International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 14, Issue 12, 2020

A Blockchain Secured Electronic Transaction Document Interchange Architecture (DIA): A Public Sector Analysis from Thailand

Chaiporn Thoppae[a], Nivet Jirawichitchai[b] [a,b] Faculty of Information Technology Graduate School, Sripatum University, Bangkok, Thailand.
E-mail: [a]chaiporn.tho@gmail.com, [b]nivet.ch@spu.ac.th

Thailand like many other nations and governments has been plagued with countless incidents of corruption and inefficiency. However, even though the primary causes of these problems remain uncertain, there are methods available today to reduce the ongoing systemic problems. One of the potential solutions lies in using secure document interchange architecture (DIA) with blockchain technology. Using a quantitative research design and cluster sampling across 20 Thai ministries and related agencies, 500 individuals eventually participated in the study. A five-level scale questionnaire was used as the research instrument. The structural equation model (SEM) was analysed to validate the consistency of the empirical data. The results of the research indicated that after adjusting the SEM by increasing the relationship between the errors, the consistency with the empirical data of the model was very good. Of the eight hypotheses examined, all were found to be positive. However, social and cultural aspects (SCA) had the greatest positive influence on strategy/policies/legal approaches (SPL) (r = 0.72*). This was closely followed by SPL's influence on secure electronic transaction DIA (SET) (r = 0.68*), and technology (TEC) on security semantics (SEC) (r = 0.62*). However, SEC was deemed to have the least influence on secure electronic transaction DIA (SET) (r = 0.31*). Overall, there was a high level of satisfaction with the prototype system, with the architectural efficiency showing networked integrity while verifying and authenticating with the accuracy of the electronic documents. Also from the use of electronic signatures, electronic documents could be verified and authenticated as well. Networked integrity was also proven as the

DOI: 10.53333/IJICC2013/141254

DIA system could validate the accuracy and authenticity of electronic documents.

Keywords: *Blockchain, cybersecurity, e-government, e-transactions, electronic transaction, encryption, Thailand.*

Introduction

Globally, the need for secure systems supporting large and complex financial transactions, with high operational availability, has become a critical need for both the private and public sectors (Sangwan et al., 2020). Additionally, there needs to be great flexibility and interoperability between these systems and sectors and how they interface across international lines.

However, this vision is not new, as it was over a decade ago that a secure data framework was outlined in a regional initiative by the member states of the Association of Southeast Asian Nations (ASEAN). Referred to as the ASEAN Single Window (ASW) initiative, it was conceptualized as each ASEAN nation's ability to exchange and synchronize data across borders for the primary purpose of expediting cargo clearances and tighter economic integration. Some of the further benefits listed within the outline were improved risk management, track-and-trace capabilities, supply chain integration, pre-arrival clearance, harmonization of data and procedures, and, overall, improved trade facilitation and compliance (Benjelloun et al., 2012).

It can be noticed that a document interchange mechanism for electronic transactions in the public sector, in terms of integrating public sector services to increase efficiency and the system of public e-services in one channel (National Single Window) (Cataldo et al., 2018), are deprived of connectivity in public operations to be a single integrated organisation, as it was just connectivity and interchange basic data. This is not sufficient and requires international design standards due to a lack of integration of organisational connectivity, transparency, trust, and security.

Although digital economy policies and governance vary widely within countries, Thailand has been an innovator in the field (Bukht & Heeks, 2018), which recently created a new *Ministry of Digital Economy and Society* (MDES) to oversee implementations of these policies. Furthermore, a *National Digital Economy Master Plan* (NDEMP) was introduced which lays out Thailand's goals as '*five key pillars*', with pillar '3' described as '*soft infrastructure*' to drive its digital economy initiative (Collen & Kulikowski, 2015; Okeleke & Stryjak 2015). Under *Pillar 3*, public confidence is stated as the foundation to success. To achieve this, digital technology must ensure cybersecurity and verification systems to identify individuals and guarantee secure and trusted digital transactions (Siriruchatapong 2016). It must also be available as a tool to fight corruption.

DOI: 10.53333/IJICC2013/141254

This process will thus involve the modification and creation of all existing standards, regulations, and laws for e-transactions, data protection, and cybersecurity laws. In addition to electronic transaction promotion, the NDEMP also addresses trade facilitation with the usage of electronic document interchange architecture (DIA) (Bukht & Heeks, 2018).

Moreover, three approaches have been suggested as necessary in securing Thailand's new digital economy. There are a strategic approach, a policy lead approach, and a legal or regulatory approach. Thus, these have been added as a key latent variable to the research framework in Figure 1.

Blockchain

In the discussion of blockchain outlined by Raikwar et al. (2019), the authors suggested that the technology is both new and disruptive. They also described it as a distributed ledger managed by a peer-to-peer network collectively adhering to some consensus protocol. Also, the Engineering Institute of Thailand endorsed blockchain and stated it to be an efficient method of collecting data and accounting changes by using cryptography and the arrangement of the data entry in chronological order. The group of data will be published and distributed to all designated network users. At all times, all users will know the amendment and addition of all transactions in the blockchain.

Concept and Basic Working Principles of Blockchain

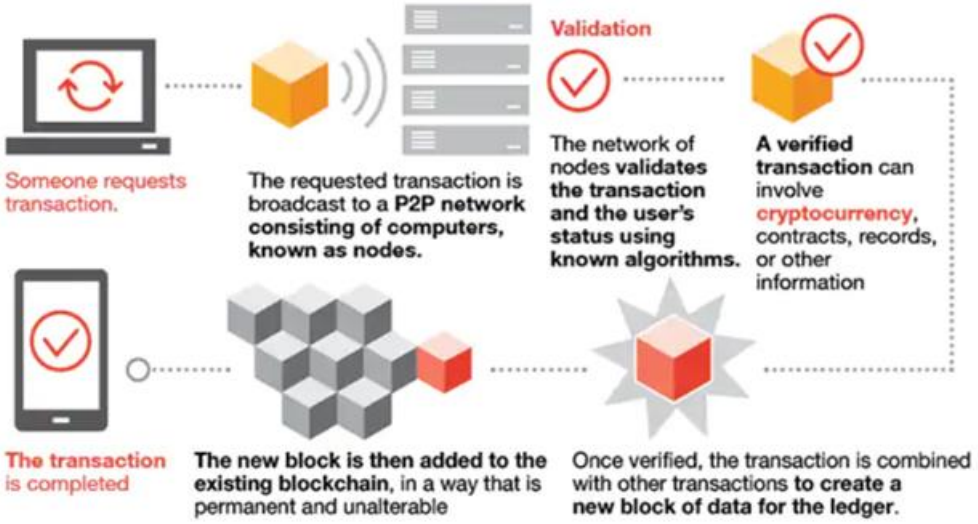
In 1970, Merkle (1988) proposed the Merkle Tree or Hash Tree to start developing blockchain and patented the concept in 1979. It is a tree structure in which every leaf node is labelled with the cryptographic hash of a data block, and every non-leaf node is labelled with the cryptographic hash in the labels of its child nodes. In 1991, Haber and Stornetta (1991) began to develop the concept of blockchain, and the Markle tree concept was combined in their concept and became '*blockchain*'. Nakamoto (2008) utilised this concept to invent cryptocurrency in 2008, which was designed as a global network for routing value without trusted intermediaries (Tierion, 2016). Also, according to Tapscott and Tapscott (2018), Sathosi Nakamoto's seven design principles of the blockchain economy are networked integrity, distributed power, value as an incentive, security, privacy, rights preserved, and inclusion.

