DIPONEGORO JOURNAL OF MANAGEMENT *Volume 11 Nomor 3 Tahun 2022, Halaman 1*
https://ejournal3.undip.ac.id/index.php/djom/index ***ISSN (Online): 2337-3792***

CONVINCING SUPPLIERS TO ACCEPT BLOCKCHAIN IMPLEMENTATION WITHIN SUPPLY CHAIN BY SOLVING THEORETICAL OBSTACLES USING BLOCKCHAIN-RELATED TRUST ATTRIBUTES: A STUDY CASE OF VEHGRO B.V

Muhammad Emyr Gunawan Rahmatullah, Mahfudz[1]

Emyrgunawan45@gmail.com

Departemen Manajemen Fakultas Ekonomika dan Bisnis Universitas Diponegoro
Jl. Prof. Soedharto SH Tembalang, Semarang 50239, Phone: +31644977054

ABSTRACT

Supply chain industries are involved with a lot of transactions concerning various parties. To maintain a relationship between wholesalers and suppliers, each party should have trust in the transaction. Which mean that the wholesalers should believe that the suppliers will be capable and credible to fulfil their responsibility in the transaction, while suppliers should believe that wholesalers will not misuse the information shared when doing transaction for instance, infer wholesale pricing strategies and other supplier parameter that could be used to manipulate future negotiation. In this research, currently VehGro rely on third party to check on the obligation of their supplier and they put their trust mainly based on personal connection that the CEO had with the supplier. Hence, they are thinking to implement blockchain in their operation as a platform that is seen to be able further enhance the trust in their business transaction. This research aims to help an organic food wholesaler, Vehgro, convince their suppliers to accept their blockchain implementation plan within the supply chain process. This research uses the framework of blockchain-related trust attributes to address this issue.

After conducting qualitative research based on the blockchain-related trust attributes derived from Kochovski Model by looking through literature and interview with a half-structured with CEO of VehGro, Blockchain Expert, and Information System Expert, the author found out that blockchain does contribute to trust, especially its capability to be traceable and immutable that are not seen on the current system used by VehGro. However, not all blockchains are suitable for supply-chain, the only appropriate type of blockchain is permissioned blockchain. In addition, to ensure privacy and security of the blockchain system, the system should be built with viewing keys or private smart contract. Furthermore, to make sure that information shared within the blockchain is credible, the blockchain system should allow users to add correction data on top of wrong data. Moreover, to make suppliers switch to the new system, it is advised to make an incentive plan that can be achieved by creating a token inside the blockchain with a particular utility. Next alternative is to also put into account a possibility of better public image due to implementation of blockchain that will give a feeling that the supply chain environment is secure and credible. Other possibility is creating a hybrid system with a mixture of the current operating system and some part of the blockchain system to make it easier for people to accept the change. In the end, the system that will be implemented should make everything easier and bring advantage over the previous ones, not the other way around.

[1] *Corresponding author*

Keywords: Supply Chain, Blockchain Implementation, Organic Food, Trust

INTRODUCTION

In recent years, blockchain has been quite a hot topic of discussion for researchers. They start to think on its implementation possibility throughout several sectors of business, and one of the segments aimed at is its implementation on supply chain management. Blockchain has already started to help solve the issue of trust and open participation when dealing with process related to management of product supply information, product lifecycle, and transport history (Yousuf & Svetinovic, 2019).

In this research, the writer is given a task by his company coach Mr. Kees Tesselhof to help VehGro B.V, an international wholesaler specializing in importing, exporting, and distributing natural food and care products (Vehgroshop, 2021) in the implementation of a blockchain system for their supply chain process.

VehGro as a wholesaler of organic products in the Netherland specializing in importing, exporting, and distributing exclusive natural food and natural care products, came from their worldwide network of regional products. They wish to deliver healthy, high-quality products and strive for sustainable and trusting partnerships with their stakeholders. They perceive quality as something that should be comprehensible and traceable (Vehgroshop, 2021). In accordance with the value that VehGro is trying to deliver, these recent years, consumers themselves are starting to increasingly value the origin of products and foodstuff that they order (Shahid, A., Almogren, A., Javaid, N., Al-Zahrani, F. A., Zuair, M., & Alam, M., 2020). This means that unnecessary links and processes on the supply chain will harm the business more than good. As an organic food wholesaler that handles the movement of natural products, they need to be exactly aware of their product origin, how it is handled, how long the transportation will be, and the stock availability (or more) (Hilten, M., Ongena, G., & Ravesteijn, P., 2020) as they wish to offer an honest story about the product to the customer (Vehgroshop, 2021). In relation to quality perceived by VehGro and the consumer's demand about the knowledge of their product across the supply chain process, they are going to implement blockchain because it offers similar attributes such as transparency and traceability (Shrier, D., Wu, W., & Pentland, A., 2016) that could help VehGro to attain their mission. However, the project has been halted due to several reasons. One of the reasons is that they need to convince their suppliers to switch to the blockchain system.

This research aims to help VehGro convince supplier to accept the usage of blockchain system that they are going to implement by eliminating or reducing the (theoretical) cause of supplier distrust toward blockchain implementation that is addressed on the fishbone diagram that related with blockchain system and the credibility of information. Therefore, the researcher comes up with the following research questions.

Main research question:
What (theoretical) obstacles must be solved in order to convince suppliers to implement Block Chain application of VehGro?

Sub research question:

- RQ1. What type of blockchain is suitable for the supply chain?
  This question will be asked in accordance with the related attributes of trust and blockchain, which are traceability and transparency.
- RQ2. What kind of blockchain feature should be added to ensure the privacy and security of blockchain users?

This question will be asked in accordance with the related attributes of trust and blockchain, which are privacy and security.

- RQ3. What kind of blockchain feature should be added to ensure the credibility of information inside the blockchain?

  This question will be asked in accordance with the related attributes of trust and blockchain, which is credibility.

These questions will be answered using conceptual model that is going to be explained in the theoretical framework

THEORITICAL FRAMEWORK AND HYPOTHESIS DEVELOPMENT

In order to answer main research question of what theoretical obstacles should be solved to help VehGro convince their supplier to accept the implementation of Blockchain system in their supply chain process, researchers will start by making an operationalization based on conceptual model derived from previous research on similar topic. That will be followed by literature review related to the operationalization.

Conceptual Model

In this research we will discuss the attributes of blockchain related to trust derived from the conceptual model in Figure 2.1 to help solve the research question.

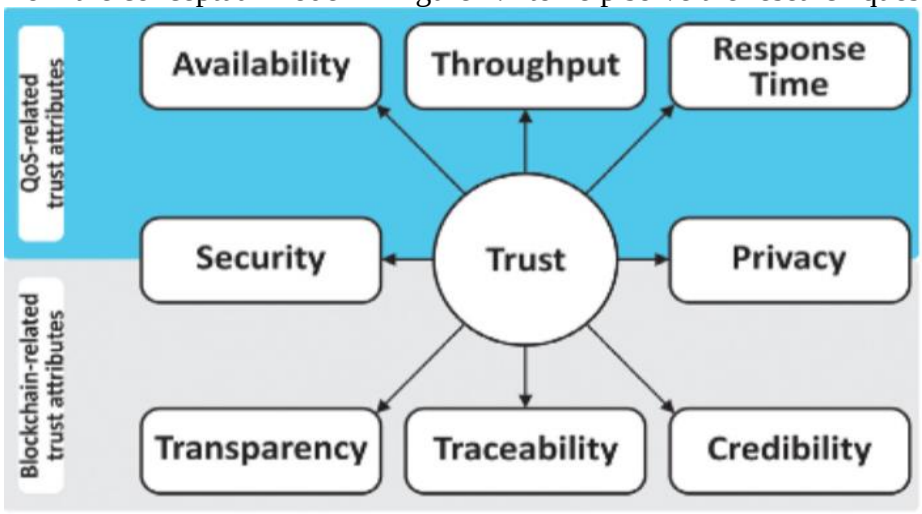

Figure 2.1 Trust Attributes in relation to blockchain and Quality of Service (Kochovski P., Gec, S., Stankovski, V., Bajec, M., & Drobintsev, P. D., 2019)

There are several attributes of trust that are related to quality of service and blockchain namely availability, throughput, response time, security, privacy, transparency, traceability, and credibility. However, because this research is about the blockchain implementation thus researchers will only use the blockchain related trust attributes. Therefore, the researcher uses the following figure 1.4 that are derived from figure 1.3 to show the focus of the research.

