Secure Methods for Supplychain Management to Protect from Attacks in Blockchain

B. Ratnakanth[1], K. Venkata Ramana[2]

[1]Research Scholar, [2]Assistant Professor

Department of Computer Science & System Engineering, Andhra University College of Engineering (A), Visakhapatnam, India

Abstracts: ***The expatiation of increase in demand variations in today's globalized supply chain economy is disruptive, costly which is every supply chain management wants to reduce. The traditional supply chain management system's attribute to high complex centralized organizational structures, increased costs throughout Supply Chain, Poor system design; need for improved speed, quality and service. The speed, expenditure and levels of security employed in traditional supply chain management model depends on few hands in the organizational committee. Hence, this dynamic behaviour of customers indicates the need for a secure, decentralized and a trusted environment to function with. Decentralization improves the performance of Supply Chain in its way of distributing its decisions on financial aspects. The most erupting technology - Blockchain provides an efficient and viable solutions to the aforementioned hurdles that are restricting today's supply chain. Through blockchain, massive networks of decentralized autonomous individuals and organizations can grow and operate seamlessly within a decentralized, distributed operating platform. The problems that arise in blockchain can be like – changing fair data to malicious data that is collected from web pages, Synchronization of information and data in the network, disruption to services etc. In this paper an efficient top-down method is employed for testing various participating entities and modules in this Supply Chain Model. An in-depth analysis for the root-cause of different kinds of threats, vulnerabilities and risks is conducted on the supply chain management system as simulated in various environments***

Keywords: Supplychain management, Blockchain, Attacks, Secure methods, JVM environment

1. Introduction

In the era of digitalization, the people in the society are more consumeristic nature. Consumers demand customizable products tailored to their needs, simplified buying experience and transparency in the real value of goods. These needs have created both the new opportunities and challenges in the current supply chains. The major activities and procedures in a supply chain incorporates that: obtaining raw materials and ancillary components, manufacturing and assembly, warehousing and inventory tracking, order access and order management, sharing among all entities, delivery to the consumer, and to manage and monitor of these activities. The view of [1], that the activities are mapped into four vital procedures, such as plan, source, make and deliver.

The coordination among these processes is very complex task. Thus, the discipline of supply chain comes in the picture. The standard definition was proposed by the council of Supply Chain Management professionals (CSCMP)[2]. According to their notion "The planning and management of all activities involved in sourcing and procurement, conversion, and all Logistics Management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third-party service providers, and customers. In essence, SCM integrates supply and demand management within and across companies".

From the above stated definition, SCM provides a lot of coordination and cooperation among the different entities, and so, manage the information flow between the resources. The goal is to minimize total cost of information flow among these stages [3].

1.1 Challenges in SCMs

After rigorously studying the concept of supplychain evolution, we have identified some challenges mentioned below:

1) In supplychain, there are many stakeholders involved and multiple operations performed to move product from manufacturer to customer. The main challenge in supplychain is the synchronization, the flow of information across the supplychain.
2) The flow of information across the supply chain may contain sensitive information and also payment process involved by using third party service, which is not a secure method and time consuming process.
3) The product is moving in the supplychain across the different warehouses and distributors to reach to the customer. So, tracking and tracing the product is another challenge in supplychain.
4) The information contained in the supplychain must be immutable, as there are many participants involved in supplychain, There is possibility of alteration of information.

1.2 Research Questions

From the control perspective in a system, the following questions are proposed:

1) How to differentiate blockchain technology from centralize Systems? This thesis commences with the centralized systems and its disadvantages as compared to blockchain systems. It then proceeds with the explanation of blockchain technology and its terms and internal functionalities.
2) Inspite of many security concerns why is blockchain prone to cyber-attacks? This paper discovers the

Licensed Under Creative Commons Attribution CC BY

weaknesses in blockchain system and encapsulates the causes for these attacks.