Since then, although extremely controversial, bitcoin and other cryptocurrencies (based on blockchain) are being perceived by many as a 'store of value' (Campbell-Verduyn, 2018; Gladstein, 2021). Cryptocurrencies and Bitcoin are also seen as a mechanism to remove personal, corporate, or even national financial transactions from any regulatory oversight or sanctions (e.g. Iran and Venezuela) (Ciphertrace, 2021; Gladstein, 2021). There is also no need for a 'middle-man' (Figure 1). However, Bitcoin uses a massive amount of energy

DOI: 10.53333/IJICC2013/141254

(more than the entire country of Argentina) in supporting the networks data mining' and coin transaction clearing operations (Criddle, 2021), with energy use concerns having been voiced as problematic for other types of blockchain use operations such as for land title transfer (Ameyaw and de Vries, 2020).

Figure 1. How blockchain works



P2P = peer-to-peer Source: PWC. (2021).

Types of Blockchain and Potential Uses

Moreover, the taxonomy of the blockchain systems uses three main categories. These include a private, public, and consortium blockchain. In these environments, multitudes of situations exist for secure and trusted communications between end-users and/or government agencies.

As an example of where blockchain implementation would be quite useful, Santhanamery and Ramayah (2012) surveyed 1,000 Malaysian e-filing taxpayers in the five cities of Johor, Kuala Lumpur, Penang, Perak, and Selangor. They concluded that although there was a sense of trust due to the system being a federally controlled system, the taxpayers were still wary of how the data was transmitted and the underlying security of the connection and the database.

Bennett et al. (2021) investigated three blockchain Proofs-of-Concept (PoC) for 'smart contracts' in land management for three countries (Sweden, Australia, and Canada) from vastly different regions. In simple terms, the authors felt that placing an entire title or deed registry, and all related transactions and processes, on a blockchain system was fanciful, with full tokenisation of property in a given jurisdiction still likely to be many years away. However, it was suggested that smaller-scale, targeted applications using blockchain with specific land dealings might be more realistic and more useful in the land administration domain. However, in Thailand, a discussion is underway on how to use blockchain to '*tokenise*' large project property investments across a broad spectrum of potential investors.

DOI: 10.53333/IJICC2013/141254

Tokenising property projects have the potential to link ownership and its value, to a digital token (Srupsrisopa, 2019).

In a fascinating real-world report, Tierion (2016) published their blockchain healthcare project report after a year of working with some of the world's largest healthcare and insurance companies. In the report, the company stated that the key characteristics of blockchain include no central point of control, strong data integrity, high availability, and network-wide consensus. Remembering that the report was compiled in 2016, strong statements were given as to the problems of defining what blockchain was and regulatory issues concerning its use. Also, switching costs can be prohibitively high, thus it might be better to wait for established software vendors to integrate new technology than to try and build something from scratch. They concluded that over time they were optimistic about blockchain's impact, however, blockchain presents more pitfalls than promises in its early stages within the healthcare sector.

However, Meijer et al. (2017) saw more potential for blockchain use and a voting verification system based on machine-readable travel documents. Blockchain attributes were stated to entail a decentralized transaction ledger, where every transaction is immutable and built following predefined rules. They are also visible and verifiable for anyone connected to the decentralized network to see. Due to blockchain's decentralized design, the network is resilient against distributed denial-of-service (DDoS) attacks and has no single point of failure (Wani et al., 2021).

Document Interchange Architecture (DIA)

From a review of the literature concerning disruptive technology use (e.g. blockchain) and other information technologies used by Thai government agencies, we synthesised the needs for a secure electronic transaction (e-transactions) DIA as follows:

1. Facilitate and increase speed, a reduction of processing and transmission times, and a reduction in operating cost by government officials.
2. To elevate job tracking.
3. Build transparency in public service integration efficiently utilizing an information gateway (Thailand Gateway), an investment gateway, a trade gateway, a citizen gateway, a tourist gateway, and finally, a DIA which supports functions within the *Thailand national single window* (THAINSW) system (NSW, 2018). THAINSW simplifies both processes and documents associated with international trade transactions and provides a significant reduction in the number of processes, documents, and time required for completing regulatory requirements at borders. THAINSW has been estimated at saving Thailand's logistics costs of over $1.5 billion annually (UNECE, 2012).
4. To encourage government agencies to share and integrate agency data.

DOI: 10.53333/IJICC2013/141254

5. Encourage *government to business* (G2B) data integration such as in custom's clearance information.
6. Encourage *business to business* (B2B) data integration for both data input, and data output.

Concerning the aforementioned models of the operating-system structure, they are all centralised systems, while the secure e-transactions DIA system is available from government agencies to citizens (G2C).

Moreover, one of the most important developments in public-key cryptography implementation for the above systems was the Diffie-Hellman key exchange (Lake, 2019).

The Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange method was the first *publicly-used* (there was an early system developed used by British intelligence) mechanism that allowed users who have never met or prearranged a key to safely create and send messages to each other (Diffie & Hellman, 1976; Lake, 2019), over an insecure channel that adversaries may be monitoring. Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information (Smirnoff & Turner, 2019). The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, are used to encrypt and decrypt messages.

Electronic Signature

An electronic signature is an alphabet data set or '*bit string*' showing the credibility of digital documents that are signed in the form of digital signatures (Lupton, 1999). An asymmetric encryption process is used to create an electronic signature to reassure the receivers that the documents they receive are from actual senders. An electronic signature scheme typically consists of three algorithms, including signing, key generation, and signature verifying (Schellekens, 2004).