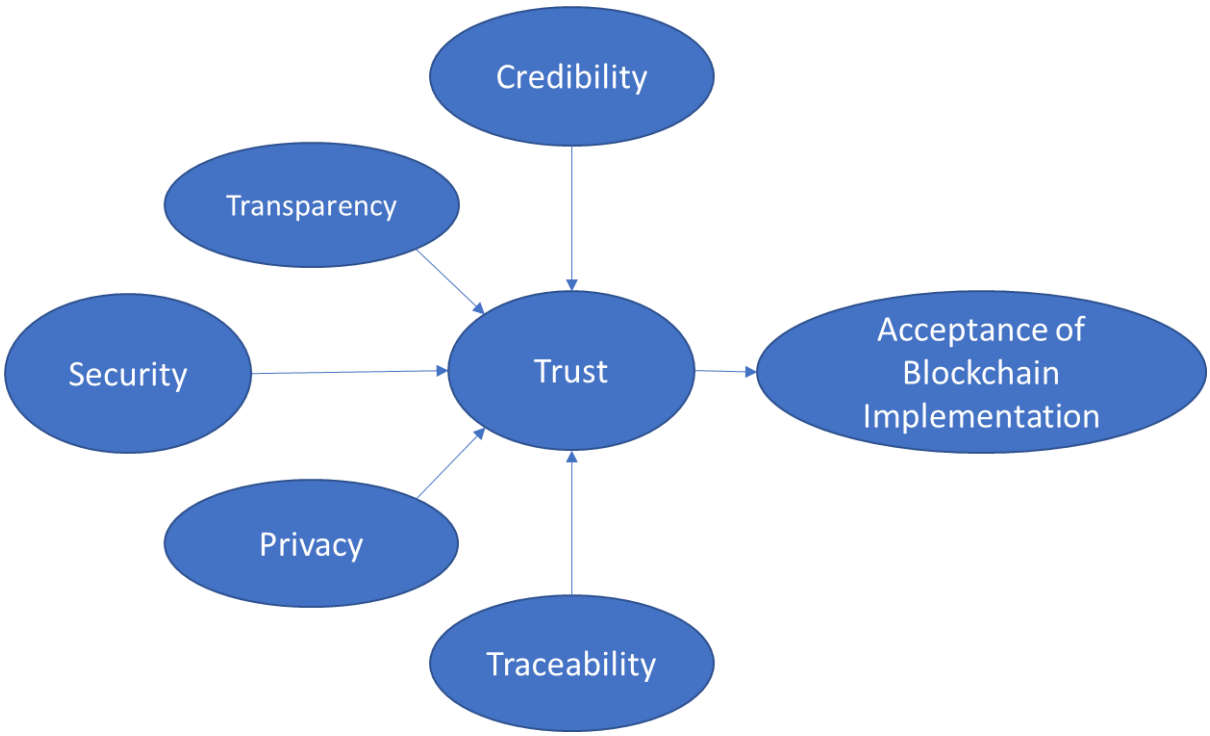

Figure 2.2 Conceptual Model of Blockchain-related trust attributes derived from Figure 2.1

This conceptual model is derived from the theory of Kochovski et al. (2019) from figure 2.1 that focused only on the blockchain-related trust attributes. This figure shows that the blockchain-related attributes: credibility, traceability, transparency, privacy, and security will contribute to trust. Therefore, it will increase the acceptance of blockchain implementation.

These attributes that define trust were further explained in the context of blockchain as follows:

1. Privacy

   Include the following aspects on blockchain: individual control over the data collection and personal data processing, knowledge of the security dangers posed by smart gadgets around people, and awareness and control over the future usage and disclosure of personal data by related parties to other parties outside the individual control sphere in which at this case is to the competitor (Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K., 2013).

2. Credibility

   Credibility is the extent to which the source of information or the information is seen to be genuine, a notion that may be applied to any data item. (Kochovski et al., 2019).

3. Security

   Security is an assessment of the system's capacity to protect itself from unintentional or intended external assaults. This trust attribute is closely linked to privacy or confidentiality, which determines whether the data in the blockchain is secured from being accessed by unauthorized entities (Kochovski et al., 2019).

4. Transparency

   Transparency is a characteristic that enables the blockchain ledger to be completely auditable. This characteristic allows for all related parties within a network to access the blockchain's stored transactions. (Kochovski et al., 2019).

5. Traceability

   a quality closely associated with transparency Since all history can be traced back to the initial transaction, traceability allows you to trace back the interaction

between entities on the blockchain (Kochovski et al., 2019). It helps cross-check on the transaction that has occurred.

According to the Fishbone diagram that was used to identify the cause of the problem, there is a possibility of a problem regarding the credibility of information and the blockchain system that was going to be implemented. In this case, it is related to the possibility of people intentionally or unintentionally putting erroneous data into the blockchain system and the nature of blockchain that are transparent and traceable. From the perspective of the supplier, they might not be willing to share their data in fear of privacy leakage and being acquired by their competitor. For instance, the competitor can infer information such as wholesale pricing strategies and other suppliers' parameters from information put into a transparent blockchain (Li & Zhang, 2008). On the other hand, business partners (in this case, VehGro) need to be sure that the information shared within blockchain should also be credible because they may need to know information such as other production costs to schedule warehousing and production optimally. Otherwise, they will not be able to make an effective decision. Still, they could also use such information to manipulate future price negotiations (Kerschbaum F., Schroepfer, A., Zilli, A., Pibernik, R., Catrina, O., de Hoogh, S., Schoenmakers, B., Cimato, S., & Damiani, E., 2011).

There are numerous pieces of literature on operation management that discuss the benefit of information sharing in the supply chain. However, in practice, some supply chains could not implement adequate information sharing due to some constraints such as compatibility of information system, information quality, trust, and confidentiality (Ali M. M., Babai, M. Z., Boylan, J. E., & Syntetos, A., 2017). Therefore, the researchers believe that knowing what type of blockchain is suitable for the supply chain, what kind of feature should be added to ensure the privacy and security of blockchain users, and what kind of blockchain feature should be added to ensure the credibility of information inside the blockchain. It could increase the trust of suppliers toward the implementation of the blockchain system.

