Enhanced Blockchain Transaction: A Case of Food Supply Chain Management

Md. Ratul Amin, Megat F. Zuhairi and Md. Nazmus Saadat
Universiti Kuala Lumpur, Kuala Lumpur, Malaysia

Abstract: Distributed ledger technology is an immutable data storage and transparent system, which is a constituent component that empowers the Food supply Chain Management (FSCM). Due to the immutable data feature, the scalability of blockchain technology is quite a challenge. In essence, blockchain data may grow rapidly as compared to the existing approach, and such circumstances is an issue that need to be addressed. Also, high volumes of data process for each transaction verification couple with long period of time for computation, lead to high overhead and resource consumption. This study discusses improved methods to reduce the amount of data generated by system. The proposed method employs the header verification system for transaction to reduce data growth and data processing time. During transaction, this method will verify only the header file information with using Merkle tree. This system is able to store each transaction of a node and form blockchain. Subsequently, each node is capable to verify valid transactions only by use of header data without maintaining full data of blockchain. The expected outcome of the scheme is the significant decrease of data growth in blockchain.

Key words: Blockchain, food supply chain, block hashes, verification

INTRODUCTION

Food supply chain management is essential for both the food producer industries and consumers. Such system is designed to ensure transparency of food handling and process, leading to high quality of food production. Nonetheless, the Food Supply Chain Management (FSCM) is a lengthy process, which includes supplier, manufacturing, distributor, retailer and consumer. Each product is relayed through various stages of FSCM where information is recorded relevant to the product. In the end, every food product carries unique data along the FSCM process. The recorded data is vital because it provides feedback to the manufacturer as well as consumer about the source and the handling mechanism of the products. However, the challenges of the existing system are to sustain the integrity of information along the chain. Data tampering is one of the issues that severely affect the system (Xie et al., 2017; Bocek et al., 2017). This is due to the fact that conventional FSCM employs the traditional database process.

The blockchain technology enables digital data to be stored in a form of distributed shared ledger, i.e., distributed database (Imeri and Khadraoui, 2018). Blockchain is composed of a chain of data block created through crypto hash key. Basically, every data block consists of timestamp, transaction, previous key, and private key data which is incontestable for multiple network transactions. Once the data has been verified and added to the blockchain, the data will be permanently stored in the database. To modify a single node either permissioned or permissionless blockchain, more than 51% of the blockchain computing resources must be controlled (Lin and Liao, 2017). Such is the fundamental characteristic, leading to the immutable feature of blockchain. This study highlights the inherent properties of blockchain, utilized to ensure transparency to every user through this system (Imeri and Khadraoui, 2018). Blockchain technology is first used in Bitcoin (2008) and Xu et al. (2017), the first digital currency introduced in financial transaction. Due to the realization of bitcoin, service providers can now commercially employ blockchain technology for banking transaction, IoT application, supply chain, voting, medical treatment and etc.

Since, 2015, there is a growing interest of blockchain to be used in supply chain, on the account that the technology may still have significant challenges. To improve the efficiency of blockchain transaction, many research works exists to mitigate some of the issue (Wang et al., 2019). Firstly, blockchain performance is inferior as compared to the traditional system counterpart. It is because when a transaction is executed, a blockchain employs similar computation resources as compared to the traditional database process. However, a distributed ledger system is required to process a single transaction three-fold, i.e., verification, consensus mechanisms, redundancy. In addition, the node has to download the complete blockchain data for verification (Rouhani and Deters, 2017). Secondly, blockchain the rate of growth of data is higher than the traditional system because each block piggybacks the previous hash key. Consequently such approach may affect data processing time and data storage cost. In this study, the proposed scheme is able
to reduce the rate of data growth by using effective low bit hash signature. Subsequently, only the header block is downloaded for verification to minimize the resources incurred. Such mechanism can profoundly shrink the node’s storage growth. Third, much of the existing systems are tightly bound to traditional-based, therefore, incorporating blockchain system on the such system may cause the affect the data processing time. To that end, this paper provides an improved blockchain mechanism, where a new approach offers to minimize transaction overhead while maintaining the virtue of the present framework. Fourth, the IoT integration is another challenge in blockchain, where low power and lossy network may affect the efficacy of the blockchain transaction.

