Digital supply chain development in blockchain technology using Rijndael algorithm 256

1Ferri Andrianto Susilo, 2Yaya Sudarya Triana

1Magister Teknik Industri, Universitas Mercu Buana, Jakarta, Indonesia
2Faculty of Computer Science, Universitas Mercu Buana, Jakarta, Indonesia

E-mail: ferrykudus@gmail.com

Abstract. Information hollering through electronic links occurs across organizational boundaries with interagency that allow automatic exchange of electronic data between partners in the supply chain. In digital data networks are usually sent by copying them from one place to another, one of the main problems in this case is to verify that the information received from the network is genuine and latest. Blockchain technology is considered to solve the data verification in the data authenticity problem independently, without having to take regardless of who or where the data came from. The application of blockchain fits perfectly with the digital supply chain as it leverages Internet technology as a system that connects all organizations involved in the supply chain. Blockchain consists of a set of data consisting of a chain of data packets where each block consists of several transactions in each block can be validated using cryptographic means, cryptography itself consists of two kinds of cryptographic symmetric and asymmetric cryptography. In this paper the application of blockchain uses cryptographic symmetric with Rijndael 256 algorithm which is famous for its easy resistance, speed and design. the results of discussions using technology and blockchain on the digital supply chain is still a concept of application. From the concepts, the researcher concludes the application of blockchain technology with the data structure can be applied by sharing encryption and can be applied in some cases, such as data verification for face recognition, artificial intelligence or machine learning.

Keywords: Rijndael 256 Algorithm, Encryption, Decryption, Blowfish, Huffman

1. Introduction
The development of Information Communications and Technology (ICT) influence business strategy and operating level of SMEs, the influence of ICT changes internal logistics operations and SME relationships with external suppliers, distributors, and customers [1]. Supply chain is defined as a network that understands all organizational activities and is related to data flow and transformation of goods, starting from the raw material stage and through the process to the final use, as well as the associated information flow [2]. In inter-organizational information systems, which connect companies with their suppliers, distributors, and customers, the movement of information through electronic links (eg XML / EDI - Extensible Markup Language / Electronic Data Interchange) takes place across organizational boundaries between separately owned organizations. This requires not only electronic links in the form of basic electronic data exchange systems (such as for purchase orders, delivery notes, cash flow, etc.), but also the interaction between complex cash management systems or by accessing
common technical databases. So the problem with sharing and sharing information is still viable in the context of supply chain management [3].

The development of EDI more than 20 years ago enabled the automatic exchange of electronic data between supply chain partners. Later, Supply Chain Operating Networks (SCON) emerged to enable global transactions across trading network members based on the movement of goods. On the one hand, SCON has brought added value to the supply chain by enabling the exchange of electronic data. On the other hand, this added value is directly proportional to the level of participation of a particular industry sector within a SCON. Therefore, companies that venture into new industries or markets are forced to support many SCONs that often lead to inefficiencies and high costs [4]. In SCON transactions, the organization or industry currently processes and integrates data through trusted third parties, most often through the trade finance bank service [5]. But some tech supporters like blockchain have promised to change this [6], whereas blockchain serves to erase data duplication problems with the help of public-key cryptography and every agent or node connected has private-key. Blockchain itself is useful for distributing ledger such as transactions, record transactions, and events in the transaction [7].

In digital networks, data is usually sent by copying it from one place to another. One of the main problems in this case is how to verify that the information received from the network is genuine and up-to-date. Although this is not a very difficult problem to solve itself, so far all solutions require putting trust in someone. In many cases, taking the trusted authority for authenticity of data is very good, but in some cases it really does happen. Even when it's okay and constantly having to use intermediaries or third parties for a high price, the reason why blockchain technology is perceived as annoying is because it has the ability to solve this authenticity problem without including a trusted broker. This allows anyone to verify the authenticity of the data independently, without having to take regardless of who or where the data originates from within the network [8].

