ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Information Sharing by Block Chain Technology for Supply Chain Management

[1] Mrs. Divyaprabha K N, [2] Chaithra G, [3] Aishwarya M, [4] Kumudha M
[1] Assistant Professor, SSEC, Bangalore
[2][3][4] UG Scholar SSEC, Bangalore.

Abstract: **- The management of upstream and downstream value-added flows of materials, final goods, and related information among the companies, distributors, resellers, and final customers can be termed as the main objective of Supply Chain Management. But, at times due to base on virtual data, there occur chances of the failure of the algorithm used to devise the flow plan due to the variations, in the information shared among the people in the supply chain. The data shared between manufacturers, suppliers and customers are affected.**

Keywords— Supply chain management; Blockchain; SCM

I. INTRODUCTION

Now, high pressure on the prices and the global competition forced manufacturers to focus on their core competences like engineering and final assembly as original equipment manufacturers thus outsourcing almost the whole manufacturing operations. These higher levels of complexity are the result of random changes in manufacturing and distribution, including globalization and outsourcing. As a result, independent firms manage different parts of global supply chains. Each firm in the supply chain sets strategic and operational goals to maximize its own profit by using local information such as cost structures, profit margins and forecasts. Even though advances in information technology enable firms to collect, process, and share information, firms may be reluctant to do so because of conflicting incentives. Aligning incentives improves firms' profits and sustains the use of information technology. In this situation, it is important to build competitive supply chain. To build it, Information in supply chains is one of the most valuable resources for manufacturers. The coordination of information, as well as operations and logistics optimization, has become increasingly order to overcome this problem, it is necessary to ensure reactivity towards markets variability. Especially, Double Benefit for the distributors is a widespread and serious problem in supply chain management which leads to supply insufficiencies, in the cases of both deterministic and random demands. This paper proposes a Block Chain based solution to address the problems of supply chain such as Double Marginalization I.e. Double Benefits and Variations in Shared Information etc

The main motto of this paper to avoid the customer of facing a double marginalization problem, it may cause by the suppliers of the company.

II. PROBLEM OF SUPPLY CHAIN

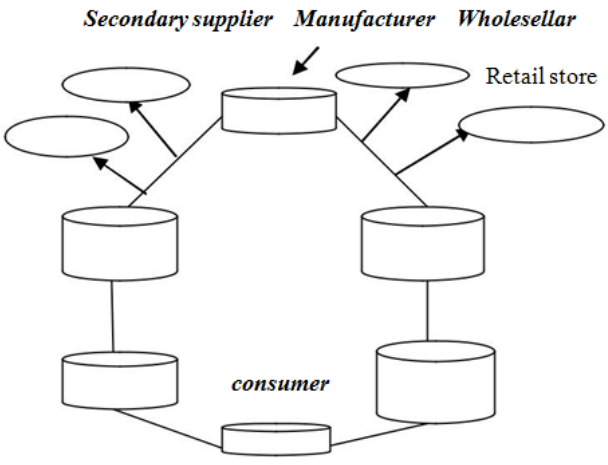
Demand forecasting is becoming difficult because of short product life cycles and long production lead-times. Then, supply chains face the risk of either excess capacity due to low demand realization or lack of product availability. In a decentralized supply chain, lack of proper capacity risk sharing increases the cost of capacity risk. To deliver on time, the contract manufacturer secures capacity in advance of an original equipment manufacturer order. For such a supply chain, if consumer demand turns out to be high, both the contract manufacturer and the original equipment manufacturer face upside capacity risk. However, if consumer demand turns out to be low, only the contract manufacturer faces downside capacity risk To reduce capacity risk for each party depends on the contractual agreements. Under a wholesale price contract, the original equipment manufacturer pays a wholesale price W to the contract manufacturer for each unit ordered and sells the product to the market at R per unit. The contract manufacturer secures capacity at a unit cost of C, which could represent an equivalent annual cost of capacity. So, the contract manufacturer's

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

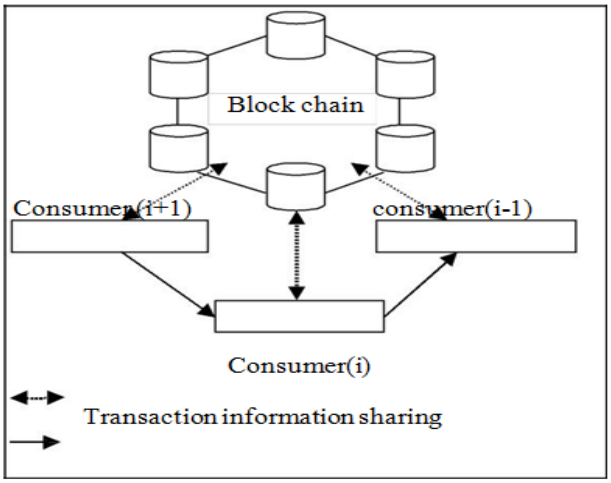
marginal profit W-C is less than the vertically integrated supply chain's marginal profit R-C. This difference is known as double marginalization. The contract manufacturer protects itself by securing less capacity than what would be optimal for a vertically integrated supply chain. The original equipment manufacturer may eliminate this adverse effect of decentralization by sharing the contract manufacturer's upside capacity risk. Thus, the contract manufacturer's marginal cost is C, whereas the original equipment manufacturer's marginal cost is zero. This all transaction makes the consumer to face the Double marginalization problem. To maximize profit of each party, the original equipment manufacturer can agree to pay back P per unit of unused capacity. This would reduce the contract manufacturer's marginal cost to C-P, and induce the contract manufacturer to build a higher capacity, thus aligning incentives. We refer to this as a payback contract. But this payback contract deals between contract manufacturer and original equipment manufacturer order, this will not give solution for consumer/customer problem. So, to prevent the double benefit to the supplier of the companies by cheating a consumer. We must provide the proper communication or interaction between each domain of the companies with the consumer using the supply chain management(SCM)and Block chain concept.