3) What are the risks, security threats, vulnerabilities involved in blockchain implementation of Supply Chain Management? This paper identifies the risks involved while implementing blockchain.
4) How to prevent attacks on blockchain? This paper proposes secure ways of implementation of code in the blockchain by eliminating various vulnerabilities.

1.3 Research & Exercise

1) Review traditional centralized systems and blockchain systems in the context of security. To identify the advantages of blockchain system over traditional supply chain management system we conducted a detailed analysis on various traditional supply chain models.
2) Analysing heists, vulnerabilities and threats which were successful on blockchain systems. By conducting a comprehensive review on the public blockchain systems various threats were identified depending on the type of attack and place of their occurrence.
3) Conducting analysis of security incidents and grouping cyber-attacks occurred against blockchain. This analysis categorizes various vulnerabilities and threats which were already successful on blockchain.
4) Design of a potentially effective, secure and flexible framework for Supply Chain Management systems. Keeping in view of all the attacks and threats this thesis proposes a novel framework for supply chain management system with the integration of security parameters.

1.4 Objectives

In SCM, a product's life cycle can be roughly divided into the many phases the product goes through, down from the raw materials up until the finished product ends in the hands of a consumer.

Speed of delivery: The effects of the evolution of SCM throughout the last few decades are visible to everyone. Products are bought and shipped from one side of the globe to the other in a matter of weeks or sometimes even days. The world around us moves quickly, it might happen that sometimes weeks or days are not enough. The faster the products arrive to their buyer, the faster the buyer can satisfy their needs. This holds true not only for the final customer of a product, but also for any enterprise that provides products and services to other enterprises, be it in the role of supplier, manufacturers, distributors or retailers ˆ

Tracking: During a product's lifetime, a lot of alterations occur and, sometimes, the records about the origins of the products are lost, falsified, or flat out not kept in a registry. This leads to unreliability in the goods the consumer's use every day and it may happen that some products are falsified and not the real product they were advertised to be. ˆ

Synchronization: Many times, the data from a company is synchronized with its own servers and software, in protocols and data formats that can only be understood by that specific piece of software. If many companies share this same software, then they can easily integrate the information between themselves. The real problem occurs when the companies have no common ground and the data is not transmittable in an automatic way, leading to a lot of unnecessary manual work to export the data from once system and import it into another.

Security: This point is one of the most important to deal with, as security is comprised of many aspects, such as: whom to authorize to access the information and how to restrict this, what authentication methods should be used, how to accurately detect and prevent fraud, etc. Information in a supply chain is highly sensitive and should be controlled so that only trusted entities can access it. Most enterprises (or groups of enterprises) compete amongst themselves to make the most sales, the most deliveries and have the fastest product cycles. Therefore, the information that is generated in the process of managing a supply chain might be too sensitive to share, in order to keep the edge on the competition.

1.5 Benefits of Blockchain based Supply Chain

The advantages of blockchain in supply chain over other solutions are listed below: ˆ

- Less error prone: The manual data entry errors are reduced, particularly when it integrated to IoT and other automated processes.
- Security of transactions has improved: Blockchain is perform not only ledger immutable but also easily detect frauds.
- Tracking ability is enriched: The ledger can easy to analyze and convey the results making fast and also shows the status of order at any instant. If any error, due to either accidental or on purpose, that succeeds to detect its way into the system is easily traceable. ˆ
- Trust on supplier by the consumer has improved: blockchain allowing the users to verify the provenance of their products. Thus, customer and supplier relationship of trust has to be developed.
- A governance cost for exchange the information is reduced.
- Increase efficiency and sustaining competitiveness in the internal management of supply chain life cycle.

2. Related Work

From last decade, due to rapid change in consumer – based economy, many organizations may no longer dependent only their strengths, but also they are start working together with supply chain partners to achieve competitive advantages. Latest technologies, due to globalization and the resulting increasing competition strengthened the importance of SCM and it has become a solution strategy to improve the overall supply chain management [4].