Operationalization

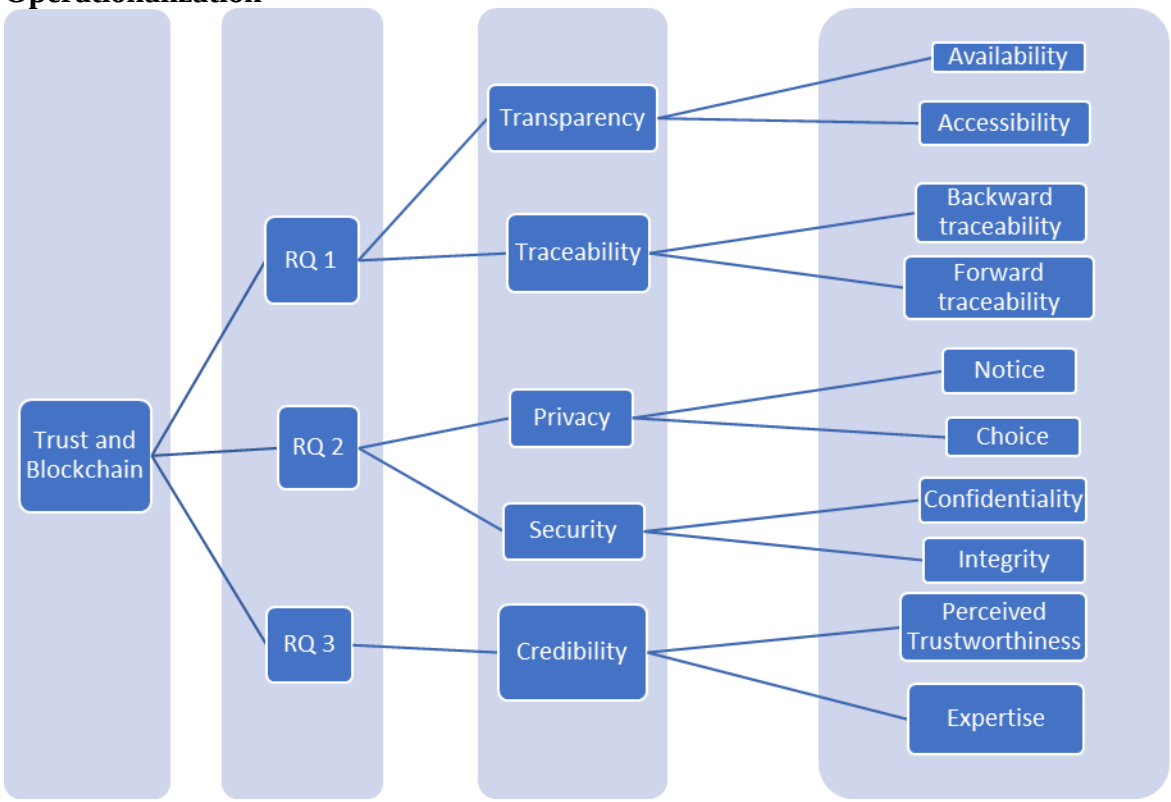

Figure 2.3 Operationalization

This operationalization shows that each sub-research question that will be discussed in the literature review and asked during the interview is based on the blockchain-related attributes and its sub dimension to limit the interview scope.

- Credibility will be asked around its sub-dimension: expertise (Seiler & Kucza, 2017; Ismagilova, E., Slade, E., Rana, N. P., & Dwivedi, Y. K., 2020) and perceived trustworthiness (Ismagilova et al., 2020).
- Privacy will be asked around its sub-dimension: notice (Liu C., Marchewka, J. T., Lu, J., & Yu, C. S., 2005) and choice (Liu et al., 2005).
- Security will be asked around its sub-dimension: confidentiality and integrity (Samonas & Coss, 2014).
- Transparency will be asked around its sub-dimension: availability and accessibility (Hosseini, M., Shahri, A., Phalp, K., & Ali, R., 2018).
- Traceability will be asked around its sub-dimension: backward traceability and upward traceability (Panetto, H., Baïna, S., & Morel, G., 2007).

Literature Review

In this literature review, researchers discuss all the necessary term related to the operationalization that will serve as supplementary sources to help answering main research question.

Definition of Blockchain

According to Michael, J., Cohn, A. L. A. N., & Butcher, J. R. (2018), Blockchain is a type of digital ledger technology with a peer-to-peer digital log of transactions that may be disseminated publicly or privately to all users (thus the terms decentralized and distributed). Blockchain technology verifies transactions using cryptography and a consensus process, ensuring transaction validity, eliminating double-spending, and enabling high-value transactions in a trustless environment. Transparency is provided via blockchain, which eliminates the need for intermediaries or third-party administrators (Michael et al., 2018).

There are two types of blockchain which are permissioned blockchain and permissionless blockchain:

- Permissioned Blockchain

  Permissioned blockchain networks need users publishing blocks to be approved by a third party (centralized or decentralized) (Wüst, K., & Gervais, A, 2018). Because only authorized users to maintain the blockchain, it is feasible to limit read access and who may issue transactions. Permissioned blockchain networks can enable anybody to view the blockchain or limit read access to approved persons. They may also allow anybody to submit transactions for inclusion on the blockchain or limit this access to authorized individuals. Permissioned blockchain networks may be created and managed with either open source or closed source software (Wüst, K., & Gervais, A, 2018). These networks are private networks used by certain persons or businesses to perform activities (Michael et al., 2018). It is appropriate for semi-closed networks of a few companies, generally structured as a consortium (Viriyasitavat & Hoonsopon, 2019). The degree of data openness varies, but it often involves access rules established by the consortium to regulate access in both participants and information within Blockchains. Even if the system is not entirely open, the benefits of decentralization can be obtained in part.

- Permissionless Blockchain

Permissionless blockchain networks are decentralized ledger platforms that allow anybody to publish blocks without the requirement for approval from any authority (Wüst, K., & Gervais, A, 2018). Permissionless blockchain systems are frequently open-source software that anybody may download (Michael et al., 2018). Because everyone has the ability to publish blocks, anyone can read the blockchain and issue transactions on the blockchain. Every blockchain network user can read and write to the ledger within a permissionless blockchain network.

Blockchains may be generalized and utilized to establish an agreed-upon set of rules that no one, neither users nor system operators, can breach. Applications involving numerous parties who require minimal confidence in each other, such as fragmented supply chains, rely on a distinct system design platform (Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L., 2018). This method does not necessitate any specific behavior on the users; instead, the underlying technology ensures the system's integrity even in the face of dishonesty or inactivity. Participants have access to the lecrodgers and may analyze transactions. This feature provides transparency (Tian, 2016) while also maintaining anonymity by cryptographics that are used to preserve records (Crosby, M., P. Pattanayak, S. Verma, and V. Kalyanaraman., 2016)

Some characteristics of blockchain, according to Viriyasitavat and Hoonsopon (2019), are:

- Decentralization

  Transactions in conventional centralized database systems are inherently trusted or authorized by central trusted intermediaries that ensure authenticity. This transaction incurs additional costs and performance that become a major concern when employing central servers. Blockchain technology is a promising answer to the issues of distributed transaction management (Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K. L., 2017). Under blockchain, any member may run the whole network rather than depending on a centralized mechanism built upon trust. Every transaction is distributed over the Blockchain's peer-to-peer network, with each participant maintaining their own local copy of the ledger (Hackius & Petersen, 2017).
- Persistence

  Transactions recorded in a Blockchain ledger are deemed persistent because they are distributed over the network, with each node maintaining and controlling its records. Persistence is maintained as long as the majority of nodes are benign. This feature gives rise to several characteristics, including transparency and immutability (temper resistance). Blockchains are auditable due to their transparency and immutability (Viriyasitavat & Hoonsopon, 2019).
- Validity

  Unlike other distributed systems, Blockchains do not need executions from every node. In a Blockchain system, transactions, or blocks, would be validated by other nodes. As a result, any fabrication may be quickly recognized (Correia, M., Veronese, G. S., Neves, N. F., & Verissimo, P., 2011).
- Anonymity and Identity:

  The fundamental feature of public Blockchains is anonymity. Identity in this system can be untethered from a user's real-world identity. To avoid identity exposure, one person might establish numerous identities (Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J. P. C., & Ko, K., 2018). There is no need for any central body to keep private information. Consequently, according to the transaction information, the real-world identity cannot be established, protecting a certain level of anonymity. On the other hand, identity is typically necessary for

controlled and governed systems by known organizations, such as private and permissioned Blockchains (Viriyasitavat & Hoonsopon, 2019).