Supply chain management is the strategic and systematic coordination of traditional business functions within particular firms and businesses in the supply chain for the purpose of improving the long-term performance of individual enterprises and the overall supply chain [9]. Supply chain management is an integrated system that coordinates the entire process in an organization or company in preparing and delivering products or services to consumers [10]. Supply chain management is the management of upstream and downstream relationships with suppliers and customers to deliver superior customer value at a lower cost to the overall supply chain [11]. Supply chain is a network of companies that work together to create and deliver a product into the hands of the last user [9]. There are three kinds of flow that must be managed, among others, the flow of goods flowing from upstream to downstream, the flow of money and the like that flows from upstream to downstream, the flow of information that can occur upstream to downstream or vice versa.

The supply chain network complexity based on the distribution channel is divided into five layers: the first layer consists of the importer, the second layer is the second owned distributor, the third layer belongs to the distributor medium, the fourth layer belongs to the small distributor, and the last fifth layer belongs to the customer, commodities between layers one and two are easy to manage for monitoring and control purposes, but the third, fourth and fifth layers are a growing layer, such as the number of distributors and small to medium businesses. The topology of supply chain network complexity is shown in figure 1 [12].
High speed, low cost, communication, and collaboration with customers and suppliers are critical success factors for managing the supply chain more effectively. The core of supply chain management is effective information and material flow across customer networks and suppliers. Of course, the benefits are based on using the correct process effectively and supporting information technology. Information, inventory positions, order fulfilment, inventory management, and all other information exchange activities will change the way products are sold, provide products, and make and receive payments for goods and services, the relevant speed of relevant information will be very fast as a result responding to changes that are not can be circumvented in the expected consumer demand and support processes that provide faster change in material flow to match demand [13]. The benefits of digital supply chain management include [14]:
1. Reduce the cost by 90%
2. Reduce the cost of purchasing goods and services by 2 to 6 percent
3. Help reduce costs and improve performance by strengthening procurement policies in product design and supply chain management

Through improving the quality of information, accessibility and time, digital supply chain is more transparent to achieve common goals.

**Cloud Computing**
Cloud computing is a technology that is easy to adopt with the simplest and latest architecture and this architecture presents information technology as a paid service in terms of deployment and maintenance,
cloud computing technology is not a new concept for most sectors such as bank, car, retail, health care, education, logistic [15]. Various cloud computing deployment models make adoption easy for all sectors, depending on usage requirements. This innovative technology makes collaboration easier among companies by using cloud [16]. Some of the major benefits of cloud computing are the reduction of hardware and software costs, better information visibility, computing resources managed through software as a service and faster deployment [17].

Cloud computing has three service models, namely Software as an Services (SaaS), Platform as an services (PaaS) and Infrastructure as an Services (IaaS). These services are delivered through industry standards such as Service-Oriented Architecture (SOA). SaaS is an application that is hosted as a service and provided to customers by using the Internet. Service providers maintain software maintenance and support related to the application. For example, CRM, Google Office, Salesforce, etc. PaaS provides a computing platform that is networked, servers, storage, and other services. Consumers create software and also control software deployment and configuration settings. Examples are Facebook, Google App Engine, Azure etc. IaaS provides storage, network capacity, and other computing resources based on rent. Customers use the infrastructure to deploy their services and software. They can manage or control OS, storage, applications, and network components. Examples of IaaS are OpSource, Blizzard, Gogrid, etc. [17]. The cloud computing architecture for SaaS can be seen in figure 3.

![Figure 3. Cloud Computing Architecture [17]](image)

**Cryptography**

Cryptography is the art and science to protect information from unwanted people and turn it into a form that cannot be distinguished by an attacker even if it is stored and sent [18]. The main purpose of cryptography is to keep data safe from unauthorized persons. Most cryptographic data are scrambling for data content, such as text data, image and audio related data, video-related data to compile unreadable, invisible or unenforceable data understood during a communication or storage process called Encryption. The opposite of data encryption process is called data decryption, this process can be described in Figure 4. Cryptography provides a number of security purposes to avoid security problems. Because the security advantages of cryptography, widely used today. The following are different purposes of cryptography, among others [18]:

1. **Confidentiality (Confidentiality)**
   No one can read messages excluding recipients in the future. Information in computer information is transmitted and should be contacted only by the competent authorities and not by unauthorized persons
2. **Authentication (Authentication)**
   This process proves one's identity. Information received by the system then checks the sender's identity that whether the information came from an authorized person or an unauthorized person or false identity.
3. **Non-Repudiation**
Non repudiation is a mechanism to prove that the sender actually sent this message. So if there is a sender who denies that he or she does not send a message, this method is not allowed to do such actions to the sender.