Based on the abovementioned reasons, the researcher is interested in studying document interchange architecture for secured e-transactions in public sectors by using blockchain technology. Therefore, after a review of the literature and theory, we present Figure 2 as a conceptual model for a secure electronic transaction DIA framework using blockchain technology to facilitate the sustainable development of Thailand's digital economy.

DOI: 10.53333/IJICC2013/141254

Research Objectives

RO1: To analyse a development *guideline* for a secure electronic transaction DIA framework in both Thailand and abroad.
RO2: To study the necessary factors affecting the *preparation* of a secure electronic transaction DIA framework in Thailand.
RO3: To *develop* a secure electronic transaction DIA framework for the public sector using blockchain technology in Thailand.
RO4: To *assess* a secure electronic transaction DIA framework for the public sector by using blockchain technology in Thailand.

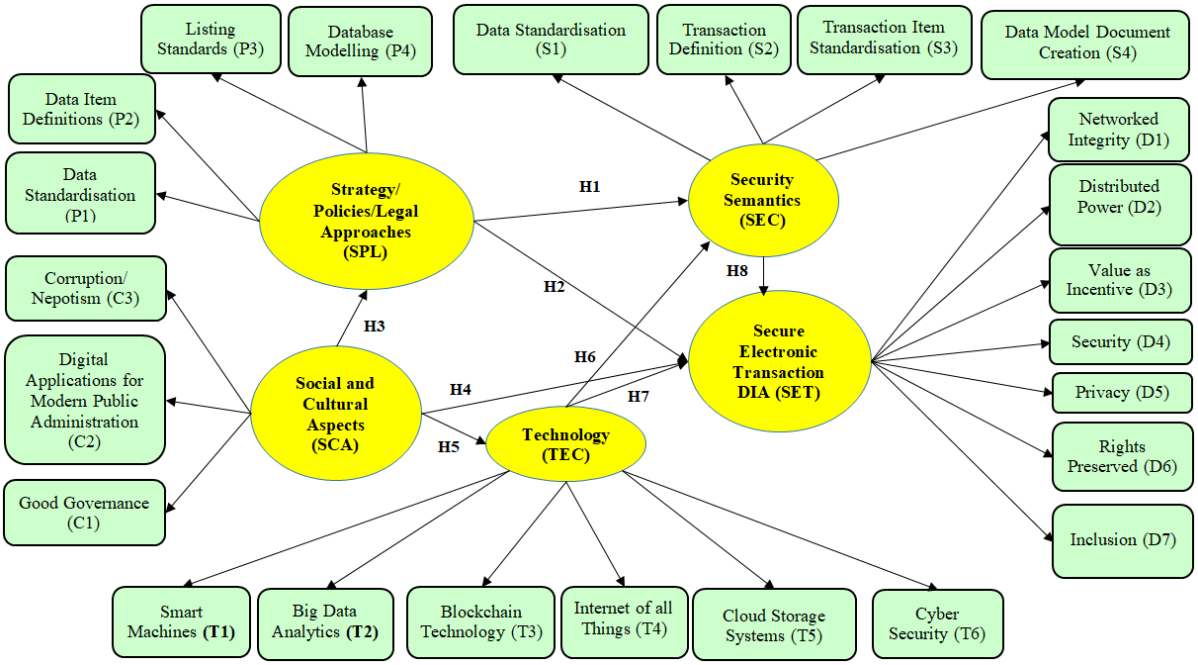
Conceptualization Hypotheses

From a review of the literature and related theory, we developed the following eight hypotheses as well as the conceptualized model in Figure 2.

H1: *Strategy/policies/legal approaches* (SPL) directly and positively influences *security semantics* (SEC).
H2: *Strategy/policies/legal approaches* (SPL) directly and positively influence *secure electronic transaction DIA* (SET).
H3: *Social and cultural aspects* (SCA) directly and positively influence *strategy/policies/legal approaches* (SPL).
H4: *Social and cultural aspects* (SCA) directly and positively influences *secure electronic transaction DIA* (SET).
H5: *Social and cultural aspects* (SCA) directly and positively influences *technology* (TEC).
H6: *Technology* (TEC) directly and positively influences *security semantics* (SEC).
H7: *Technology* (TEC) directly and positively influences *secure electronic transaction DIA* (SET).
H8: *Security semantics* (SEC) directly and positively influences s*ecure electronic transaction DIA* (SET).

DOI: 10.53333/IJICC2013/141254

Figure 2. The secure electronic transaction DIA conceptual framework



Methodology

The first stage involved qualitative research, the second stage involved quantitative research, then the try-out phase, and finally the performance assessment.

The Qualitative Research

A focus group was used to obtain in-depth interviews from 23 individuals concerning development guidelines for a Thai secure electronic transaction DIA framework using blockchain technology. Each member of the focus group was an organisational executive who had some form of expertise in digital technology and/or blockchain technology. Their position titles included electronic transaction specialist, organisational architecture specialist, cybersecurity specialist, blockchain technology specialist, digital economy specialist, digital technology specialist, and three other specialists in a related field. Furthermore, there were five information technology chief executives from five different ministries. The data obtained from the in-depth interviews used a content analysis in which seven keyword or phrases were used which included, 1) networked integrity (D1), 2) distributed power (D2), 3) value as incentive (D3), 4) security (D4), 5) privacy (D5), 6) rights preserved (D6), and 7) inclusion (D7) (Figure 2) ((Bukht & Heeks, 2018; Tapscott & Tapscott, 2018; Wladawsky-Berger, 2016).

DOI: 10.53333/IJICC2013/141254

Population and Sample

The population for the study included staff and executives from 20 Thai ministries and their related agencies. These included the Thai office of the Food and Drug Administration (FDA), Hatyai Hospital, Srinakarin Hospital, Songkhlanagarind Hospital, Directorate of Joint Communications, Royal Thai Army, National Intelligence Agency, and CAT Telecom Public Co. Ltd, as well as other related agencies.

The sample was selected using a non-probability sampling method with purposive sampling to serve the appropriateness of the research, in which specialists were randomly selected from 20 ministries and their related agencies until 500 persons were obtained to participate in the study. These individuals were then classified into three groups from the 20 targeted Thai ministries, departments, and agencies.
Group 1 – Chief executives and other executives.
Group 2 - Digital technology support officers who performed duties related to technology management and technology support.
Group 3 - Officers and employees who provided services to people outside their respective Thai ministries, departments, and agencies.

