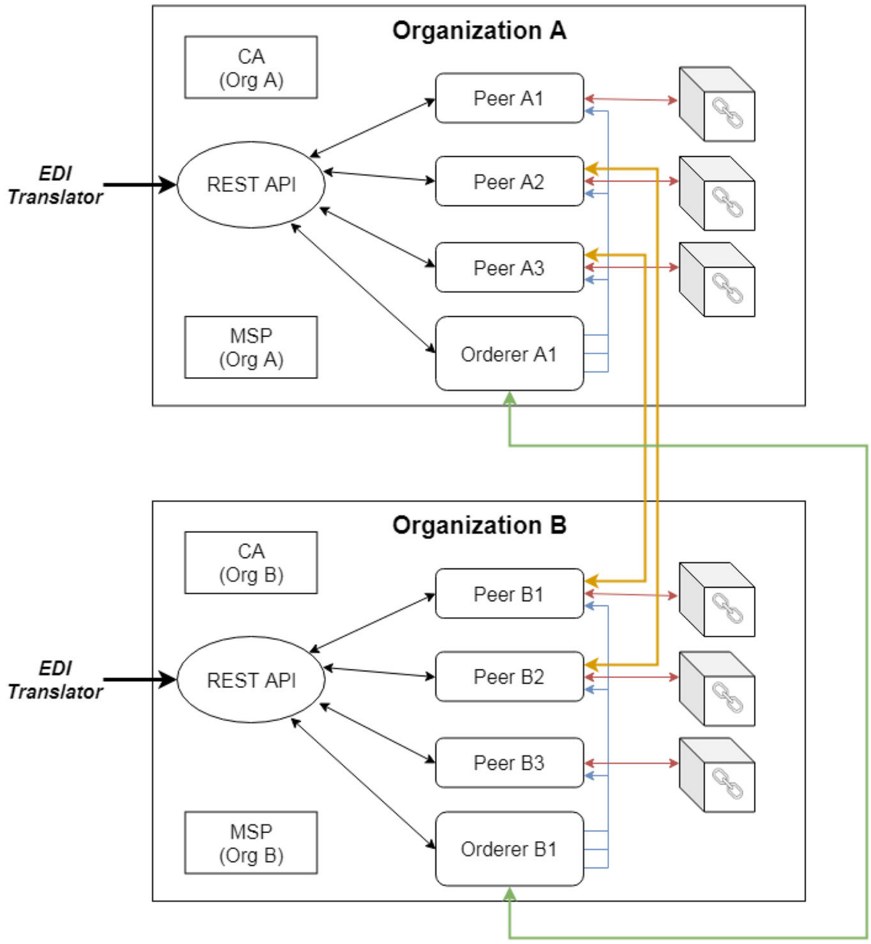


Figure 11. Network structure of the proposed model.

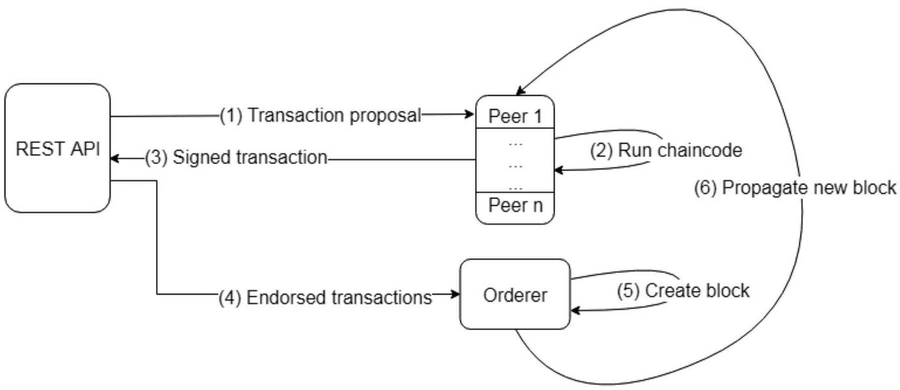


Figure 12. Commit process of the proposed model.