4. **Integrity (Integrity)**
   Only authorized parties modify the information or messages sent. No one can change the message given.

5. **Access Control**
   Only authorized parties can contact the information provided.

![Figure 4. Example Cryptosystem [18]](image)

In symmetric key encryption, the same key is used for both encryption and decryption processes. Symmetrical algorithms have the advantage of not consuming too much computing power and working at high speed in their encryption. Symmetric key encryption takes place in two modes as either a block cipher or as a flow cipher. In block cipher mode, the entire data is split into several blocks. This data is based on block length and key is provided for encryption. In the case of a stream cipher, the data is split as small as a single bit and randomized then encryption takes place. Symmetric key crypto systems are much faster than asymmetric key crypto systems [19].

**Symmetric Cryptography**
In symmetric key encryption, the same key is used for both encryption and decryption processes. Symmetrical algorithms have the advantage of not consuming too much computing power and working at high speed in their encryption. Symmetric key encryption takes place in two modes as either a block cipher or as a flow cipher. In block cipher mode, the entire data is split into several blocks. This data is based on block length and key is provided for encryption. In the case of a stream cipher, the data is split as small as a single bit and randomized then encryption takes place. Symmetric key crypto systems are much faster than asymmetric key crypto systems [19].

**Data Encryption Standard (DES)**
DES is a symmetric key algorithm developed by IBM in 1977. DES uses a 64 bit block size, 56 bit key size. DES always operates on blocks of the same size and uses permutations and substitutions in the algorithm. DES uses 16 rounds of transposition and substitution to encrypt each group of 8 (64 bits) plaintext letters and output from each round one by one. The number of rounds is exponentially proportional to the amount of time and keys using brute force attacks. Therefore the number of rounds increases then the security of the algorithm increases exponentially. DES is clearly no longer immune to the attack [20].

**Triple DES**
Triple DES is equivalent to DES operation. It uses a 64-bit key and an overall key length of 192 bits. Triple DES runs by typing all 192-bit keys (24 characters) rather than inserting each of the three
incidently keys. The procedure for encryption is exactly the same as DES, but this process is repeated three times. It's encrypted with the first key then decrypted with the second key, and finally encrypted again with the third key. The procedure for decrypting something is the same as the procedure for encryption, unless it accepts the same as the reverse process [20].

**Blowfish Algorithm**

The Blowfish algorithm is an important type of symmetric key encryption that has a 64 bit block size and variable key length from 32 bits to 448 bits in general [21]. It is based on 16 rounds of fiestel cipher networks that use large key sizes. The key size is greater because it is difficult to break the code in the blowfish algorithm. Additionally, with all the attacks separate from the attack to the key is very weak because of the larger key size and difficult to decode in the blowfish algorithm [18].

**SHA (Secure Hash Algorithms) 256**

SHA-2 was published in 2002 by the National Institute of Standards and Technology (NIST). SHA-2 is a stronger version of its predecessor SHA-0 and SHA-1. SHA-256 is the algorithm specified in the SHA-2 family, sharing functions similar to other versions with higher security such as SHA-384 and SHA-512 (see table 1). It calculates the digest of long arbitrary messages in the following way. The input message m is filled with one and zero to the message length (in bits) to multiples of 512. The last 64 bits in a layered message are used to store the original message length as a 64-bit number [22].

| Algorithm          | SHA-1  | SHA-256 | SHA-384 | SHA-512 |
|--------------------|--------|---------|---------|---------|
| Message Size       | <2^64  | <2^64   | <2^128  | <2^128  |
| Block Size         | 512    | 512     | 1024    | 1024    |
| Word Size          | 32     | 32      | 64      | 64      |
| Message digest size| 160    | 256     | 384     | 512     |
| Security           | 80     | 128     | 192     | 256     |