As soon as the DIA was obtained, an experimental workshop at the Thai office of the FDA in Nonthaburi province was conducted.

Results

The researcher studied and collected fundamental data related to the study subject to formulate a guideline to develop a DIA framework. The results were reported in accordance with the research objectives.

Guidelines Analysis Results (RO1)

The results from the qualitative research, which comprised studying related data, theories, and research studies, including data from the in-depth interviews with specialists, were analysed. From this, 24 observed variables and 5 latent variables were identified for further study (Figure 2) and analysis (Figure 3).

Preparation and Goodness-of-Fit (GOF) Results (RO2)

This phase of the research entailed using a survey research technique. After the model was adjusted by increasing the relationship between the errors in the model, the outcome revealed that the SEM was consistent with the empirical data to a high degree (Figure 3). Furthermore, from the GOF shown in Table 1, it was determined that the data was consistent with the modelling.

DOI: 10.53333/IJICC2013/141254

Table 3: Criteria and theory of the values of goodness-of-fit (GoF) appraisal

Criteria Index	Criteria	Supporting theory	Values	Results
Relative Chi-square: $\chi 2/df$	≤ 2.00	(Sahoo, 2019)	0.91	passed
RMSEA	≤ 0.05	(Jöreskog et al., 2016)	0.00	passed
GFI	≥ 0.90	(Schumacker & Lomax, 2016)	0.99	passed
AGFI	≥ 0.90	(Schumacker & Lomax, 2016)	0.97	passed

Furthermore, correlation coefficient (*r*) strength values have frequently been assessed by using a scale in which the absolute value of *r* from 0.00 - 0.19 is regarded as very weak, 0.20 - 0.39 as weak, 0.40 - 0.59 as moderate, 0.60 - 0.79 as strong and 0.08 - 1.00 as a very strong correlation (Pimdee, 2020). However, these scales are rather arbitrary and should be considered within the context of the total results.

Therefore, from the structural equation modelling results shown in Figure 3, we can interpret that from the eight hypotheses proposed, H3 (r = 0.72*) showed the strongest relationship (SCA to SPL). This was followed by H2 (r = 0.68*) and the strong relationship between SPL and SET, then H6 (r = 0.62*) a strong relationship between TEC and SEC. Also, there were moderately strong relationships in H5 (r = 0.55*) between SCA and TEC as well as in H7 (r = 0.52*) between TEC and SET. However, the SEM showed that both hypotheses H4 and H8 had somewhat weak relationships as in H4 r = 0.40* between SCA and SET and in H8 r = 0.31* between SEC and SET. Moreover, additional analysis showed an indirect and positive effect between SPL and SET through SEC. There was also an indirect and positive effect between SCA and SET through SPL. Finally, a third positive but indirect relationship between TEC and SET existed through SPL.

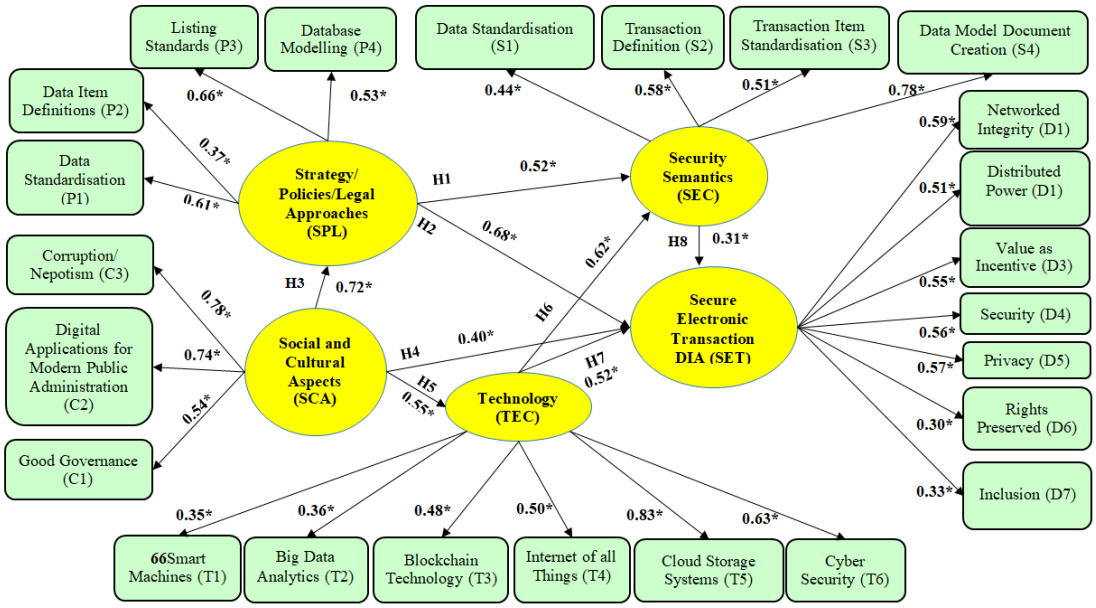
Table 2. Results of the hypotheses testing on secure electronic transaction DIA (SET) in Thailand

Hypotheses	*r*	Validity
H1: *Strategy/policies/legal approaches* (SPL) directly and positively influences *security semantics* (SEC).	0.52*	valid
H2: *Strategy/policies/legal approaches* (SPL) directly and positively influence *secure electronic transaction DIA* (SET).	0.68*	valid
H3: *Social and cultural aspects* (SCA) directly and positively influence *strategy/policies/legal approaches* (SPL).	0.72*	valid
H4: *Social and cultural aspects* (SCA) directly and positively influences *secure electronic transaction DIA* (SET).	0.40*	valid
H5: *Social and cultural aspects* (SCA) directly and positively influences *technology* (TEC).	0.55*	valid
H6: *Technology* (TEC) directly and positively influences *security semantics* (SEC).	0.62*	valid
H7: *Technology* (TEC) directly and positively influences *secure electronic transaction DIA* (SET).	0.52*	valid
H8: *Security semantics* (SEC) directly and positively influences *secure electronic transaction DIA* (SET).	0.31*	valid

*= $p \leq .05$, *r* = correlation coefficient

DOI: 10.53333/IJICC2013/141254

Figure 3. Secure electronic transaction DIA final model



Development Guidelines Results (RO3)

From the findings of which factors have the greatest influence on SET, it was determined that *networked integrity* (D1) was viewed as the most crucial factor (r = 0.59*). This was followed closely by *privacy* (D5), *security* (D4), and *value as incentive* (D3) with correlation coefficient values of 0.57*, 0.56*, and 0.55*, respectively. Further back, but yet moderately strong, was *distributed power* (D1) with an r = 0.51*. However, both *inclusion* (D7) and *rights reserved* (D6) with values of r = 0.33* and r = 0.30* (respectively), considered weak.