- Auditability

  Record timestamps and persistence information enable easy verification and tracing of prior records across nodes in a Blockchain network. The degree of auditability is determined by the type of Blockchain technology and its implementation. Permissioned blockchains are less auditable than permissionless blockchains because some agreements, such as encrypted data, may prevent information from being fully auditable. Permissionless Blockchains are the most auditable because nodes are truly decentralized (Viriyasitavat & Hoonsopon, 2019).

- Openness

  Blockchains are considered to have openness because they rely on public nodes to keep track of transactions. As a result, anybody may publish a transaction and join the system by adhering to a set of rules and information included inside this Blockchain. Permissioned Blockchains are semi-opened since nodes must be pre-specified or confirmed before entering. They exist in the space between public and private Blockchains. The information included inside this Blockchain is governed by the consortium's policies, restricting whether the information is entirely open, partially open, or closed. Permissioned Blockchains, based on regulations, regulate how nodes are selected and the degree of data transparency. They do, however, rely on a single organization or owner (Viriyasitavat & Hoonsopon, 2019).

Definition of trust

A recent study shows that trust plays an essential role in enabling users to overcome risk perception and uncertainty in the usage and acceptance of new technologies (Li, X., Hess, T. J., & Valacich, J. S., 2008). Therefore, it is essential to know the meaning of trust itself and the factors that contribute to it.

However, Trust is hard to define as it has a vast and diverse area coverage. Thus, depending on their discipline of study, researchers might have their own definition of trust (McKnight & Chervany, 2000). We cannot simply define trust only from one perspective of view. Trust could be seen and categorized into several dimensions: trust as individual expectation, trust as interpersonal relation, trust in social structure, and trust in an economic transaction (Hosmer, L. T, 1995).

Trust as individual expectation has three characteristics: Firstly, expecting that the natural (and current) social order would be persisted and met in which the person was founded, secondly the expectation that those concerned with the person might perform a technically capable role, and lastly that those associated with the individual would perform the morally correct role (Hosmer, L. T, 1995).

Trust as interpersonal relations has a more extensive coverage that it examines not only on the level of individual perspective but the relation between persons. It has been argued that a person or organization trustworthiness could be examined based on these attributes (Butler & Cantrell, 1984)

- Integrity: the trustworthy individual's reputation for honesty and truthfulness.
- Expertise: technical knowledge and skills required by individuals to do the work.
- Consistency: reliability, predictability, and effective management judgment.
- Loyalty: the readiness to safeguard, assist and promote others.
- Openness: mental accessibility or desire to openly exchange thoughts and data with others

In the sense of social structure as a collective expectation that is inter exchanged within society, trust is the consequence of a behavior "good," "just," and "fair," that is, acts based on ethical principles of analysis that are perceived as morally correct, which recognize and defend the rights and interests of others in society (Hosmer, L. T, 1995). It could also be defined in the perspective of society as the expectancy of a single person, group, or business to act morally appropriate based on the moral principles of the other group or enterprise analysis in a cooperative undertaking of economic transaction and that it is ethical and justified (Hosmer, L. T, 1995).

The source of collective expectation of trust itself could be categorized into three sources according to Zucker, 1986:

- Process-based trust: it was linked to prior operational records. Here, exchanges were typically restricted to individuals with recognized and reputable trading histories.
- Person-based trust: it was linked to people's commonalities. The conversations here were restricted to individuals with a common cultural system with common background assumptions.
- Institutional-based trust: it was linked to formal measures such as professionalism or insurance from third parties. The interactions here have been restricted to those who have access to those assurances.

In economic terms, Bromily and Cummings (1992: 4) argued that trust might lessen transaction costs and provide a definition afterward. 'Trust' they said: 'would have a good faith attempt from another person or group to behave according to either express or implicit promises; to be honest in all talks preceded by those commitments, and not overtake others even if renegotiating is possible.

Through those perspectives of trust, there are also similarities in which trust is typically stated as optimism regarding the result of an event or the conduct of an individual. The person who trusts is always assumed to expect the finest (Hosmer, L. T, 1995). Perhaps this is not immediately apparent in situations in which economic transactions and social institutions predominate. In such circumstances, it is considered that wise persons predict the worst and are protected by market contracts, hierarchical controls, legal requirements, and informal responsibilities against this result or behavior. But trust is the reverse of the denied assumptions; it always remains a positive expectation. Confidence typically develops when people's interests are vulnerable and dependent on other people's behavior. A key component of a Trust definition is the anticipation of a loss in the event of a breakdown of trust that would be significantly higher than profit if the trust was maintained (Hosmer, L. T, 1995). Hence, trust is built upon a willingness to gain benefit through what is called cooperation.

Blockchain Related trust attributes

Trust is the main obstacle to the broad exchange of data (Rouhani & Deters, 2021). Many data owners are prevented from sharing their data because of a lack of transparent data-trust infrastructure, and people are concerned about data quality. Data trust is a paradigm enabling easy data sharing by making the process of sharing and reuse visible for the data users. By using numerous parties to preserve consensus on an unchangeable leader, Blockchain technology presents a shared and accountable administration (Rouhani & Deters, 2021). Therefore, trust becomes the major consequence of decentralization since there is no need for an appraisal of the trustworthiness of the intermediary or other members in the network (Nofer, M., P. Gomber, O. Hinz, and D. Schiereck., 2017).

According to the research of Kochovski et al. (2019), namely Credibility, Privacy, Security, Transparency, and Traceability attributes of blockchain are deemed having ability that could contribute toward trust.

1. **Credibility**

Credibility is the extent to which the data source or data is seen to be genuine, a notion that may be applied to any data item. (Kochovski et al., 2019). According to the research Ismagilova et al., (2020), there are three sub-dimensions of credibility: expertise, trustworthiness, and homophily. However, homophily is more inclined toward the credibility of consumer behavior (Jalees, T., Tariq, H., Zaman, S.I., Kazmi, S.H.A., 2015; Saleem and Ellahi, 2017), not between supplier and wholesaler. Therefore, the researchers only use two sub-dimensions of credibility.

- Expertise

  Expertise is the extent to which an entity can provide correct information to the receiver (Ismagilova et al., 2020). It has a positive effect on source credibility (Seiler & Kucza, 2017)

- Trustworthiness

  Another factor influencing source credibility is the sender's perceived trustworthiness. When the source is reliable, the receiver has less reason to doubt the veracity of the information. If the statement is judged to be valid, honest, and to the point, the information source and recommendation provided are considered trustworthy. (Ismagilova et al., 2020).

2. Privacy

Privacy has been described as a right to be left alone and regulate the release of their personal information (Liu et al., 2005). it includes the following aspects of blockchain: which is individual control over the data collection and personal data processing, knowledge of the security dangers posed by smart gadgets around people, and awareness and control over the future usage and disclosure of personal data by related parties to other parties outside the personal control sphere in which at this case is to the competitor (Ziegeldorf et al., 2013). There are four sub-dimensions of privacy: Notice, Choice, Access, and Security (Liu et al., 2005). However, as the other dimension already addressed the other sub-dimension, thus, the researchers only chose two out of four subdimension. There are:

- Notice

  Notifying the data owner that their data is being collected or accessed (Liu et al., 2005).

- Choice

  Providing a choice whether to allow a particular person or organization to use and share data collected (Liu et al., 2005).