**Rijndael Algorithm**

The Rijndael algorithm also known as Advanced Encryption Standard (AES) is considered a new block cipher that also acts as a new substitute for Data Encryption Standard (DES). AES uses 128-bit blocks with only three types of 128-bit, 192-bit, and 256-bit encryption keys [23]. AES was formally selected by the National Institute of Science and Technology (NIST) after conducting a five-year standardization process. The famous name Rijndael comes from the Belgian creators Joan Daemen and Vincent Rijmen [24]. The AES algorithm is a block cipher because it processes individual data blocks with 128 bits fixed length with cipher keys that have variable key lengths independently selected as 128, 192 or 256 bits [25].

The generated sub-key is used as input with the round function. Rijndael is designed based on the following three criteria [26]:
1. Resistance to all known attacks
2. Speed and code on various platforms
3. Easy design

**Blockchain**

Blockchain is a distributed data structure consisting of a series of blocks. Blockchain acts as a distributed database or global ledger that keeps records of all transactions on the Blockchain network. These transactions are stamped and grouped into blocks where each block is identified by its cryptographic hash. The blocks form a linear sequence in which each block references the hash of the previous block, forming a block chain called blockchain. Blockchain is managed by a network node and each node executes and records the same transaction. Blockchain is replicated between the nodes in the Blockchain.
network. Each node on the network can read transactions [27]. Blockchain structure can be seen in figure 5.

![Blockchain Structure](image)

**Figure 5. Blockchain Structure [27]**

A blockchain consists of a data set consisting of a data packet chain (block) in which the block consists of several transactions (TX1-n, see Fig. 6). Blockchain is extended by each additional block and therefore is the complete ledger of transaction history. Blocks can be validated by the network using cryptographic means. In addition to a transaction, each block contains a time, hash value of the previous block, which is a random number to verify a hash. This concept ensures the integrity of all blockchains up to the first block. Unique hash values and fraud can be effectively prevented because block changes in chains will soon change their respective hash values [28].

The advent of blockchain technology in recent years also supports other concepts that have been suggested in the literature [28]. The concept is a smart contract, which combines computer protocols with a user interface to execute contract terms. Because of blockchain, smart contracts are becoming more popular because they can be used more easily by using blockchain compared to the technologies available at the time of their discovery 20 years ago. This innovative approach can, for example, replace lawyers and banks that have been involved in contracts for bidding assets depending on predetermined aspects [28]. Smart Contracts can also be used to control property ownership. This property may be real (e.g. home, car) or intangible (e.g. shares, permissions).

![Blockchain Example](image)