After consensus of the orderers, a commitment order is sent to peers who are connected to the orderer. The peers will not commit until they have checked that the transaction is indeed signed by the endorsing peers and that it follows the channel's endorsement policy. These steps of the commit process in the proposed model are illustrated in Figure 12.

Notice that Peer-A2 is connected to Peer-B2 and Peer-A3 is connected to Peer-B1. A question arises as to how do peers who are not directly connected to another organization, such as Peer-A1 is not connected to any peer in organization B, listen to commits from the orderers of another organization. The answer is that peers do not need to have a valid link to another member of the same channel. They just must be connected to an orderer. All orderers, after consensus, will broadcast the message to the peers whom they are connected to. This means that a commit order from Orderer-B1 will be repeated by Orderer-A1 so that it can reach peers in organization A.

5.4.8. State database

A state database is not a new technique like the others proposed in the model. It is a form of lightweight database solution used alongside Blockchain to provide quick access to stored values without needing to traverse through the Blockchain. Thus, it maintains the latest "state" in a simple form of key-value pairs. We adopt the basic form of a state database and tweak it to better suit the requirements of organizations who conduct B2B transactions.

We tweak CouchDB, a lightweight state database with querying capabilities, as a state database for the PoCs Blockchain. It allows the use of rich queries similar to those of structured query language (SQL).

6. Mapping the security and privacy countermeasures, and evaluation

6.1. Mapping the security and privacy countermeasures

At the beginning of this research, six security and privacy issues were mentioned. The way each issue was tackled is discussed in the previous sections. The following list will summarize the solution approaches.

(1) MitM attacks: Multiple CAs were deployed, each belonging to an individual organization. Organizations trust each other's CA when they are first enrolled together in a private channel. Refer to Section 5 for applicability to point-to-point transactions.

(2) Supply chain attacks: More stringent restrictions on the allowable transactions. Transactions follow the least privilege principle. The same validation rules could be implemented in EDI processors but are more readily and securely implemented in chaincode language.

(3) Weak cryptography: Mandated the use of strong cryptographic algorithms through REST security policies. Such algorithms are not uniformly mandated by point-to-point EDI, but could be retrofitted.

(4) Deleting transactions: All transactions conducted using Blockchain are immutable.

(5) DoS attacks: Blockchain is immune to DoS attacks due to its distributed nature.

(6) Poor access controls: Stronger interorganizational-level ACLs and newly introduced employee-level ACLs. Those ACLs can be retrofitted to EDI processors but are readily available in common Blockchain software.

6.2. Security and privacy evaluation

The proposed model has implemented all the points in ISO27001 and ISO27002 that pertain to EDI security. Referring back to Figure 9, the mode provided the appropriate protections. It protected the confidentiality, integrity and availability of messages, and ensured that it is transported in a correct way to receivers.

The services provided by the model are reliable due to their cryptographic underpinnings. They will always provide the intended results, and are fail-safe. Identities of communicating entities are verified using signatures.

Before joining a private channel, organizations are required to convert the trading rules specified in their agreements to smart contracts and access control rules. Users are authenticated using PKI which ensures that any attacker masquerading the identity of a user must first seize the user's private key.

7. Results and discussion

7.1. Reliability of data

The PoC shows that the proposed model can link records across organizations. The sales invoices entered in the system by one organization show up as purchases of another organization. This clearly improves the efficiency of business processes. The data does not need to be cross-checked.

Such a result is advantageous for organizations. The accuracy and consistency of data which is linked to other sources is better than unlinked data. Thus, the proposed model brings better reliability of data than common EDI because data is linked across organizations in the proposed model but it's not linked in common EDI.

7.2. Discussion

If Blockchain was implemented to host citizen health records, the chain would normally contain all the data. All the data, include resource-heavy images and other files, would have implications on the storage capacity of the nodes hosting the Blockchain. This is because the same Blockchain is stored by all nodes upon joining the P2P network. Furthermore, there are privacy concerns as the citizen health records will be completely accessible from any node.