**Literature review:** The FSCM is a pressing issue which warrant research (Wang et al., 2019). In October 2016, big retail industries, i.e., Walmart and IBM have collaborated with Tsinghua University to explore the opportunities of blockchain in food products authentication and supply chain operation (Sternberg and Baruffaldi, 2018). Walmart is one of the crucial IBM clients for testing the distributed ledger technology for FSCM. In another research work (Wang et al., 2019), Provenance Ltd. explores the value of blockchain in our society. The outcome of the work has identified a substantial reduction of food material waste during production and blockchain is able to keep good relationship between consumer and organization. In 2013, 50,000 tons of meat sold as beef but founded to contains horse DNA. To protect the consumers from the increasing risk of food fraud the Provenance Ltd. has developed a blockchain based supply chain. The new approach ensures every product to be physically embedded with a digital ‘passport’ that proves authenticity and origin of the raw source. Such technique also enables an auditable record of the journey for all physical food products.

According to Euromonitor International (Zhen and Mansori, 2012), Malaysian food and beverage retail industries such as packed foods, dairy and bakery markets are substantially growing. Within the ASEAN countries, Malaysia has the biggest daily intake of fresh fish and seafood expenditure per capita (Ahmad et al., 2015). In 2011, the domestic fish supply was estimated at 1.6 million tons, and almost one third of the product are imported. And there is also potential customer demand for imported beef, chicken, mutton and many types of halal products. In addition, food producers are also keeping the pace of the competition by creative marketing to promote their products. To date, in Malaysia, 8 industries out of 16 the annual growth will be higher at 2025 than the previous 10 years annual growth. According to New Zealand Trade and Enterprise, food manufacturing industries (2.4%) is one of them (Ahmed, 2012; Chan et al., 2014).

The rise of demand for ready-made food packed for consumers causes the producers to struggle to meet the demand. As a result, quality is compromised for quantity. Food products are now at the risk of being contaminated due to poor hygiene and handling. Food poison is the result of taking contaminated, spoiled or toxic food (Ndraha et al., 2018). In places with low quality of food handling, food poisoning is a not uncommon. In addition to the low-quality packed food and couple with high humidity climate, foods can be easily contaminated with micro-organisms. The high demand also has led to some food producers and distributors to temper with the expiry date (Tian, 2017). Such fraud has severe impact on consumers (Tian, 2016). Based on the points previously stated, FSCM indeed is facing many problems such as supplier raw materials quality, manufacturer original equipment, packaging, safely transportation, and warehousing (Nakasumi, 2017; Chen et al., 2017). Therefore, it is deemed imperative that a new mechanism to improve the existing FSCM is needed.

The current approach of supply chain process is acceptable but it requires to implement an advance method to improve the consumer trustworthiness on the food product. Blockchain is the potential technology which can avoid, if not all the data tampering of such product. An essential feature of blockchain is the immutability of data. Data immutability and data share is the preventive strategy for food quality and security management which is able to enhance consumer confidence in the food system (Tse et al., 2017).

Recent application of blockchain in various industry has caught the interest of some research work for the application in FSCM. Caro et al. (2018) has implemented an efficient blockchain-based solution known as P2P (peer-to-peer) digital ledger to eliminate the issues previously discussed. In the research work, the blockchain network has many nodes which are sparsely distributed and communicates with each other by P2P mode (Angrish et al., 2018). Every participant in the blockchain network can independently interact with other nodes that are connected in the network (Imeri and Khadraoui, 2018). From the business perspective, the data security is a crucial issue in the current world. The data stored in the blockchain is cryptographically signed. Therefore, if someone desires to tamper the data such action shall invalidate the chain of hashes. In addition to immutability feature, blockchain mechanism is also deemed to be transparent due to the fact that every nodes must approve a pair of transaction in the network, thus, requiring the data to be visible.