**Figure 6. Blockchain Example [28]**

2. Results
Based on previous research in Table 2, the researcher can describe the concept of digital supply chain development using blockchain technology with rijndael algorithm as in Figure 7.
| No | Year | Title                                                                 | Result                                                                                                                                                                                                 | Focus                                                                 |
|----|------|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| 1  | 2017 | A Hybrid Peer to Peer Framework for Supply Chain Visibility (Zhijie Li) | This study presents the physical distribution framework of the hybrid peer-to-peer supply chain that addresses this increasingly critical gap in global markets. Proposed blockchain technology to improve the security level of the proposed framework | Supply chain management and blockchain technology                       |
| 2  | 2017 | A Performance Test On Symmetric Encryption Algorithms-RC2 Vs Rijndael (Neeraj Anand Sharma, Mohammed Farik) | In this research the researcher concludes Rijndael Algorithm (AES) with 256 bit key length as the number one choice to achieve secure message transmission compared RC2 Algorithm, Rijndael Algorithm is the most preferred algorithm because the key length is 192 bit and 256 bit | Rijndael 256                                                          |
| 3  | 2017 | Blockchain (Michael Nofer, Peter Gomber et al)                       | Penelitian ini menyimpulkan inovasi blockchain ini dapat mengubah banyak model bisnis yang ada, menciptakan yang baru dan mungkin memiliki dampak buruk pada seluruh industri. | Blockchain                                                            |
| 4  | 2017 | Digital Supply Chain Transformation toward Blockchain Integration (Kari Korpela, Jukka Hallikas, Tomi Dahlberg) | This research describes how supply chain integration through blockchain technology can achieve disruptive transformation in digital supply chains and networks | Digital Supply chain and Blockchain                                   |
| 5  | 2016 | Blockchain Platform for Industrial Internet of Things (Arshdeep Bahga and Vijay K. Madisetti) | The study presents a decentralized, peer-to-peer platform called BPIIoT for the Internet of Things Industry based on Blockchain (BC) technology. Using BC Technology, the BPIIoT platform allows peers in decentralized, unreliable, peer-to-peer networks to interact with each other without the need for a trusted intermediary | Blockchain                                                            |
| 6  | 2016 | FPGA Based Hardware Implementation of AES Rijndael Algorithm for Encryption and Decryption (Srinivas, N.S and Akramuddin, MD) | This study presents the hardware implementation of AES Rijndael Encryption and Decryption algorithm using Xilinx Virtex-7 FPGA, the results of the implementation conclude the proposed architecture has good efficiency in terms of latency, throughput, speed / delay, area and power | Rijndael 256                                                          |
| 7  | 2016 | The Blockchain Phenomenon (Juri Mattila)                             | In this working paper the author of the paper discusses phenomena occurring in finance, payment, identity management, supply chain, smart contract, internet of things, voting systems and decentralized autonomous organizations | Blockchain                                                            |
| 8  | 2016 | Trends in industrial supply chains and networks (Katarina Kemppainen and Ari P.J. VepsäEläEinen) | In this explorative research, researchers analyze SCM changes both in terms of operational practices and organizational capabilities in some industrial companies. A focused survey tracked the development of supply chains and networks over the past two decades. Pay attention to the expected growth in the use of IT support systems, the extent to which information sharing and scope of coordination efforts. | Supply chain management                                                  |
| 9  | 2015 | E-Supply chain management : The New Competitive Weapon (Anil Vashisht, Manor Pandey, and Devendra Kumar Pandey) | The study concludes that companies using e-business to redefine supply chain integration will achieve significant efficiency improvements and gain tremendous competitive advantage over their competitors. | Digital Supply chain management                                       |
Table 2. Previous research

| No | Year | Title | Result | Focus |
|----|------|-------|--------|-------|
| 10 | 2014 | Cloud computing technology: reducing carbon footprint in beef supply chain (Akshit Singh et al.) | In this study, an integrated system is proposed using Cloud Computing Technology (CCT) where all stakeholder supply chain beef can minimize and quantify carbon emissions in the end with reasonable costs and infrastructure. An integrated approach to map the entire supply chain of beef by cloud computing will also enhance coordination among stakeholders. | Supply chain management |

So the researcher concludes that the application of digital supply chain using blockchain technology with rijndael algorithm will produce data verification concept with easy resistance, speed and design for the implementation of digital supply chain using blockchain technology, if described the steps of applying digital supply chain using blockchain technology with rijndael algorithm 256 will be reflected in Figure 7.

![Figure 7. Rijndael 256 Algorithm](image-url)

3. Conclusion
From the concepts, the researcher concludes the application of blockchain technology with the data structure can be applied by sharing encryption and can be applied in some cases, such as data verification for face recognition, artificial intelligence or machine learning. The obstacles in this study in terms of testing systems that require a long time and validation of data to answer whether this blockchain technology is accepted to the public in general in various respects. For research in this paper the researcher makes the concept of application of blockchain with Rijndael 256 algorithm.
References