We find commercial support for these findings in the knowledge that over 50 million Bill of Ladings (B/L) are created each year. From these, there is an average cost of $100 per B/L document for courier use, representing $5 billion per year (CargoX, 2021). Additionally, a courier service averages 5-10 business days to get these B/L documents from the origin to the destination. From the use of blockchain technologies, nearly all these costs and time loss can be eliminated (UNECE, 2012).

Armed with these results and the potential for large cost and time savings, permission was granted to implement a test-bed DIA system in Thailand's FDA. Therefore, the first step was to connect the FDA information system (IS) to external agencies (Figure 4). Users were instructed on the new system and sign-in procedures to the various other FDA systems.

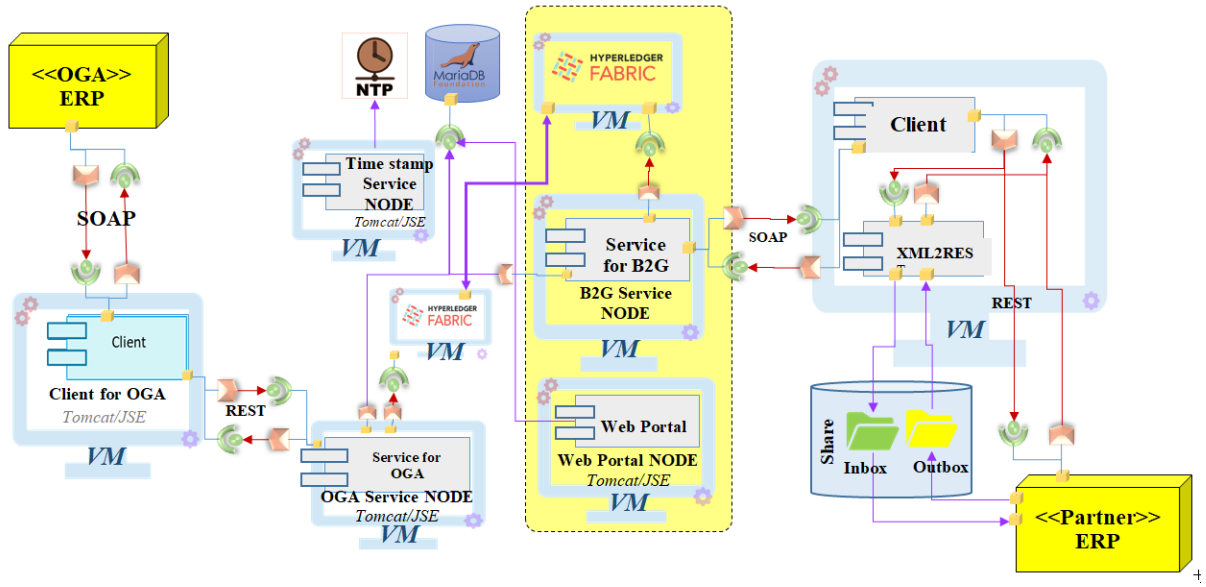
Furthermore, it was determined from previous blockchain studies that there needed to data standardisation (P1), data definitions (P2), listing standards (P3), and database modeling (P4), as these items were an ongoing concern in blockchain implementations (Tierion, 2016). Moreover, we saw the need to assure any blockchain implantation assured access equality,

DOI: 10.53333/IJICC2013/141254

thus creating greater opportunity for the system's users (Tapscott & Tapscott, 2018; Wladawsky-Berger, 2016).

Any proposed blockchain DIA also needs to provide services conveniently and speedily (UNECE, 2012). Additional benefits include the potential to reduce corruption and intervention (Fuangswasdi, 2019) since the system is designed so that a group of transactions occurring in a blockchain cannot be altered, as the data standards are compliant with international security and data exchange standards (Meijer et al., 2017). Moreover, the definitions of transactions are set, as well as the document information models. The organisational users must also have access to smart *virtual machines* (VM), blockchain systems, cloud-based data storage systems, and big data analytics, including the *Internet of things* (IoT) (Petcharit et al., 2020), and knowledge of cybersecurity principles.

Figure 4. The test-bed architecture of the prototype DIA for secured electronic transactions from within the FDA and external public agencies using blockchain technology



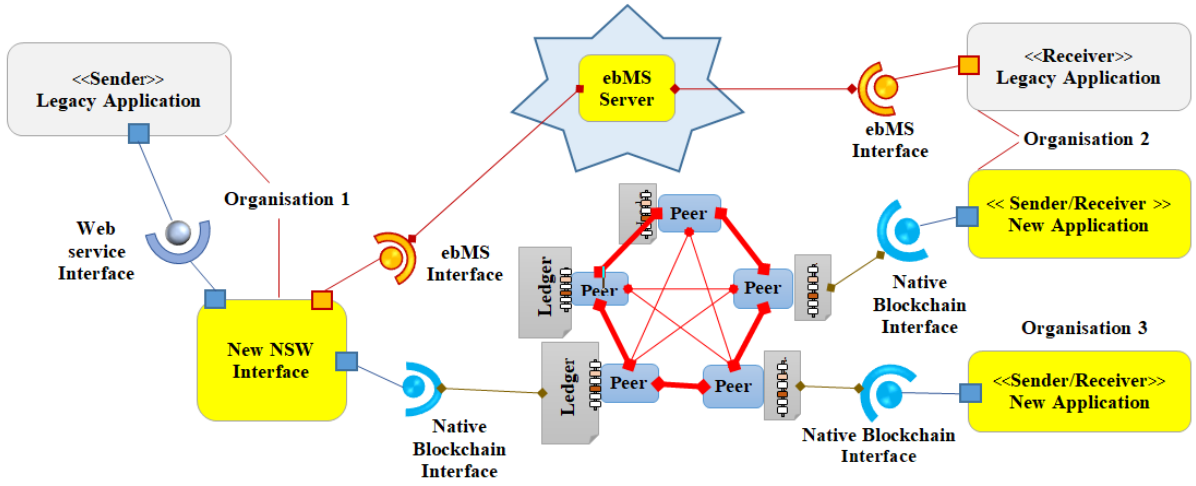
Note. B2G = business to government, SOAP = Simple Object Access Protocol, VM = virtual machine, ERP = enterprise resource planning, OGA = Other Government Agency, OBA - Other Business Agency

Based on the information above, the created architecture shall cover and focus on networked integrity and security. The details of the overall architecture are outlined as follows:

The created FDA DIA is connected to a National Single Window (NSW) network through which data is sent using an electronic business eXtensible Markup Language (ebXML) Messaging Services (ebMS) gateway between the FDA DIA and the external agencies. In this regard, blockchain technology can be used with an ebMS gateway, as shown in Figure 5.