Generally, SCM means that two or more firms work effectively together to schedule and realize different supply chain functions with the goal of increasing their profits and gaining competitive advantages [5]. Based on relevant information exchange, firms want to achieve common goals, benefits and rewards with the cooperation and also sharing

Licensed Under Creative Commons Attribution CC BY

risks [6]. For Successful collaboration, SCM is especially based on transparency and trust. Moreover, underline the significance of long - term relationship and need to modify business process to advance the general performance [7]. Many of the profits gained by working together can be reached only by long – term relationships. Suppose, firms are interested to the work together and trust each other, and they are more interested to invest in different tools for information exchange and communication, so, it may improve the overall performance [8].

Ralston, P et al. addressed that share holders in SCM should know their strengths and needs, and also their weaknesses [9]. Working together is an important part of efficient SCM and has a good impact on different business operations such as buying and order accomplishment, and also on general cost reduction [10]. The main aim of working together for all participants is to achieve better performance than they would have successfully completed individually [5]. These betterments are achieved through sharing resources, skills and processes [11]. The performance of SCM will improve, for example increasing profits, processes optimization or competitive benefits [12].

- Characteristics of Supplychain Cooperation There are varieties of aspects, which are influence on the degree of SCM [13]. They are trust, information exchange; mutuality, transparency and communication are the most important characteristics of a cooperation culture. For proper implementation of SCM, good relationship among the members is very important. And trust is also another important requirement for a successful cooperation in SCM. Partners, who are trust each other, are more ready to fulfill cooperative
- Activities such as information sharing and investments [14]. In addition, mutuality is related to both positive and negative issues such as increasing benefits, and also appearing risks [15]. Mutuality addresses different aspects of SCM [16]. For example, focus on mutual dependence and knowledge, which influence the outcome of cooperation.

Wu I-L Chung et al. emphasize the significant relation between information sharing and cooperation. Generally, information sharing and use of technology are very narrowly connected in SCM. In a cooperative relationship, firms required to face issues and regulate their sharing of information, use of technology and behavior [17]. Exchange behavior means that firmrequired to be committed to share their network resources with their cooperation partners [18].

In addition, technology use of behavior required to be controlled, since it is the basic requirement to control and gain high performance for customer satisfaction. In relation to the information exchange as a part of technology use, openness and quality of information have a very huge influence on the cooperation efforts. However, intermediation may reduce

The transparency, which is lead to increases cost and reduce the performance [19]. Kumar .G et al. addressed, transparency and sharing of information may also be considered as important drivers for successful SCM and lead to cooperative culture. Specifically, information sharing methods required to be clear to support the exchange of information and make an overall understanding of the supply chain process [20].

In addition, the different supply chain members are required to be transparent and sincere to each other, to achieve trust, and minimize the risk of implicit mistakes [19]. Kumar .G et al. suggested transparency and sharing of information, and remaining factors such as knowledge and skill sharing, trust, dedication, understanding of organization and reliability result to a strong cooperative culture.

3. Problem Statement

The main objectives that are already stated, such as to improve the security traits, pursuing the goods and tacking the final products at any time, speed up delivery for the supply chain, and synchronizing the information, along with other miscellaneous attributes. A seemingly good alternative that stands out is Blockchain. Therefore, the statement that thesis preserves as “Blockchain is a good architectural desisgn for the Supply Chain Management domain”.

4. Methodology

4.1 Design and Implementation of SCM Framework Using Blockchain

The basic notion behind Supply Chain Management (SCM) is to organize the flow of goods, services, and information in an effective way in order to accomplish high performance and decrease in potential threats. However, the fast changing economy requires that companies’ working together more closely to have effective practices and improve not only their own but also it influences the Overall Supply Chain performance [4].