[1]. Evangelista, P., McKinnon, A., & Sweeney, E. (2013). Industrial Management & Data Systems. Technology Adoption in Small and Medium-Sized Logistics Providers, 113 (7), 967-989.
[2]. Robak, S., Franczyk, B., & Robak, M. (2013). Applying Big Data and Linked Data Concepts In Supply Chains Management.
[3]. Robak, S., Franczyk, B., & Robak, M. (2012, November 20). (IEEE, Ed.) Applying Linked Data Concepts in BPM.
[4]. Li, Z. (2017, May). A Hybrid Peer To Peer Framework For Supply Chain Visibility.
[5]. Korpela, K., Halliska, J., & Dahlberg, T. (2017, January 04). Digital Supply Chain Toward Blockchain Integration.
[6]. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How Technology Behind Bitcoin Is Changing Money Business And The World. New York: Penguin Random House LLC.
[7]. Sikorski, J. J., Haughton, J., & Kraft, M. (2017). (J. Yan, Ed.) Blockchain Technology In Chemical Industrial: Machine-to-Machine Electricity Market, 195, 234-246.
[8]. Mattila, J. (2017, February 09). Berkeley Roundtable On The International Economy.
[9]. Pujawan, I. N., & Mahendrawathi. (2010). Supply Chain Management (Second Edition ed.). (I. K. Gunarta, Ed.) Guna Widya.
[10]. Martono, R. (2015). Manajemen Logistik Terintegrasi (1st Edition ed.). (Retnowati, & Vani, Eds.) PPM Manajemen Publishing.
[11]. Christopher, M. (2011). Logistics & Supply Chain Management (Vol. 4). Prentice Hall Financial Times.
[12]. Ma'arif, M. R., & Lee, Y. H. (2013). Visualizing Complex Supply Chain Network on RFID-based Environment by Using Clustering Approach in ProM Framework.
[13]. Vashisht, A., Pandey, M., & Pandey, D. K. (2015). International Journal of Logistics & Supply Chain Management Perspectives. E-Supply Chain Management: The New Competitive Weapon, 4 (2).
[14]. Anwar, S. N. (2013). Journal Ekonomi. Manajemen Rantai Pasokan (Supply Chain Management): Konsep dan Hakikat, IV, 1-7.
[15]. Al-Hudhaif, S., & Alkubeyyer, A. (2011). E-commerce Adoption Factors in Saudi Arabia. International Journal of Business and Management , 122-33.
[16]. XuanXu. (2012). From Cloud Computing to Cloud Manufacturing, Robotics and Computer-Integrated Manufacturing. 75-85.
[17]. Singh, A., Mishra, N., Ali, S. I., Shukla, N., & Shankar, R. (2014). Cloud Computing Technology: Reducing Carbon Footprint in Beef Supply Chain.
[18]. Tripathi, R., & Agrawal, S. (2014). International Journal of Advance Foundation and Research in Computer. Comparative Study of Symmetric and Asymmetric Cryptography Techniques, I (6).
[19]. Mittal, M. (2012). International Journal of Computer Applications. Performance Evaluation of Cryptographic Algorithms, 41.
[20]. Kumar, Y., Munjal, R., & Sharma, H. (2011). International Journal of Computer Science and Management Studies. Comparison of Symmetric and Asymmetric Cryptographic with Existing Vulnerabilities and Countermeasures, II (03).
[21]. Thambriraja, E., Ramesh, G., & Umarani, R. (2012). International Journal of Advanced Research in Computer Science and Software Engineering. A Survey on Various Most Common Encryption Techniques, II (7).
[22]. Nofer, M., Gomber, P., & Hinz, O. (2017). Business & Infomation System Engineering. Blockchain, 59 (3), 183-187.
[23]. Daeman, J., & Rijmen, V. (2011). Encyclopedia Of Cryptography and Security. Boston: Springer.
[24]. Sharma, N. A., & Farik, M. (2017). A Performance Test On Symmetric Encryption Algorithm - RC2 VS Rijndael. International Journal Of Scientific & Technology Research, 6 (07).
[25]. Srinivas, N. S., & Akramuddin, M. (2016). International Conference on Electrical, Electronics, and Optimization Techniques. *FPGA Based Hardware Implementation of AES Rijndael Algorithm for Encryption and Decryption*.

[26]. Singla, S., & Singh, J. (2013). Global Journal Of Computer Science And Technology Software & Data Engineering. *Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm, XIII* (5).

[27]. Bahga, A., & Madisetti, V. K. (2016). Journal of Software Engineering and Applications. *Blockchain Platform for Industrial Internet of Things, 9*, 533-546.

[28]. Bañuelos, L. G., & Ponomarev, A. (2016, December 9). *Optimized Execution of Business Processes on Blockchain*. 