DOI: 10.53333/IJICC2013/141254

Figure 5. Diagram of the data linking system of the Thai FDA based on electronic business eXtensible Markup Language (ebXML) standard.



The architecture uses an *advanced encryption standard* (AES), where the secret key length must be at least 256 bits (AES-256) or uses other encryption algorithms consistent with the US *Federal Information Processing Standard* (FIP) 140-2, which have the security of no less than AES-256 with SHA-2 or SHA-3 hash function algorithms that have a security length of at least 256 bits (NIST, 2001).

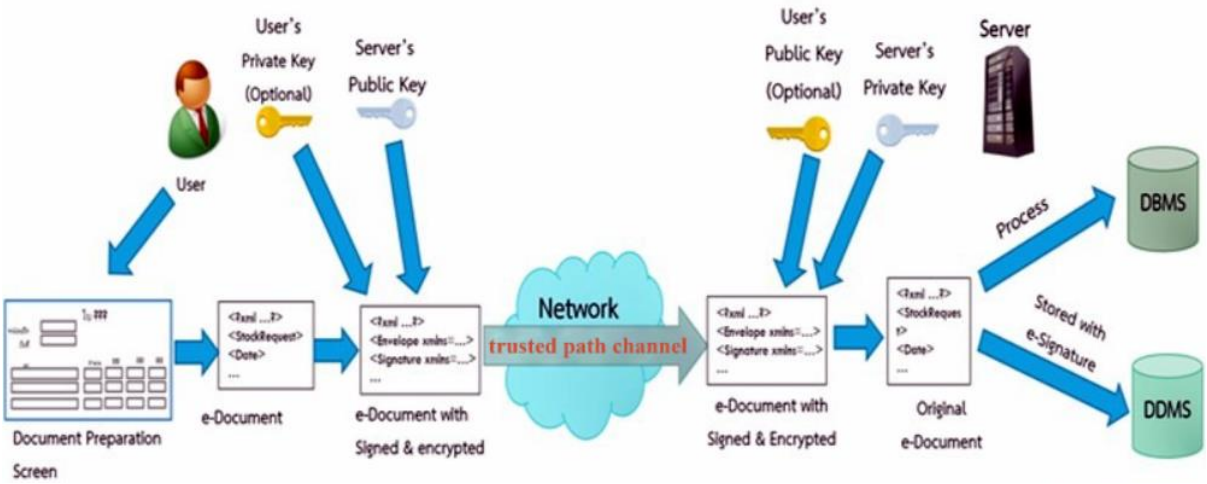
The DIA Key Exchange and Electronic Signature

The developed software in the proposed blockchain-based DIA will not send users' codes and/or passwords over the plain text network. The key exchange must require the Diffie-Hellman algorithm (Diffie & Hellman, 1976; Lake, 2019), or IKE or ECDH because the architecture was designed to create a cryptographic key for security consistent with the National Institute of Standards and Technology (NIST, 2019) '*Annex C: Approved Random Number Generators for FIPS PUB 140-2*'.

Furthermore, since electronically signed documents have now achieved the same legal validity as those signed with pen and paper, the proposed system also allows electronic signatures (Figure 6). Additionally, the DIA serves as an inspection of electronic documents to ensure they are sent from the correct destination, with electronic signatures working in conjunction with document encryption.

DOI: 10.53333/IJICC2013/141254

Figure 6. Electronic signature and encryption for a digital document management system



Thus, the connection model between the FDA DIA system and external partners is divided into four functional layers as follows:

Layer Four – At this bottom layer, the system prepares the most important data in an eXtensible Markup Language (XML) format and encrypts it with the paired key that the FDA created for encryption. This key is then passed up to *layer three*.

Layer Three – Although '*layer three*' communicates important data, special encryption is not required, as layer three brings the encrypted data from '*layer four*' to supplement and prepare for the base64 encoded data that is used by '*layer two*'.

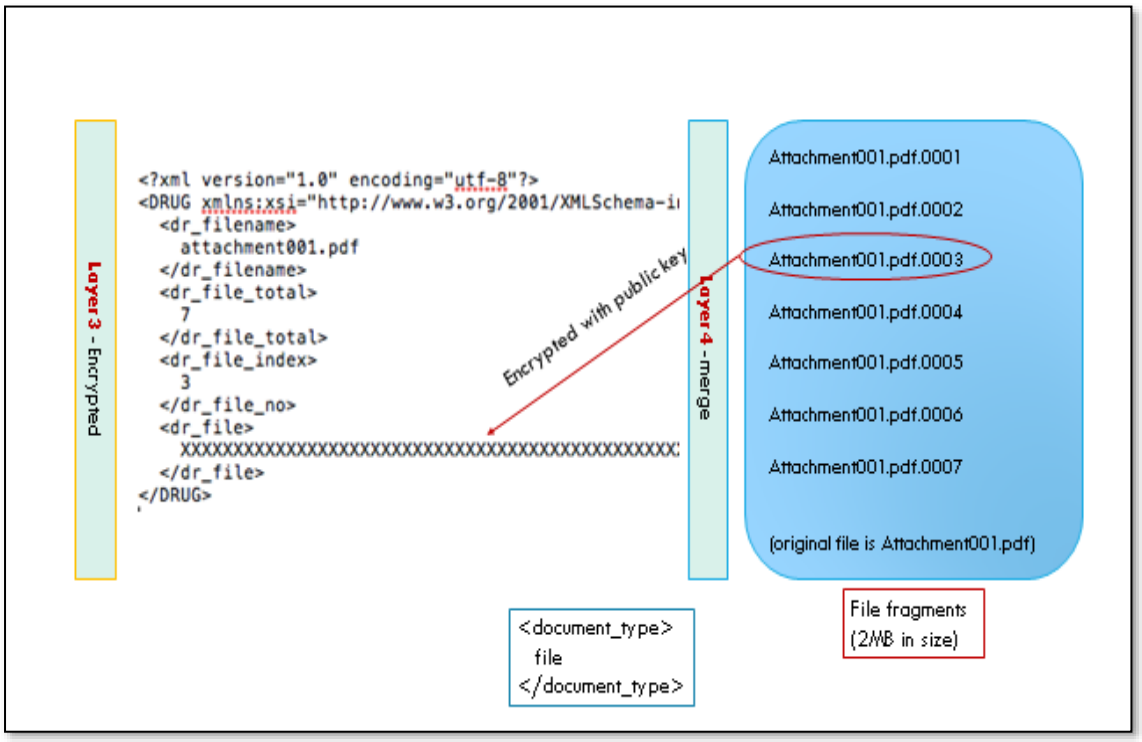
Layer Two – At '*layer two*', data is brought from the '*layer three*' for electronic signature and electronic authentication in preparation for the base64 encoded data needed for 'layer one'.