The bandwidth utilization of such a Blockchain would also be an area of concern. This is because there will be ever-increasing amount of blocks and the updates are dynamic. Downloading the blocks by the nodes during every update may consume a high amount of network resources, especially if the data throughput cannot accommodate such downloads.

The proposed model suggested significant changes to the way EDI messaging is done. Although they may seem radical, they are the way forward for any effort to modernize EDI. Having constructed this model in the form of a PoC means that it is possible to have it implemented on a larger scale.

The best way to implement this model is to begin from the Blockchain network. The network will have to be designed according to the recommendations of this research while taking into account the application and the nature of the entities who will use it. The company must design a set of smart contracts for every operation it wishes other organizations to be able to do when transacting with it.

The next step is to determine which smart contracts are the most critical. This should be done using a risk analysis. The higher risk smart contracts will have to be given more attention later on when including in any business agreements.

Configuring a REST API to interact with the nodes is done after the network becomes in a good working condition. Encrypting the connections between clients, REST API, and peers is important to prevent MiTM attacks. Note that all the entities should use certificates assigned by the organization's central CA.

After the REST API is completed, the EDI translation software should be upgraded to provide REST support. The software will have to be adjusted and mapped before usage. The final step is to conduct a pilot test of the system prior to full implementation.

7.3. Limitations

The design of this model takes into consideration the system requirements from an implementation perspective. It does not consider the changes in strategy, culture or policies needed to apply the model. Such considerations are sizable and should be discussed in follow up research.

8. Conclusion and future works

The main aims of this research were to study the security and privacy weaknesses of healthcare data sharing, determine the ways they can be solved, and to develop and validate a solution model which addresses the weaknesses.

This research conducted a review of the security and privacy issues of healthcare data sharing and found new vulnerabilities not discussed in previous publications. The loopholes can be exploited by attackers to disrupt or alter the normal flow of B2B transactions. They include susceptibility to MiTM attacks, susceptibility to supply chain attacks, use of weak cryptographic protocols, and so on. Modifications to the way common EDI works were suggested in order to mitigate those issues.

A Blockchain-based data exchange model was proposed instead of the common direct B2B EDI message exchange model to solve the vulnerabilities of EDI. The Blockchain is designed, especially to work with B2B data, essentially disposing of old EDI messaging protocols such as email, FTP and AS2. It was implemented in the form of a PoC for demonstrational purposes. The PoC was shown with a sample business process as an example. This research is the first attempt to address EDI's security and privacy issues using Blockchain. It aims to achieve a milestone within the field of EDI and cybersecurity research.

Blockchain is an emerging technology which can bring many benefits to the area of healthcare. However and like with other technologies, it must be inspected and tested thoroughly before it can be offered for real world use. Its risks should be further studies, including comparing its advantages and risks with that of cloud-based models.

We recommend developing a zero-trust unified model which assumes no device or network is trusted unless its identity is verified by the system. This model can be using Blockchain to protect the devices and networks across the smart hub and allow data to be exchanged in a secure manner between devices and services.

Using this Blockchain based model for the security layer of sharing data and access management IAM architecture, the security model combines digital assets within smart city hub and acts as a trustless layer for protecting the data behind databases. This results in enhancing the accuracy of tracking and analyzing various sensors and smart devices, such as home security sensors and internet of health things. In turn, it will enable secure sharing of smart devices and services.

In healthcare industry, the Blockchain has the potential to automate the prescription dispensation and allow to develop a new business models that allow businesses to leverage Blockchain trusted systems to provide a 24/7 services without human interaction. The Zero-trust concept can be implemented using the Blockchain for the patient data received from sensors or IoT devices and can be monitored by patient and medical institutions. The risk associated with IoT is that the device itself could be used by another person to send live data. This can be mitigated by an integrated AI solution to ensure consistency of data.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Hesham Moosa http://orcid.org/0000-0001-7597-1037
Wael Elmedany http://orcid.org/0000-0001-8827-6009

References

Abdallah, S., & Nizamuddin, N. (2023). Blockchain based solution for pharma supply chain industry. *Computers & Industrial Engineering*, *177*, 108997.