Fig:1 Information sharing using SCM



III. PROPOSED SOLUTION

Previous research works have discussed the benefits of information sharing throughout the supply chain. Sharing data such as machine loads, sales previsions and inventory positions has proven to improve the fulfil rate and the product cycle time and to decrease order fluctuations. However, it is difficult to share information in global supply chain because there are many code schemes. Using EDI network is an easy solution to integrate code schemes and realize visibility of supply chain, but it is expensive especially for small businesses. If they try to integrate their code schemes and realize visibility of supply chain by using same ERP package such as SAP, it makes another problem. Most companies don't necessarily want to share information, because they don't want to share their capacity with competitors. It is also necessary to consider about access control on information sharing scheme. It can be difficult to receive and interpret status updates from numerous carriers, brokers, and freight forwarders to gain a comprehensive perspective and assess performance and bottlenecks. Without this bird-eye's perspective, it becomes nearly impossible to implement cost-saving strategies, such as just-in-time inventory replenishment. When delivery windows are tight, even minor missteps and miscalculations can have major cost and service level consequences. For satisfying these requirements, we consider low cost and access controllable database system. In recent years, a new distributed database system emerged. The system was Bitcoin, which allows users to transfer currency (bitcoins) securely without a centralized regulator, using a publicly verifiable open ledger (or blockchain). Since then, Bitcoin demonstrated how these blockchains can serve other functions requiring trusted computing and auditability. While companies earn the benefits of information sharing via blockchain, there is growing a company's concern about protection of the order content. So, there is a possibility to satisfy the requirements as mentioned above.



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

IV. RELATED WORKS

There have been various attempts to address data protection issues. Across the industry, leading companies chose to implement their own proprietary authentication software based on the OAuth protocol, in which they serve as centralized trusted authorities. From a security perspective, researchers developed various techniques targeting data protection concerns focused on transaction data. Data anonymization methods attempt to protect personally identifiable information. k-anonymity, a common property of anonymized datasets requires that sensitive information of each record is indistinguishable from at least k_1 other records. Related extensions to k-anonymity include l-diversity, which ensures the sensitive data is represented by a diverse enough set of possible values; and t-closeness, which looks at the distribution of sensitive data. Recent research has demonstrated how anonymized datasets employing these techniques can be de-anonymized given even a small amount of data points or high dimensionality data. Other data preserving methods include differential protection, a technique that perturbs data or adds noise to the computational process prior to sharing the data and encryption schemes that allow running computations and queries over encrypted data. As you know, there are similar schemes such as smart contract. NXT is a public blockchain platform which includes a selection of smart contracts that are currently live. Ethereum is a public blockchain platform which is currently the most advanced smart contract enabled blockchain. With a "Turing complete" coding system, theoretically you can put any logic into an Ethereum smart contract, and it will be run by the whole network. There are mechanisms in place to prevent abuse, and you need to pay for compute power, by passing in "ETH" tokens, which act as payment for the miners who run your code. Enigma provides the first solution for protecting data-in-use. Share data with others for processing without giving it away. Data are guaranteed to be encrypted always, even when complex analytics are required. Our blockchain scheme has no valuable things such as virtual currency to avoid hacking. Miner can earn the transaction fee and it uses only computational power in the network.

V. CONCLUSION

In this paper, we proposed a new blockchain scheme for information sharing. It brings many benefits for supply chain management. In general, Transaction data should not be trusted in the hands of third-parties, where they are susceptible to steals and misuse. Instead, users should own and control their data without compromising security or limiting companies' and authorities' ability to provide encrypted transactions. Our platform enables this by combining a blockchain with a homomorphic encryption solution. Users are not required to trust any third-party and are always aware of the data that is being collected about them and how it is used. In addition, the blockchain recognizes the users as the owners of their encrypted data. Companies, in turn, can focus on utilizing data without being overly concerned about properly securing and compartmentalizing them Furthermore, with a decentralized platform, making legal and regulatory decisions about collecting, storing and sharing sensitive data should be simpler. Moreover, laws and regulations could be programmed into the blockchain itself, so that they are enforced automatically. In other situations, the ledger can act as legal evidence for accessing (or storing) data. We recognize some problems to be solved. For example, Search operation for emergency order brings heavy load to Miner. We need to consider about efficient incentive mechanism.

REFERENCES

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf [Accessed March 2017]

[2] R. L. Rivest, L. Adleman, and M. L. Dertouzos, On data banks and privacy homomorphisms, Foundations of Secure Computation Academia Press, pages 169–179, 1978.

[3] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inf. Theory 31(4), 469–472 (1985)

[4] R. Cramer, V. Shoup, A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, in Proceedings of Advances in Cryptology, CRYPTO'98, 1998, pp. 13–25

[5] M. Abdalla, M. Bellare, P. Rogaway, DHAES: an encryption scheme based on the Diffie–Hellman problem. Submission to IEEE P1363a, 1998. http: // www. di.ens.fr /~mabdalla /papers /dhes. pdf