Layer One – The top and final layer is '*layer one*', which brings the data from 'layer two' and prepares it base64 encryption. It then sends it to an encrypted channel (trusted path) for use again at the network level by public and private keys.

Please note, in the instance that the sent data is an attached document, layers four and three shall follow the models shown in Figure 7.

DOI: 10.53333/IJICC2013/141254

Figure 7. Layer Four and Layer Three in the scenario that an attached document is available



Performance Assessment (RO4)

From the experts and specialists who were assigned to assess the system and its efficiency, it was determined that their overall opinions had a mean of 3.86, with the standard deviation (SD) at 0.82. Moreover, it was found that the architectural efficiency showed networked integrity and the system could verify the accuracy and the authenticity of the electronic documents.

Also, the *XML Schema* that was employed was shown to be able to validate an XML document. Also, after electronic signatures were used to certify electronic documents, it was verified that the documents which were sent from the correct destination achieved a high degree of authenticity (mean = 3.66, SD = 0.64).

Regarding networked integrity (D1= r = 0.59*), it is provided that the system can validate the accuracy and authenticity of electronic documents. The *XML Schema* was employed to validate XML documents. An electronic signature was available to certify electronic documents, ensuring that they are sent from the correct destination. There was a mechanism to verify that the original data was not amended and to trace back sources of data. Tapscott and Tapscott (2018) have noted that *trust is intrinsic, not extrinsic*, with D1 being a process that encodes integrity in every step of the process and distributes it.

DOI: 10.53333/IJICC2013/141254

In Thailand, Pongnumkul et al. (2020) explored a proof-of-concept (PoC) for a blockchain that enables a land documentation registration system. The PoC determined the PoC was viable with 26 transactions per second possible. In Ghana, Ameyaw and de Vries (2020) also explored the use of blockchain in land administration, but instead focused on transparency. They also highlighted the problems with limited storage and scalability, as well as the huge electricity consumption requirements.

Tapscott and Tapscott (2018) summarised the issue of blockchain and privacy (D5= r = 0.57*), with the idea that individuals should control their data. They also have a right to decide what, when, how, and how much about their identities to share with anybody else.

In terms of security (D4= r = 0.56*), the system was judged as being able to provide a high level of data security that met international security and encryption standards (mean = 3.94, SD = 0.85). Elements of this included being able to identify individual authentication, keep confidentiality, validate accuracy and authenticity of electronic documents, validate and prevent rejection responsibility for electronic document preparation, store logs, and provide data encryption for security (which requires a digital signature to ensure security and trust between senders and receivers) to a high degree. Finally, safety measures are embedded in the blockchain network with no single point of failure, and they provide not only confidentiality but also authenticity and nonrepudiation to all activity (Tapscott & Tapscott, 2018),

In the instance that other users are joint owners, it is essential to be granted permission from the joint owners to ensure that the information is protected with high security and transparency. From the research, blockchain technology was used to protect, store, and share personal information regardless of a middleman (Fuangswasdi, 2019), such as Thailand's Office of Population Registration.

Conclusion

This paper set out to identify the essential elements and relations in the use of blockchain in the development of a secure electronic transaction DIA for Thai public organizations. Supplementing the detailed technical and literature review, 23 experts were assembled to provide insight into the development of the study's design and questionnaire (RO1).

After which, a sample from 500 individuals in 20 Thai ministries and related agencies gave their professional insight into what elements were best suited and most important in a blockchain e-transaction DIA in Thailand (RO2).

From this input, of the eight hypotheses examined, all were found to be positive with social and cultural aspects (SCA) having the greatest positive influence on strategy/policies/legal approaches (SPL) (r = 0.72*). This was closely followed by SPL's influence on secure

DOI: 10.53333/IJICC2013/141254

electronic transaction DIA (SET) (r = 0.68*), and technology (TEC) on security semantics (SEC) (r = 0.62*). However, SEC was deemed to have the least influence on secure electronic transaction DIA (SET) (r = 0.31*) (RO3).

In the final phase of the study, the performance assessment (RO4), overall there was a high level of satisfaction with the prototype system which used a secure e-transaction DIA system based on blockchain with the Thai FDA system. Moreover, the architectural efficiency showed networked integrity and the system could verify the accuracy and the authenticity of the electronic documents. Also from the use of electronic signatures, electronic documents could be verified and authenticated.

Networked integrity was also proven as the FDA DIA system could validate the accuracy and authenticity of electronic documents. If Thailand designs blockchain systems for integrity, power, value, privacy, security, rights, and inclusion, then Thailand will be redesigning its economy and social institutions to be worthy of its citizens' trust.

DOI: 10.53333/IJICC2013/141254

REFERENCES

Ameyaw, P. D., & de Vries, W. T. (2020). Transparency of land administration and the role of blockchain technology, a four-dimensional framework analysis from the Ghanaian land perspective. *Land, 9*(12), 491. https://doi.org/10.3390/land9120491

Benjelloun, R, Pantastico, D., & Wong, M. (2012). Cross-border E-Trade: The ASEAN Single Window. UN ESCAP. https://tinyurl.com/4of8x4mn

Bennett, R, Miller, T, Pickering, M, & Kara, A-K. (2021). Hybrid approaches for smart contracts in land administration: Lessons from three blockchain proofs-of-concept. *Land, 10*(2), 220. https://doi.org/10.3390/land10020220

Bukht, R., & Heeks, R. (2018). Digital economy policy: The case example of Thailand. https://tinyurl.com/x00652j0

Campbell-Verduyn, M. (Ed.) (2018). Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance, RIPE Series in Global Political Economy. Taylor & Francis Group. https://tinyurl.com/54evm2ze

CargoX. (2021). https://cargox.io/solutions/for-transport-and-logistics/

Cataldo, A., Ferrer, J.-C., Rey, P. A., & Sauré, A. (2018). Design of a single window system for e-government services: the chilean case. *Journal of Industrial & Management Optimization, 14*(2), 561 – 582. https://doi.org/10.3934/jimo.2017060