Abrams, M. D., Jajodia, S. G., & Podell, H. J. (Eds.). (1995). *Information security: An integrated collection of essays* (1st ed.). Los Alamitos, CA, USA: IEEE Computer Society Press.

Aidos, E., Ezzahra, F., Kassab, M., Benamar, N., & Falah, B. (2022). A comprehensive survey on blockchain-based solutions to combat COVID-19 pandemic. *International Journal of Computing and Digital Systems*, *11*(1), 873–892.

Al-Abbasi, L., & El-Medany, W. (2019). Blockchain security architecture: A review technology platform, security strength and weakness.

Al-Aswad, H., El-Medany, W. M., Balakrishna, C., Ababneh, N., & Curran, K. (2021). BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. *Arab Journal of Basic and Applied Sciences*, *28*(1), 154–171.

Al-Aswad, H., Hasan, H., Elmedany, W., Ali, M., & Balakrishna, C. (2019). Towards a blockchain-based zero-knowledge model for secure data sharing and access. In *2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (pp. 76–81). IEEE.

Al-Jeshi, S., Tarfa, A., Al-Aswad, H., Elmedany, W., & Balakrishna, C. (2022). A blockchain enabled system for enhancing fintech industry of the core banking systems. In *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)* (pp. 209–213). IEEE.

Alharam, A. K., & El-Madany, W. (2017). Complexity of cyber security architecture for IoT healthcare industry: A comparative study. In *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (pp. 246–250). IEEE.

Ali, S., Anwar, W., Salem, B. J., A., & Dhuhlia, M. (2022). Tracing pharmaceutical products utilizing blockchain technologies. *International Journal of Computing and Digital Systems*, *12*(1), 1173–1181.

Alromaihi, S., Elmedany, W., & Balakrishna, C. (2018). Cyber security challenges of deploying IoT in smart cities for healthcare applications. In *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (pp. 140–145). IEEE.

Alzuabi, W., Ismail, Y., & Elmedany, W. (2022). Privacy and security issues in blockchain based IoT systems: Challenges and opportunities. In *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)* (pp. 258–265). IEEE.

Amann, B., Sommer, R., Vallentin, M., & Hall, S. (2013). No attack necessary: The surprising dynamics of SSL trust relationships. In *Proceedings of the 29th Annual Computer Security Applications Conference* (pp. 179–188). ACM.

Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, *15*(1), 70–83.

Bai, T., Hu, Y., He, J., Fan, H., & A., Z. (2022). Health-zkIDM: A healthcare identity system based on fabric blockchain and zero-knowledge proof. *Sensors*, *22*(20), 7716.

Baizal, Z., Tarwidi, D., Wijaya, B. (2021). Tourism destination recommendation using ontology-based conversational recommender system. *International Journal of Computing and Digital Systems*, *10*(1), 829–838.

Baliga, A. (2017). Understanding blockchain consensus models. *Persistent*, *4*(1), 14.

Banerjee, A. (2018). Chapter three – Blockchain technology: Supply chain insights from ERP. In Raj, P. & Deka, G. C (Eds.), *Blockchain technology: Platforms, tools and use cases* (Vol. 111, pp. 69–98). Elsevier. https://www.sciencedirect.com/science/article/abs/pii/S0065245818300202

Barros, M. D. V., Schardong, F., & Custódio, R. F. (2022). Leveraging self-sovereign identity, blockchain, and zero-knowledge proof to build a privacy-preserving vaccination pass. *arXiv preprint arXiv:2202.09207*

Bendovschi, A. (2015). Cyber-attacks – Trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31.