Here we addresses how the block chain technology might apply to any enterprise or organization in general and Supply Chain in specific. The first fold of our research is create a block chain based framework called Secured Autonomous Transactions in Supply Chain (SATSChain), which ensures the traceability of different operational modes of supply chain [22]. The frame work helps track and trace every mode of operation in supply chain such as materials management, operations planning, logistics, distribution, retail, demand forecasting, order fulfillment, and so on. In the second fold of research addressed deploy and validating the framework in different working environments

Licensed Under Creative Commons Attribution CC BY

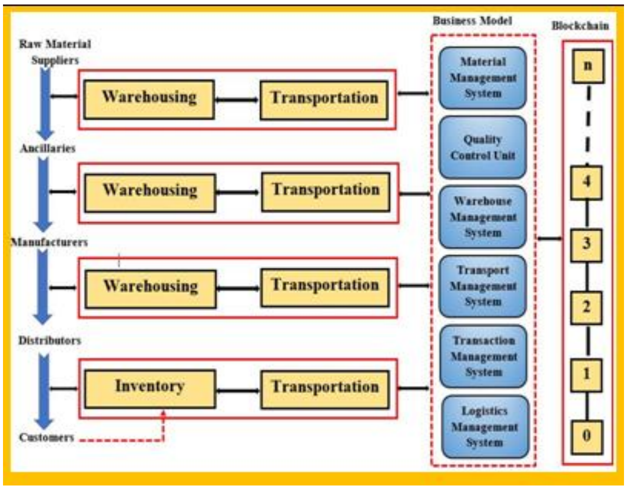


Figure 1: SAT Chain Architecture

4.2 Architecture of SAT Chain

The abstract view of proposed SATCHAIN architecture as showing in the Figure s1. The architecture ought to six major modules, such as Material Management System (MMS), Quality Control Unit (QCU), Warehouse Management System (WMS), Transport Management System (TMS), Transaction Management System (TxMS) and Logistic Management System (LMS). These modules are integrated to the block chain. The contributory roles of the system are Raw material supplier, Ancillaries parts provider [22], Manufacturers, Distributors and customers. The detail description of each module is shown in the following sub section.

Material Management System (MMS):
The task of MMS is to collect raw material from authorized sources and fulfill the requirements of participating roles.

Quality Control Unit (QCU): The main goal of this module is to check the quality of various raw materials, Ancillary products manufactured by different supporting firms and also the final products made by the manufacturers. Depending on the qualityof product, QCU issues various certificates to the corresponding authorities.

Warehouse Management System (WMS):
This module involves to governing all the warehouses and inventories maintained by the different entities. The WMS module combines with TMS, to monitor the internal transmission and maintenance of goods in the warehouse as shown in figure1.

Transport Management System (TMS): This system is associated with different other systems such as WMS, QCU, MMS and LMS to carry commodities to corresponding destinations.

Transaction Management System (TxMS): This system plays major role in the entire architecture of SCMs. because it interacts all the other entities and perform the all valid transactions among themselves[RV20]s.The transactions made by the authorized entities are updated to the block chain and it reflects entire framework.

Logistics Management System (LMS): LMS works with the integration of TMS, TxMS and WMS. The LMS operates in a bidirectional way of services, to the customers and from the customers.

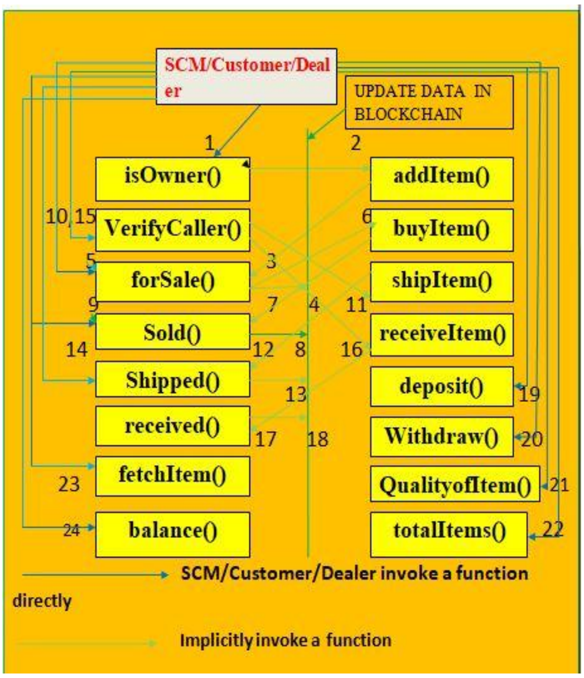


Figure 2: Supply Chain Management Interaction Diagram [22]