3. Security

Security is an assessment of the system's capacity to protect itself from unintentional or intended external assaults. This trust attribute is closely linked to privacy or confidentiality, which determines whether the data in the blockchain is secured from being accessed by unauthorized entities (Kochovski et al., 2019). There are three main sub-dimensions according to the research of Samonas & Coss, (2014) which are Confidentiality, Integrity, and Availability. However, availability is also part of the subdimension of transparency (Hosseini et al., 2018). Therefore the writer only focuses on two other subdimension:

- Confidentiality

  "Authorized restriction of access and disclosure of information, including protection of personal privacy and private data," is defined as confidentiality. The concept is that the information and data represented should be safeguarded; it implies secrecy in a manner that its use is limited solely to permitted usage by authorized persons (Samonas & Coss, 2014).

- Integrity

  It is defined as the prevention of "improper information modification or destruction," which includes information authenticity and non-repudiation. Non-repudiation refers to the inability to challenge a specific transaction or interaction between two parties, which presumes that a sufficient authentication process occurred in the first instance (Samonas & Coss, 2014). Authenticity refers to the quality of being genuine and original. Thus authentication is the process of validating, to a certain level of confidence, that a claimed identifier is valid and is genuinely linked to a specific item or person

4. Transparency

Transparency comes from the medieval Latin word "transparentum" with the meaning of light. It is therefore used to indicate "to be able to be seen through." In its present use, however, this term is occasionally described as 'open flow of information' and 'the release of information by institutions that is necessary for the evaluation of these institutions' Consequently, transparency is regarded as a need for companies and their information systems, as a system which is designed to collect, communicate, organize, and store information to its stakeholders which enables them to be accountable toward their stakeholders through disclosure of relevant information (Hosseini et al., 2018). There are several other subdimensions of transparency within Hosseini et al. (2018) research, but the sub-dimension closely related to blockchain attributes are availability and accessibility (Viriyasitavat & Hoonsopon, 2019; Wüst, K., & Gervais, A, 2018).

- Information Availability

  Reliable and timely use of information is what we called as availability (Samonas & Coss, 2014). There is obviously no openness if providers withhold information from the recipients concerned. When providing information to recipients, information providers should ensure that information quality is maintained to prevent problems such as incorrect information, partial information, incomplete information, and overload of information (Hosseini et al., 2018).

- Information Accessibility

  While providers supply the availability of information, accessibility of information focuses on the recipients' capability to obtain information. The degree to which receivers may easily find information is often referred to as visibility of the information.

5. Traceability

Traceability is a quality that is closely associated with transparency. Since all history can be traced back to the initial transaction, traceability means that it allows you to trace back the interaction between entities on the blockchain (Kochovski et al., 2019). It is useful for cross-checking on the transaction that has occurred. Some literature defines traceability based on its subdimension into Backward and Upward traceability (Panetto et al., 2007; Jansen-Vullers, J., van Dorp, A., & Beulens, B., 2003).

- Backward Traceability

  Ability to collect information and data about the product's prior history (Panetto et al., 2007)

- Forward Traceability

  Ability to trace where the products are going, all the process and output of the product went into (Panetto et al., 2007).

Blockchain implementation on Supply chain

Modern supply chains are inherently complicated, with several tiers of geographically dispersed organizations vying to service customers (Johnson 2006; Lambert

and Enz 2017). Globalization, disparities in regulatory regulations, and differences in cultural and human behavior in supply chain networks make it nearly hard to assess information and manage risk in this complex network (Sarpong 2014; Ivanov, Dolgui, and Sokolov 2018). Inefficient transactions, fraud, pilferage, and poorly functioning supply chains all contribute to a lack of confidence and, as a result, a need for improved information sharing and verifiability.

In many supply chain companies, including the agri-food sector, traceability becomes an increasingly pressing need as a distinction that contributes to their competitive advantages (Costa, C., F. Antonucci, F. Pallottino, J. Aguzzi, D. Sarriá, and P. Menesatti., 2013). Consequently, a lack of transparency in the supply value of any item impedes the verification and validation of the real worth of an item that supply chains companies and clients handle (Saberi et al., 2018). This traceability is further complicated by the costs associated with intermediaries' management, dependability, and openness. These risks and lack of openness lead to strategic and reputational competitive problems (Saberi et al., 2018). Current supply chains rely largely on centralized, sometimes divisive, independent IM systems in organizations. For example, corporate resource planning systems have their setbacks. Supply chain organizations demand substantial confidence in retaining their sensitive and valuable information by another organization that preserves their sensitive information (Abeyratne and Monfared 2016). Failure in a single point is another downside of centralized information systems that is vulnerable to the whole system to errors, hackers, corruption, or attacks (Dong, F., P. Zhou, Z. Liu, D. Shen, Z. Xu, and J. Luo., 2017). These problems raise questions about whether existing information chain supply systems can securely and confidently provide the information needed to ensure that products and services come in good time. The answer is to improve the supply chain's transparency, safety, durability, and process integrity that the implementation of blockchain might give into the supply chain (Saberi et al., 2018).

The other contribution of blockchain toward a supply chain that could enhance the cooperation of the member within the supply chain are closely related to 4 key features (Cole R., Stevenson, M., & Aitken, J., 2019):

- Supply chain Visibility

  Poor end-to-end transparency is one of the primary reasons for supply chains inefficiencies, contributing to the so-called bullwhip effect. Blockchain technology enables several Supply Chain members to share real-time information on an object's location and state. With sensor technology and the Internet of Things, any quantifiable state, such as product temperature in a cold chain or the availability of technical equipment working in the Supply Chain, can be recorded. This increases data accuracy, which in turn enhances collaborative planning and execution and the deployment of preventative and reactive risk management strategies.

- Supply chain Integrity

  Blockchain technology allows you to track assets back to their origins using a shared ledger of transparent and immutable data (Petersen, M., Hackius, N., & von See, B., 2018). Provenance information maintains the integrity of assets, including both items and technical equipment. This might compel ethical sourcing and enable for a detection, if not prevention, of product counterfeiting and other fraudulent activities. Applications might include asset ownership tracing after-sale for warranty purposes. Furthermore, BCT simplifies paperwork in global trade by

guaranteeing the authenticity of freight papers, such as those used in customs clearance.

- Supply chain Orchestration

  When transparency and validation are combined with automation via smart contracts, one may imagine a Supply chain that runs highly automated based on pre-specified criteria. Because information and associated choices or measures are transmitted across the Supply chain, this enhances speed and eases coordination. In the event of a machine breakdown, the machine may purchase a spare component from a supplier, seek maintenance assistance, and notify downstream partners of potential delays. Another advantage of automation is the ex-post enforceability of contracts, which means that contractual parties cannot back out of their obligations (Babich & Hilary, 2018).

- Supply chain Virtualization

  Virtualization is a well-known method in IT infrastructure management that creates a logical representation of physical hardware in software to enhance the utilization and flexibility of IT assets (Laudon, 2007). Tokenization of actual supply chain assets such as technical equipment and inventory follows a similar concept since there is an additional option besides transferring supply chain asset acquisition/sale to the blockchain. Tokens representing claims on capabilities or ordering alternatives might be issued and distributed outside of conventional (bilateral) contractual agreements. Similar to how IT hardware is virtualized, this would allow for better capacity use of supply chain assets because excess capabilities might be monetized.

RESEARCH METHODOLOGY

This research is qualitative research that will use both primary data and secondary data collection to answer the research question to gain in-depth knowledge on the subject of the case supported with sufficient literature.

This research aims to give suggestions on what could serve as a reason for the suppliers of VehGro to accept the usage of blockchain system that is going to be incorporated with the current supply chain. In addition, this research also gives several suggestions to counter the threat of confidentiality, transparency, and credibility of blockchain implementation within the supply chain.