Blobel, B., Pharow, P., Engel, K., Spiegel, V., & Krohn, R. (1999). Communication security in open health care networks. *Studies in Health Technology and Informatics*, *68*, 291–296.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical it systems. *Technovation*, *34*(7), 342–353.

Calder, A. (2013). *ISO27001/ISO27002: A pocket guide*. UK: IT Governance Publishing. https://books.google.com.bh/books?hl=en&lr=&id=uFObBAAAQBAJ&oi=fnd&pg=PA5&dq=ISO27001/ISO27002:+A+pocket+guide.&ots=bVgpnln4Xq&sig=4BOg-pSIkRVXZ_Amc0X1dcHnmTY&redir_esc=y#v=onepage&q=ISO27001%2FISO27002%3A%20A%20pocket%20guide.&f=false

Daneshgar, F., Ameri Sianaki, O., Guruwacharya, P., L., Takizawa, M., Xhafa, F., & Enokido, T. (2019). Blockchain: A research framework for data security and privacy. In Barolli (Ed.), *Web, artificial intelligence and network applications* (pp. 966–974). Cham: Springer International Publishing.

De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., & Ueyama, J. (2020). A survey of blockchain-based strategies for healthcare. *ACM Computing Surveys (CSUR)*, *53*(2), 1–27.

de Vasconcelos Barros, M., Schardong, F., & Felipe Custódio, R. (2022). Leveraging self-sovereign identity, blockchain, and zero-knowledge proof to build a privacy-preserving vaccination pass. *Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass.*

Dosdale, T. (1994). Security in EDIFACT systems. *Computer Communications*, *17*(7), 532–537.

Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. *Computer Communications.*

Feng, X., Shen, J., & Fan, Y. (2009). Rest: An alternative to RPC for web services architecture. In *2009 First International Conference on Future Information Networks* (pp. 7–10). IEEE.

Fu, J., Wang, N., & Cai, Y. (2020). Privacy-preserving in healthcare blockchain systems based on lightweight message sharing. *Sensors*, *20*(7), 1898.

Graham, I. (1995). The dynamics of EDI standards development. *Technology Analysis & Strategic Management*, *7*(1), 3–20.

Gullkvist, B. (2002). *Towards paperless accounting and auditing*. Finland: Citeseer.

Gunasekaran, S., Shanmugam, S., Rajan, D. P., & Rontala, P. (2023). Blockchain technology-enabled healthcare IoT to increase security and privacy using fog computing. In *Machine Learning, Blockchain, and Cyber Security in Smart Environments* (pp. 127–144). Chapman and Hall/CRC.

Hill, N. C., & Ferguson, D. M. (1989). Electronic data interchange: A definition and perspective.

Ingham, M., Marchang, J., & Bhowmik, D. (2020). IoT security vulnerabilities and predictive signal jamming attack analysis in lorawan. *IET Information Security.*

Jamil, F., Ahmad, S., Iqbal, N., & Kim, D.-H. (2020). Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors*, *20*(8), 2195.

Kim, M., Yu, S., Lee, J., Park, Y., & Park, Y. (2020). Design of secure protocol for cloud-assisted electronic health record system using blockchain. *Sensors*, *20*(10), 2913.

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Islam, A. N., & Shorfuzzaman, M. (2022). Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Transactions on Industrial Informatics*, *18*(11), 8065–8073.

Lee, H., & Whang, S. (2000). Information sharing in a supply chain. *International Journal of Technology Management*, *20*, 373–387.

Lee, S. L., Ainin, S., Dezdar, S., & Mallasi, H. (2015). Electronic data interchange adoption from technological, organisational and environmental perspectives. *International Journal of Business Information Systems*, *18*(3), 299–320.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). *A survey on the security of blockchain systems*. Future Generation Computer Systems.

Matullo, K. S., Amato, C. A., & Burskii, P. (2023). Use of blockchain technology for implantable medical device tracking. In *Blockchain in Healthcare: From Disruption to Integration* (pp. 201–214). Cham: Springer.