In principle, the blockchain technology employs different types of cryptography algorithm, i.e., Rivest Shamir-Adleman (RSA), Elliptical Curve Digital Signing Algorithm (ECDSA), Secure Hash Algorithm (SHA). RSA is an ISO standard public key that was developed in 1978 (Karakra and Alsadeh, 2016) for financially secure
transaction (Wu and Wu, 2017). But this algorithm generates large number of keys. ECDSA is a public/private cryptography key (Islam et al., 2018). The ECDSA use a much smaller keys to obtain the same level of security of RSA. The SHA-1, SHA-2 (SHA-224 and SHA-256) is very well-known algorithm and SHA-2, which takes fewer time to generate the key (Omran and Jumma, 2017). This algorithm key length is 512 bits and considering hexadecimal Y [0-15] words of 32 bits.

In recent years, blockchain technology is the way forward to the traditional technology-based food supply chain management. Such technology is becoming prevalent for food supply chain management. Blockchain may be able to solve much of the fundamental problem of traditional technologies (Casado-Vara et al., 2018; Swan, 2018). Nevertheless, blockchain has many implementation challenges (Imeri and Khadraoui, 2018). The researcher described goods flow in FSCM but fail to present a multi-user design because of blockchain implementation challenges. In another research work (Imeri and Khadraoui, 2018) food tracking for data security is guaranteed by use of blockchain technology (Yao et al., 2016). Some of the challenges of implementing blockchain in FCSM are high integration cost, i.e., time and money (Mondragon et al., 2018; Caro et al., 2018), hardware fork, software fork (Gilbert and Dasgupta, 2017; Xie et al., 2017) and slow performance (Islam et al., 2018). The first project of pharmaceutical supply chain-based on blockchain has measured 7576 temperatures points with ten minutes (Bocek et al., 2017). Blockchain require 10 min to confirm a single transaction (Tian, 2017). On the contrary, it takes only a few seconds to confirm a transaction on the Visa-card system while Bitcoin need 10 min processing time per transaction (Liu et al., 2017). Such performance is not practicable for business environment. In research works (Banerjee, 2018; Tse et al., 2017) blockchain and traditional system such as Political, Economic, Social, Technological (PEST) analysis, Enterprise Resource Planning (ERP) and Content Management System (CMS) are integrated, PEST analysis can scan only external environment. The technique needs high integration cost and slow performance challenges (Kshetri, 2018; Viriyasitavat and Hoonspon, 2019). In a report survey of blockchain (Lin and Liao, 2017) and based on the output of Blockchain Economic Summit in Malaysia (August, 2018), blockchain is still an inadequately accepted technology. The main reasons are high implementation cost, high transaction time cost, cyber security, highly data growth (Leng et al., 2018) and old market authority’s policy.

Existing system and proposed scheme: In much of the related work previously presented, many improvement efforts focusing on transparency in the blockchain are done. The aim is to minimize the cost incurred while finding effective potential of utilizing distributed ledger technology. Naturally, each block contains main data such as crypto-hash of previous block, crypto-hash of current block, timestamp and transactions. Only genesis block does not have the previous block hash. Figure 1 illustrates the stored data block structure and relation of each other’s in block-chain.

The block header hash signature is not sent by the network but instead is calculated by every node as part of the verification process of every block. Transaction is the main constituent of the blockchain. When a transaction is executed in the blockchain, a block of chain generates hashes which is then broadcast to every node. The amount of transaction records in a single network of blockchain can be extremely large. In addition, blockchain technology employs Merkle tree function to produce the final hash value, known as Merkle tree root. The final hash value is fixed in a block header, i.e., current block hash by using Merkle tree function. In addition, other constituent of the information such as timestamp, i.e., block generated time, signature of the block, and nonce value are used for securing a user’s identity. Blockchain provides distribution and trusted consensus mechanism in which data of FSCM products during the logistics method could be stored and accessed by both providers and consumers through smart contract (Bocek et al., 2017).

Block header verification: The current blockchain technology maintain the entire blockchain data for verification during transaction time (Palai et al., 2018). The amount of computing resources required for such operation is considered significant and accountable for slow performance (Lin and Liao, 2017).

Figure 2 demonstrates blockchain base current system and some nodes. The node H is as a new node just has connected in this system. If node H is to perform a transaction with node C, node H have to maintain full data of node C for verification.

Blockchain verifies each transaction through the process shown by Fig. 3. Such mechanism is also used in Bitcoin transaction verification. Transaction 2 made is by using the data contained by transaction 1.