Apart from the information retrieved from articles, journals, previous research, and relevant websites that is included in the literature review; This research also combines knowledge gained from the interview with VehGro CEO, an expert on blockchain technology and an expert on the information system. By interviewing VehGro CEO, the researchers gain a deeper insight into the initial reason of the project to implement blockchain and the current condition of the company. While, interviewing an expert in blockchain technology gives a professional insight around the topic that is beneficial to be added to this research. On the other hand, researcher also interview an expert in information system to gain a comparative view between the common information system and what blockchain could offer. Combined information between both literature review and interview will be a good balance to solidify the considerations that are served in this research

Data Collection Techniques

This qualitative research uses both primary data gained from interview with related parties and secondary data from literature review to answer main research question based on the operationalization on theoretical framework.This research will be conducted as follows:

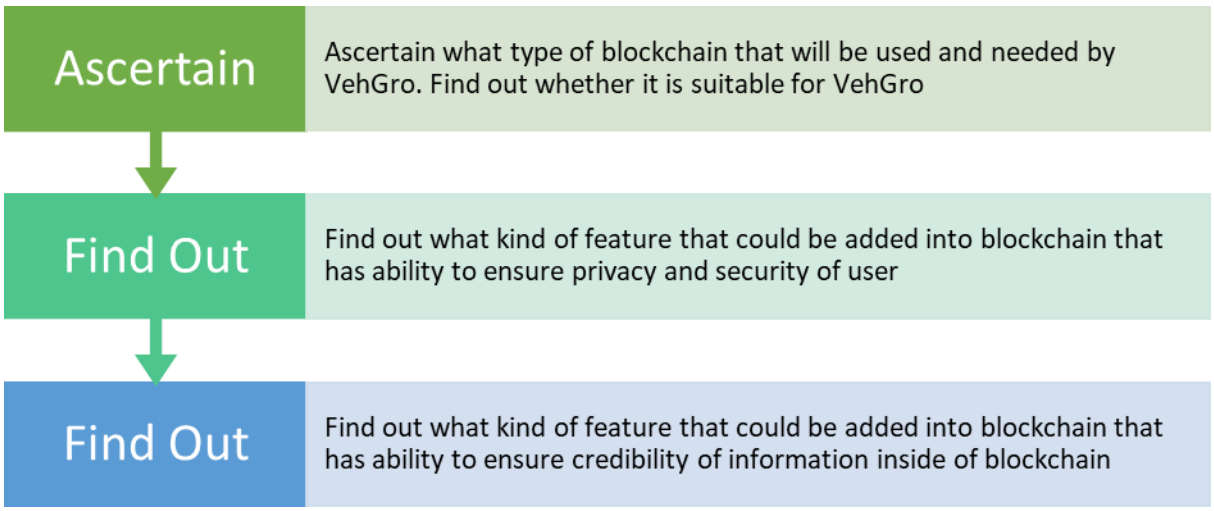

Figure 3.1 research design

This research design explains how the researcher is planning to conduct this research to answer the main research question by solving each sub research question

- RQ1. What type of blockchain is suitable for the supply chain?

  This question will be answered by interviewing VehGro to know what blockchain capability they wish to implement in their supply chain and interviewing an Expert in Blockchain to know what kind of blockchain is suitable for the supply chain. The question that will be asked is related to the blockchain-related trust attributes: traceability and transparency. Apart from that, the researcher will also find literature that provides relevant information about the type of blockchain that has characteristics that suitable for supply chain
- RQ2. What kind of blockchain feature should be added to ensure privacy and security of blockchain users?

  This question will be answered by first interviewing VehGro to know what feature they are planning to implement that could ensure the privacy and security of users. Secondly, interview with blockchain specialist to know what type of feature can be implemented into the blockchain to ensure the user's privacy and security. The researchers will also investigate some literature regarding privacy and security in the blockchain system.
- RQ3. What kind of blockchain feature should be added to ensure the credibility of information inside the blockchain?

  This question will be answered by first interviewing VehGro to know what feature they are planning to implement that could ensure the credibility of information inside the blockchain. Secondly, interview with blockchain specialist to know what type of feature can be implemented into the blockchain to ensure the credibility of information inside the blockchain system. The researcher will also look at relevant articles about credibility in blockchain to support the data.

Following this research design, researcher has collected primary data from interviews with the related parties based on the 3-sub research question area supported by the relevant dimension of the blockchain-related trust attributes and its sub-dimension. The question will be presented as a half-structured question in the following interview protocol (attached) to gain in-depth knowledge regarding the research topic. The researchers will later make a transcript of the interview and examine it based on the code related to the blockchain-related trust attributes and its sub-dimension.

The interview has been conducted using a half-structured method to get more in-depth knowledge about the topic. All of the findings that do not fit into this research's

current operationalization but are useful to answer the main research question will be treated as explorative findings. The transcript and coding process is being put as attachment of this research.

Secondary data are retrieved from scholarly articles, journals, and relevant websites added to the literature review. The following keywords have been used in various combinations to retrieve relevant article topics from the search engines: Permissioned and permissionless blockchain, supply chain, privacy protection, security, visibility, credibility, traceability, transparency, information quality, organic food, wholesaler, the food chain.
The search resulted in a hundred thousand articles and was selected by the writer based on titles, abstracts, and most relevant conclusions with the keyword and topic of this research. Those selected relevant literature has been put in the previous chapter on the literature review. This literature review will serve as supplementary sources to compliment the result of the research.

The combination of this data will serve as the basis of consideration for VehGro to help them make decisions on blockchain implementation project.

Data Analysis

The first interview was conducted with the CEO of VehGro company to gain a deeper view on the initial reason for the blockchain project, such as his objective of implementing blockchain on supply chain, the company's current condition, and why has the project been halted. The second interview was conducted with a blockchain technology specialist that is also a professional practitioner and researcher with several years of experience. The main reason is to add professional insight and recommendations regarding the issues faced by implementing blockchain. The third interview is conducted with a digital traceability expert on old information system that will give insight on the comparison between the old information system that usually being used by company compared to the blockchain from the perspective of expert in the old Information System. Having knowledge from those respondents add an adequate knowledge on current condition of the company, the objectives of the blockchain project, a professional view on the blockchain implementation on the research, and a comparative perspective from professional in information System.

RESULT ANALYSIS AND DISCUSSION

This result analysis will be separated into 4 sub chapter that discuss the result based on each sub research question and explorative finding gained from interview. This sub research question will contribute to solve main research question on “What (theoretical) obstacles must be solved in order to convince suppliers to implement Block Chain application of VehGro?”.

Type of blockchain that suitable for the supply chain.

From the interview result, researchers found out that currently VehGro operation is lack of transparency and traceability. Therefore, they intend to implement blockchain that would give those attributes. However, they are also faced with an issue of supplier that scared of privacy leakage when implement a system that has transparency and traceability. This issue has been addressed by expert respondents by advising that related to the transparency attributes of blockchain, the suitable blockchain that VehGro should use is a permissioned blockchain and they need to make a proper design of access control that incorporate a private smart contract with a viewing key. Furthermore, to address the issue of traceability, apart from implementing a rating feature for blockchain user that VehGro is planned, the expert adds that the blockchain should have immutability of information that could be backward-traced by authorized user.

Blockchain feature to ensure privacy and security of blockchain users

From the interview result, researchers found out that currently VehGro ensure security and privacy of their supplier by first handing out supplier questionnaire that list what are mandatory requirement of information that should be shared, do frequent checking, get certification from third party control union that check them at least twice a year. They also plan to define what are the term and agreement related to future usage of blockchain system. In order to further enhance VehGro current operation related to ensuring privacy and security, expert respondent has given advise. First to ensure privacy of blockchain's user, expert respondent has advised that the blockchain feature should implement viewing keys that will give owner notification and choice whether or not to release viewing keys, defining mandatory field, term and agreement that is required. While to ensure security of blockchain's user, the blockchain features that should be added is private smart contract, decentralization of data storage, and third parties' check.