Miller, J. F. (2013). *Supply chain attack framework and attack patterns*. The Mitre Corporation.

Morkel, T., & Eloff, J. (2004). Encryption techniques: A timeline approach. In *Information and Computer Security Architecture (ICSA)*. South Africa: Research Group, University of Pretoria.

Mozumdar, M., Aliasgari, M., Venkata, S. M. V., & Renduchintala, S. S. (2016). Ensuring authentication and security using zero knowledge protocol for wireless sensor network applications. *International Journal of Computing and Digital Systems*, *5*(3), 225–234.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Narayanan, S., Marucheck, A. S., & Handfield, R. B. (2009). Electronic data interchange: Research review and future directions. *Decision Sciences*, *40*(1), 121–163.

Ni, W., Huang, X., Zhang, J., & Yu, R. (2019). Healchain: A decentralized data management system for mobile healthcare using consortium blockchain. In *2019 Chinese Control Conference (CCC)* (pp. 6333–6338). IEEE.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing.

Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In Rocha, Á., Serrhini, M., and Felgueiras, C. (Eds.), *Europe and MENA cooperation advances in information and communication technologies* (pp. 523–533). Cham: Springer International Publishing.

Rahulamathavan, Y., Phan, R. C., Rajarajan, M., Misra, S., & Kondoz, A. (2017). Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 1–6).

Ratnasingham, P. (1998). Edi security: The influences of trust on EDI risks. *Computers & Security*, *17*(4), 313–324.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135.

Salminen, A. (1994). Reflections on EDIFACT: Seven issues for the future international EDI message standardization. In *ECIS*, 631–642.

Serme, G., de Oliveira, A. S., Massiera, J., & Roudier, Y. (2012). Enabling message security for *Conference on Web* restful services. In *2012 IEEE 19th International Services* (pp. 114–121). IEEE.

Shahzad, S., & Heindel, E. (2012). *What is EDI and how does it work*. Hochschule Furtwangen University.

Shen, B., Guo, J., & Yang, Y. (2019). Medchain: Efficient healthcare data sharing via blockchain. *Applied Sciences*, *9*(6), 1207.

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, *97*, 101966.

Sousa, J., Bessani, A., & Vukolic, M. (2018). A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In *2018 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN)* (pp.51–58). IEEE.

Srivastava, G., Parizi, R. M., & Dehghantanha, A. (2020). The future of blockchain technology in healthcare internet of things security. In *Blockchain Cybersecurity, Trust and Privacy* (pp. 61–184). Springer, Cham: Springer.

Su, Q., Zhang, R., Xue, R., & Li, P. (2020). *Revocable attribute-based signature for blockchain-based healthcare system*. USA: IEEE Access.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media. https://www.oreilly.com/about/contact.html

Swan, M. (2018). Blockchain economics: Ripple for ERP. *European Finance Review*, *1*, 24–27.

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407.

Thorud, G. (1994). Message handling systems. *TELEKTRONIKK*, *90*, 86–86.

Tripathi, G., Ahad, M. A., & Paiva, S. (2020). S2hs-a blockchain based approach for smart healthcare system. In *Healthcare* (Vol. 8, pp. 100391). Elsevier. https://www.sciencedirect.com/science/article/abs/pii/S2213076419302532

Truong, N. B., Sun, K., & Guo, Y. (2019). Blockchain-based personal data management: From fiction to solution. In *2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)* (pp.1–8).

Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2020). GDPR-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security*, *15*, 1746–1761.

Turi, B. B. D. (1993). Security for EDIFACT messages. *Computers & Security*, *12*(5), 447–455.

Vasudevan, V. (2008). *Application security in the ISO27001 environment*. UK: IT Governance. https://www.itgovernancepublishing.co.uk/

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*, 1–27.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data* (pp. 557–564). BigData Congress.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352–375.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (pp. 180–184).