Once the verification of transaction 2 is completed, then transaction 3 is verified based upon the data in the previous transaction, i.e., transaction 2. The process is deemed completed when each transaction in the chain is verified. As such, the amount of time to verify each block in the chain will be significantly high. However, in this study, the proposed algorithm maintains only the header file for verification. The header file is proved with using Merkle tree, where it keeps every hash key. During a transaction, only the current header file will be downloaded for verification. Therefore, this system is able to minimize the overhead incurred by reducing the
If the transaction number is odd, this system by default will create another transaction to ensure an even number of transactions is produced. For instance, transaction number five i.e., $H_4$ is to be verified. Merkle tree can be used to ensure that the $H_4$ hash key is not corrupted. To do this, initially the Merkle Tree will check in what way $H_4$ generates the binding with other transaction:  

$$H_4 + H_4 = H_4$$

Then, it will check whether $H_4$ peer has been combined with another peer, for instance:
Subsequently, $H_{4567}$ is further combined and verified with another pair of hash key:

$$H_{0123} + H_{4567} = H_{01234567}$$

By using this approach, eventually the last key $H_7$ is verified. If the key is correct, the transaction will proceed, otherwise the process is halted. Header key verification algorithm is able to reduce process time and data growth. The subsequent points describe the calculation of header data size and shows how the algorithm is capable to
improve blockchain transaction. Assume that a single block size of blockchain is at 1 Mbyte (Zheng et al., 2018; McGinn et al., 2016). The block size is the total of the block header data size and the list of transactions data size. The block header keeps all these data:

- Version = 4 bytes
- Previous block header hash = 32 bytes
- Merkle root hash = 32 bytes
- Time = 4 bytes
- nBits (encoded POW target) = 4 bytes
- Nonce = 4 bytes

Therefore, the block header size = 4+32+32+4+4+4 = 80 bytes. The list of transactions is shown below:

- Transaction count = 1-9 bytes
- Transactions = varies

In each block, the number of transactions could vary. The below list is the calculation of a single transaction byte:

- Version-4 bytes
- Transaction in size = 1-9 bytes
- Transaction of data size is shown below:
  - Previous transaction out hash = 32 bytes
  - Previous transaction out position = 4 bytes
  - Public key script = varies depending on script (max 10,000 bytes)
  - Signature script = varies
  - Sequence = 4 bytes
  - Transaction out size = 1-9 bytes
  - Transaction data size is described below:
    - Value = 8 bytes
    - Pubkey script length = 1-9 bytes
    - Pubkey script = varies
    - Locktime = 4 bytes

Assume H is a new node with 10 transactions and C is an old node with 300 transactions, where every block size is 1 Mb. Table 1 shows the comparison of the current blockchain technology approach and proposed scheme. Scalability has always been an issue with blockchain. The most significant and relevant problem is the block size which is currently almost around at 1 Mb. The average Bitcoin transaction size is around 495 bytes. Therefore, the calculation of transactions of each block is:

\[
\text{Maximum block size/Average transaction size} = \frac{\text{Average transaction per block}}{1000000 \text{ bytes}/495 \text{ bytes}} = 2020 \text{ transaction}
\]

Bitcoin need 10 min for confirmed a transaction. To calculate transactions per second (tps), the equation used is below.

\[
\text{Number of transactions per block/Block time in seconds} = \text{Transactions sec}^{-1}
\]

2020 transactions/600 Sec = 3.37 transaction sec\(^{-1}\)

Similarly, BitcoinPlus needed 50.5 transactions per second because it needs one minute to confirm a transaction. On the other hand, the proposed system take less than one minute to confirm a transaction, and as such, the transaction per second will be significantly improved.

**CONCLUSION**

This study has described the natural properties of blockchain base technology with header file verification during transaction for FSCM. Blockchain offers to address the fundamental challenges present in the traditional system but it has a setback of high data growth. The proposed scheme is able to mitigate such problem. The scheme is capable to make transactions by using only header file verification without maintaining the whole data of blockchain. In addition, this system can significantly reduce data growth and the data processing time.

**REFERENCES**