Collen M. F., & Kulikowski C. A. (2015) The development of digital computers. In M. Collen & M. Ball M. (Eds.), *The History of Medical Informatics in the United States. Health Informatics*. Springer. https://doi.org/10.1007/978-1-4471-6732-7_1

Ciphertrace. (2021, February). Cryptocurrency crime and anti-money laundering report. https://tinyurl.com/ywm522wf

Criddle, C. (2021). Bitcoin consumes 'more electricity than Argentina'. *BBC*. https://tinyurl.com/3hkycucl

Diffie, W., & Hellman, M. E.. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644 – 654. https://tinyurl.com/yph3ug4v

Fuangswasdi, K. (2019). Blockchain – A corruption killer. *Suthiparithat, 33*(106), 92 – 106. https://tinyurl.com/24gxa2ep

Gladstein, A. (2021, February 21). Can governments stop Bitcoin? *Quillette*. https://quillette.com/2021/02/21/can-governments-stop-bitcoin/

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology, 3*, 99 – 111. https://doi.org/10.1007/BF00196791

Jöreskog, K. G., Olsson, U. H., & Fan, Y. W. (2016). *Multivariate analysis with LISREL*. Springer.

Lake, J. (2019, March 15). What is the Diffie–Hellman key exchange and how does it work? *Comparitech.* https://tinyurl.com/q0tjyaxp

Lupton, W. E. (1999). The digital signature: Your identity by the numbers. *Richmond Journal of Law and Technology, 6*(2), Article 7. https://core.ac.uk/download/pdf/232774639.pdf

Meijer, W. K., Middendorp, D., Raes,J. M., & Tubbing, R. (2017). Digital voting pass.

DOI: 10.53333/IJICC2013/141254

[Published Thesis, Delft University of Technology]. Netherlands. https://tinyurl.com/pxs9vj0y

Merkle, R. C. (1988). A digital signature based on a conventional encryption function. In C. Pomerance (Ed.), *Advances in Cryptology — CRYPTO '87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293* (pp. 369-378). Springer. https://doi.org/10.1007/3-540-48184-2_32

Nakamoto, S. (2008). Bitcoin: A peer to peer electronic cash system. https://bitcoin.org/bitcoin.pdf

NIST. (2001, May 25). Security requirements for cryptographic modules. https://csrc.nist.gov/publications/detail/fips/140/2/final

NIST. (2019, June 10). *Annex C: Approved Random Number Generators for FIPS PUB 140-2,Security Requirements for Cryptographic Modules*. National Institute of Standards and Technology. https://tinyurl.com/1j6kp8bu

NSW. (2018, August 8). Thailand national single window & ASEAN single window. https://tinyurl.com/3dps588j

UNECE. (2012). Interagency collaboration for single window implementation: Thailand's experience. http://tfig.unece.org/cases/Thailand.pdf

Okeleke, K. & Stryjak, J. (2015). *Building digital societies in Asia*. GSMA. https://tinyurl.com/tyadyffp

Petcharit, A., Sornsaruht, P., & Pimdee, P. (2020). An analysis of total quality management (TQM) within the Thai auto parts sector. *International Journal of Online and Biomedical Engineering*, *16*(2), 131 – 144. https://doi.org/10.3991/ijoe.v16i02.11917

Pimdee, P. (2020). Antecedents of Thai student teacher sustainable consumption behavior. *Heliyon*, *6*(8), e04676. https://doi.org/10.1016/j.heliyon.2020.e04676

Pongnumkul, S., Khonnasee, C., Lertpattanasak, S., & Polprasert, C. (2020). Proof-of-concept (PoC) of land mortgaging process in blockchain-based land registration system of Thailand. *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology*. https://doi.org/10.1145/3390566.3391669

PWC. (2021). Making sense of bitcoin, cryptocurrency and blockchain. https://tinyurl.com/y8fb3jtt

Raikwar, M., *Gligoroski*, D., & K*ralevska, K.* (2019), SoK of used cryptography in blockchain. *IEEE Access 7*, 148550 – 148575. https://doi.org/10.1109/ACCESS.2019.2946983

Sahoo, M. (2019). Structural equation modeling: Threshold criteria for assessing model fit. In R. N. Subudhi & S. Mishra (Eds.), *Methodological issues in management research: Advances, challenges, and the way ahead* (pp. 269-276.). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78973-973-220191016

Sangwan, R. S., Kassab, M., & Capitolo, C. (2020). Architectural considerations for blockchain based systems for financial transactions. *Procedia Computer Science, 168*, 265 – 271. https://doi.org/10.1016/j.procs.2020.02.252

Santhanamery, T., & Ramayah, T. (2012). Continued usage intention of e-filing: The role of optimism bias. *Procedia - Social and Behavioral Sciences, 65*(1), 397 – 403.

DOI: 10.53333/IJICC2013/141254

https://doi.org/10.1016/j.sbspro.2012.11.140

Schellekens, M. H. M. (2004). Electronic Signatures: Authentication Technology from a Legal Perspective. T.M.C. Asser Press.

Schumacker, R. E., & Lomax, R. G. (2016). *A beginner's guide to structural equation modeling*. (4th ed.). Routledge.

Smirnoff, P., & Turner, D. M. (2019, January, 18). Symmetric Key Encryption - why, where and how it's used in banking. *Cryptomathic*. https://tinyurl.com/o7pgti1g

Siriruchatapong, P. (2016). *Thailand digital economy and society development plan*. MICT. https://tinyurl.com/1w21wxbt

Srupsrisopa, J. (2019, August 6). Blockchain and real estate. *Bangkok Post*. https://tinyurl.com/p7kwy3tz

Tapscott, D., & Tapscott, A. (2018). *Blockchain revolution: How the technology behind Bitcoin and other cryptocurrencies is changing the world*. Penguin Pub.

Tierion. (2016, October 5). *Blockhain Healthcare 2016 Report – Promise & Pitfalls*. https://tinyurl.com/1vwmctuy

Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K. M., Almotairi, S., & Gulzar, Y. (2021). Distributed denial of service (DDoS) mitigation using blockchain—A comprehensive insight. *Symmetry*, *13*(2), 227. https://doi.org/10.3390/sym13020227

Wladawsky-Berger, I. (2016, August 24). Blockchain as 'Technological Genie'. *The Wall Street Journal*. https://www.wsj.com/articles/BL-CIOB-10390

DOI: 10.53333/IJICC2013/141254