Here, the functions are classified into two categories

1) Functions directly invoked from the contract (represented in the figure by blue solid line)
2) Functions that are invoked indirectly i.e. from another function (represented in the figure by green dotted line). The working of these functions is as follows.

The operations as shown in the Supply Chain Management Interaction Diagram can be explained with the following algorithms.

Add Item: It describes all the operations required for adding items into supply chain repository. Addition of items can only be done by the seller of that item. Hence, the addition algorithm fetches the caller’s address, Item name and price of the item from the smart contract [22]. Then the callser’s address is compared with seller’s address, if there is a match the item will be added to the repository, updating all the state variables elsewhere it displays a message stating only seller’s can add item to repository.

Purchase Items: The operations required for purchasing items from supply chain repository. Purchase of items can only be done by the buyer. This algorithm fetches the caller’s address, Item name and total price from the smart contract. Then the caller’s address is checked to confirm if he is a buyer.

If it matches the smart contract checks the conditions further to see if the item is stated for sale or not. If the caller is a seller and item is for sale, then it confirms whether the item requested is in stock. When all the conditions are satisfied, buyer will be given access to purchase. updating these

Licensed Under Creative Commons Attribution CC BY

details to the state variables, else displays the corresponding failure message to the buyer.

Ship Item: It describes the steps involved in shipment of an item. Shipment is done by the seller, soon after receiving the payment from the buyer. To validate these conditions the algorithm fetches item code and user address from the smart contract. If the fetched user address is seller's address it proceeds by checking the state of the item. To ship the item the state should be sold, any variation in this will display a message to the user displaying Sorry, item is not sold yet elsewhere the required item gets shipped updating the state variable's information.

Receive Item: The steps involved while receiving an item are described. The item can only be received by buyer. To check whether it is being received by the intended person the address has to be validated. For this the algorithm fetches Item code and user address from the smart contract. If the fetched user address is that of a buyer, it proceeds with the verification of the state of the item. For receiving an item its state should be marked as shipped, any mismatch in the state information displays a message item not shipped elsewhere the buyer will receive his item changing the state to received.

Fetch Item: It describes the steps involved for fetching an item. This operation can only be performed by the user. The algorithm fetches item code and user address from the smart contract to validate the addresses. If the fetched address is that of a buyer, the algorithm further checks if the item code entered by the user is valid. On successful validation of the conditions the details of the item are fetched and sent to the user otherwise displays a message stating item code mismatched.

Revoke the Item: It helps the user to revoke the purchase made by him. In order to revoke the item, the buyer's credentials have to be verified. For this purpose the algorithm fetches buyer's address and item code. If the fetched item's state is sold and requested for cancellation then the status of the item gets changed to cancel, further updating the state variables. Any mismatch in the above conditions, the algorithm displays a failure message halting the execution process.

Replace the Item: It helps the user to replace the purchased items. Upon validating the buyers details the algorithm fetches the item's status and the request of the buyer. The state of the item being received and request for replacement being defective or damaged and the item is in stock, the replacement request will be accepted. The information in the state variables will be updated. Any violation to the validation of above conditions displays a failure message halting the replacement operation

Quality of item: It helps the user to provide feedback about the item purchased. Item code is fetched from the user for further validation. If item code exists and state of item is sold then the condition of the item gets verified. If the condition is good the message with quality is good will be updated otherwise the substandard item report will be updated.