Blockchain feature to ensure the credibility of information inside the blockchain

From the interview with CEO, researcher identify that currently VehGro maintain their credibility of information using transformation of supplier-ship into partnership, knowing their supplier personally, held annual meeting with supplier and have a validation from third party using certification. Researcher also address one issue related to credibility of information about what should VehGro do if there is malicious or false information inputted to the system of information intentionally or unintentionally. This issue has been answered by one of expert respondent.

From the interview with experts, researchers concluded that in order to further enhance their current operation in ensuring the credibility of information, blockchain feature that will be implemented should allow a user to make changes on top of previous wrong information when they put false or malicious information. From the front-end side of the blockchain application it should only shows the latest data. User should not have the ability to erase any information that is put into blockchain system. This way blockchain will still be immutable and allow authorized user to trace what are the previously mistake that has been done by user, who responsible for the mistake, and other relevant information related to it.

Explorative Findings

From the interview, researchers found out several explorative finding that is not related with conceptual model but still could contribute on answering main research question. First is the idea to use token to monetize the project. This token should have a value based on certain utility and-or underlying physical assets. Secondly, is to put into account the effect of project on the company public image. The image that might come from the implementation of blockchain is that the supply chain environment will be more secure and credible which is a good image for the supply chain stake holders. Next, is to make use of the current information system and make a hybrid system rather than fully blockchain application. By doing so it is expected to make people more easily to adapt with the change because there is still a sense of familiarity. Lastly, to keep in mind that system should always be easy to use because a system should make everything become easier not complicated instead.

CONCLUSION

To conclude implementation of blockchain will give several advantages toward VehGro current operation. From the research it is found out that blockchain implementation will enhance the trustworthiness of the transaction, give traceability, better public image, less transaction fees and more secure information compared to their current operation. This advantage can serve as offer for supplier to accept the implementation of blockchain.

Acceptance of Blockchain Implementation

The acceptance of blockchain implementation will be faithful to conceptual model of blockchain-related trust attributes derived from Kochovski Models (figure 1.4). Starting from the "Credibility" that was identified in this research by transforming supplier-ship into partnership, have a validation from third party using certification, knowing supplier personally and allowing user to make change when there is wrong data inputted. Secondly, "Privacy" that is identified by implementation of viewing keys that will give owner notification and choice whether or not to release viewing keys, defining mandatory field, term and agreement that is required. Third, "Security" that is addressed by using private smart contract, decentralization of data storage, and third parties' check. Fourth, "Transparency" is addressed by the usage of permissioned blockchain, and proper user access control design. Lastly, "Traceability" is addressed by implementing a rating option for user, immutability of information that could be backward-traced by authorized user.

Advise

In conclusion, there are four points that VehGro can do to convince suppliers to accept the implementation of blockchain systems in their supply chain.

1. They need to implement permissioned blockchain rather than permissionless blockchain.
2. The permissioned blockchain should be made with a good access control design, such as having viewing keys and private-smart contracts.
3. The Blockchain system should allow users to add correction data on top of the wrong data.
4. The blockchain system should be better than the current system. It is advised to make an incentive plan or use the current system to build a hybrid system.

The implementation of blockchain does contribute to trust because it allows traceability and immutability. However, not all types of blockchain are suitable for implementation into the supply chain. The permissionless blockchain that is too public will not be favourable for the supply chain because some data should be kept confidential, and only a few people should be allowed to access the information. It is also not allowed by the privacy law to store private information on a public blockchain that is transparent to everyone. Therefore, the type of blockchain suitable for the supply chain is permissioned blockchain.

Permissioned blockchain should be made with a good design of access control, private or viewing keys, and private-smart contracts. Using this kind of blockchain, when users need proof for certain transactions, the owner will be notified and choose whether to allow release of the viewing keys. Therefore, people can still verify all the transactions made on top of the blockchain using the viewing key. The new system should also define the mandatory field and what information cannot be shared into the blockchain.

To ensure the credibility of data inputted, the blockchain system should also allow users to add additional correction data when wrong data is inputted. However, to maintain the immutability characteristic of blockchain, people should only be allowed to add new data for correction that will be put on top of the previous wrong data but cannot erase or change the preceding data. Therefore, only the new corrected data could be seen in the user interface. On the other hand, from the back-end or blockchain side, we could always trace the previously wrong data, who is responsible, and what time it is being inputted. This is the combination of two blockchain strengths: immutability and traceability, which could not be found on a conventional information system.

Besides creating a new system that has an advantage over the current system that is being used, the usage of token to incentivize the project could be one way to convince suppliers to switch to a blockchain system. One important thing to keep in mind is that the

token should hold a certain utility for the token to have a value. Otherwise, people will not be willing to make an effort to adapt to the new system. The other suggestion is to also put into account a possibility of better public image due to implementation of blockchain, from customer perspective the implementation of blockchain will give value toward the company. It would make the ecosystem of the supply chain looks more credible and secure. Lastly, consider making a hybrid system with a combination blockchain system and the current operating system. It makes it easier for people to adapt to the change rather than completely change everything. After all, system should make everything simpler, not the other way around.

POLICY

Blockchain has taken a lot of interest from many people. Many people try to incorporate this new technology to improve their current business model. On the other hand, some people prefer to stick to their old ways of doing things, and the rest is afraid of something unknown to them. Many issues have not been completely solved, such as privacy and confidentiality issues. Thus, it makes it hard to adopt blockchain technology, especially its implementation on the organic food supply chain in the Netherlands.

Currently, blockchain is still quite a new subject that is still in its initial stage of advancement. Therefore, there is still limited research and regulation regarding the usage of blockchain in the supply chain. Consequently, not many people are aware of its capabilities. However, blockchain has a lot of possibilities for its development, especially concerning the implementation on supply chain industries that need traceability.

LIMITATION

The author acknowledges several limitations on this research; Firstly, although this research is about how to convince suppliers to accept blockchain implementation in the supply chain. However, the result given is only from the perspective of VehGro, a blockchain specialist, and literature review. The researcher did not interview the supplier of VehGro to confirm its findings because of the inability to gain contact information. Secondly, due to the researcher's background, this research could only give consideration of the blockchain capability that could be beneficial for the company regarding its contribution toward trust, not a technical blueprint of the blockchain that can be implemented. Third, any legal issues concerning the usage of blockchain are not explained within this research because the author lacks knowledge about that matter. Fourth, this research only focused on the case of VehGro and did not make any comparative studies towards similar companies in the same industries. Hence, the author doubts external validity if it is being applied in different circumstances, such as different companies or countries. The author believes that this limitation could be a consideration for further enhancement of the research on a similar topic.

REFERENCES

Abeyratne, S. A., and R. P. Monfared. 2016. “Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger.” International Journal of Research in Engineering and Technology 5 (9): 1–10.

Ali, M. M., Babai, M. Z., Boylan, J. E., & Syntetos, A. (2017). Supply chain forecasting when information is not shared. European Journal of Operational Research, 260(3), 984–994. https://doi.org/10.1016/j.ejor.2016.11.046

Bromily, P., & Cummings, L. L. 1992. Transaction costs in organizations with trust. Working paper No. 28, Strategic Management Research Center, University of Minnesota, Minneapolis.

Butler, J. K. 1991. Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory. Journal of Management, 17: 643-663.

Butler, J. K., & Cantrell, R. S. 1984. A behavioral decision theory approach to modelling dyadic trust in superiors and subordinates. Psychological Reports, 55: 19-28

Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: implications for operations and supply chain management. *Supply Chain Management: An International Journal*.

Correia, M., Veronese, G. S., Neves, N. F., & Verissimo, P. (2011). Byzantine consensus in asynchronous message-passing systems: a survey. *International Journal of Critical Computer-Based Systems*, *2*(2), 141. https://doi.org/10.1504/ijccbs.2011.041257

Costa, C., F. Antonucci, F. Pallottino, J. Aguzzi, D. Sarriá, and P. Menesatti. 2013. "A Review on Agri-Food Supply Chain Traceability by Means of RFID Technology." Food and Bioprocess Technology 6 (2): 353–366.

Crosby, M., P. Pattanayak, S. Verma, and V. Kalyanaraman. 2016. "Blockchain Technology: Beyond Bitcoin." Applied Innovation 2: 6–9.

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K. L. (2017). BLOCKBENCH. Proceedings of the 2017 ACM International Conference on Management of Data. Published. https://doi.org/10.1145/3035918.3064033

Dong, F., P. Zhou, Z. Liu, D. Shen, Z. Xu, and J. Luo. 2017. "Towards a Fast and Secure Design for Enterprise-Oriented Cloud Storage Systems." Concurrency and Computation: Practice and Experience 29 (19): e4177.

Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: trick or treat?. In *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23* (pp. 3-18). Berlin: epubli GmbH.

Hilten, M., Ongena, G., & Ravesteijn, P. (2020). Blockchain for Organic Food Traceability: Case Studies on Drivers and Challenges. Frontiers in Blockchain, 3. https://doi.org/10.3389/fbloc.2020.567175

Hosseini, M., Shahri, A., Phalp, K., & Ali, R. (2018). *Four reference models for transparency requirements in information systems. Requirements Engineering*, 23(2), 251-275.

Hosmer, L. T. (1995). Trust: The connecting link between organizational theory and philosophical ethics. Academy of management Review, 20(2), 379-403.

Ilie, G., & Ciocoiu, C. N. (2010). Application of fishbone diagram to determine the risk of an event with multiple causes. Management research and practice, 2(1), 1-20.

Ismagilova, E., Slade, E., Rana, N. P., & Dwivedi, Y. K. (2020). The effect of characteristics of source credibility on consumer behaviour: A meta-analysis. *Journal of Retailing and Consumer Services*, *53*, 101736. https://doi.org/10.1016/j.jretconser.2019.01.005

Ivanov, D., A. Dolgui, and B. Sokolov. 2018. "The Impact of Digital Technology and Industry 4.0 on the Ripple Effect and Supply Chain Risk Analytics." International Journal of Production Research, 1–18.

Jalees, T., Tariq, H., Zaman, S.I., Kazmi, S.H.A., 2015. Social media in virtual marketing: antecedents to electronic word of mouth communication. Mark. Forces 10 (1), 15–32.

Jansen-Vullers, J., van Dorp, A., & Beulens, B.(2003). Managing traceability information in manufacture, International Journal of Information Management, 23, 395

Johnson, M. E. 2006. "Supply Chain Management: Technology, Globalization, and Policy at a Crossroads." Interfaces 36 (3): 191–193. http://www.jstor.org.ezproxy.wpi.edu/stable/20141388.

Kerschbaum, F., Schroepfer, A., Zilli, A., Pibernik, R., Catrina, O., de Hoogh, S., Schoenmakers, B., Cimato, S., & Damiani, E. (2011). Secure Collaborative Supply-Chain Management. Computer, 44(9), 38–43. https://doi.org/10.1109/mc.2011.22.

Kochovski, P., Gec, S., Stankovski, V., Bajec, M., & Drobintsev, P. D. (2019). Trust management in a blockchain based fog computing platform with trustless smart oracles. Future Generation Computer Systems, 101, 747-759.

Lambert, D. M., and M. G. Enz. 2017. "Issues in Supply Chain Management: Progress and Potential." Industrial Marketing Management 62 (Supplement C): 1–16.

Laudon, K. C. (2007). *Management information systems: Managing the digital firm*. Pearson Education India.

Li, L., & Zhang, H. (2008). Confidentiality and Information Sharing in Supply Chain Coordination. Management Science, 54(8), 1467–1481. https://doi.org/10.1287/mnsc.1070.0851

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289–304. https://doi.org/10.1016/j.im.2004.01.003

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, *17*(1), 39–71. https://doi.org/10.1016/j.jsis.2008.01.001

McKnight, D. H., & Chervany, N. L. (2000). What is trust? A conceptual analysis and an interdisciplinary model. AMCIS 2000 proceedings, 382.

Michael, J., Cohn, A. L. A. N., & Butcher, J. R. (2018). Blockchain technology. *The Journal*, *1*(7).

Nofer, M., P. Gomber, O. Hinz, and D. Schiereck. 2017. *"Blockchain." Business & Information Systems Engineering 59 (3): 183–187*

Over ons | VehGroshop.nl. (n.d.). Vehgroshop. Retrieved June 13, 2021, from https://www.vehgroshop.nl/over-ons

Panetto, H., Baïna, S., & Morel, G. (2007). Mapping the IEC 62264 models onto the Zachman framework for analysing products information traceability: a case study. *Journal of Intelligent Manufacturing*, *18*(6), 679-698.

Petersen, M., Hackius, N., & von See, B. (2018). Mapping the sea of opportunities: Blockchain in supply chain and logistics. it-Information Technology, 60(5-6), 263-271.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2018). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Saleem, A., Ellahi, A., 2017. Influence of electronic word of mouth on purchase intention of fashion products on social networking websites. Pak. J. Commer. Soc. Sci. 11 (2), 597–622.

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Sarpong, S. 2014. "Traceability and Supply Chain Complexity: Confronting the Issues and Concerns." European Business Review 26 (3): 271–284.

Seiler, R., & Kucza, G. (2017). Source credibility model, source attractiveness model and match-up-hypothesis : an integrated model. *Journal of International Scientific Publications: Economy & Business*, *11*. https://doi.org/10.21256/zhaw-4720

Shahid, A., Almogren, A., Javaid, N., Al-Zahrani, F. A., Zuair, M., & Alam, M. (2020). Blockchain-based agri-food supply chain: A complete solution. IEEE Access, 8, 69230-69243.

Shrier, D., Wu, W., & Pentland, A. (2016). Blockchain & infrastructure (identity, data security). Massachusetts Institute of Technology-Connection Science, 1(3), 1-19.

Tian, F. 2016. "An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain Technology." 13th International Conference on Service Systems and Service Management (ICSSSM), 2016.

Vehgroshop. (2021). Driven by health. Retrieved 13 June 2021, from https://www.vehgroshop.com/about-us?utm_source=vehgro&utm_medium=menu_item&utm_campaign=about-us_button

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32–39. https://doi.org/10.1016/j.jii.2018.07.004

Wüst, K., & Gervais, A. (2018, June). Do you need a blockchain?. In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 45-54). IEEE.

Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J. P. C., & Ko, K. (2018). Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. *IEEE Access*, *6*, 1513–1524. https://doi.org/10.1109/access.2017.2779263

Yousuf, S., & Svetinovic, D. (2019, November). Blockchain Trust and Decentralization in Supply Chain Management. In 2019 27th Telecommunications Forum (TELFOR) (pp. 1-4). IEEE.

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2013). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728–2742. https://doi.org/10.1002/sec.795

Zucker, L. G. 1986. Production of trust: Institutional sources of economic structure, 1840-1920. In B. M. Staw & L. L. Cummings (Eds.), Research in organizational behavior, vol. 8: 53-111. Greenwich, CT: JAI Press.