5. Experimental Setup

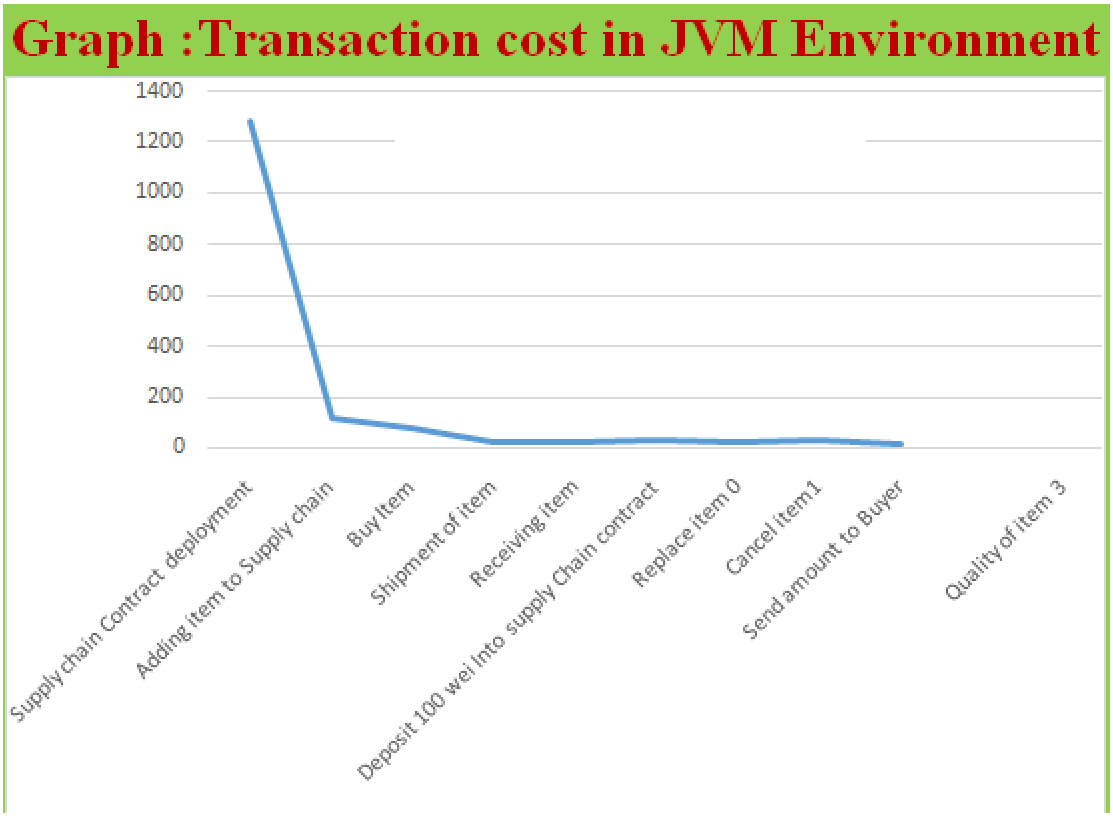
The SCM application is designed for implementing various functionalities of Supply Chain Management System. In order to provide security to this system we implemented this new framework using blockchain technology which is tamper proof and authentic. System interaction is provided only to the registered users. The registered users are provided with their own personal credentials. Upon validating their details, the system grants permission to perform various operationsbased on their role. Sellers are given permissions to add item, ship item. Buyers can purchase item, fetch item details and receive the item. The operations that are performed in SCM are validated by SCM smart contract. The prototype of the proposed system is implemented to study the performance and also to check the attainment of security levels.

The prototype of this system is implemented using Solidity which is object-oriented, high-level language for implementing smart contracts. Smart contracts are software programs that govern behavior of the accounts within the Ethereum.IDE used for deploying smart contracts is REMIX.

Table 1: Results Produced by deploying in JVM Environment

S. No.	Operation performed	Transaction cost (GAS)	Execution cost (GAS)	Transaction cost (INR)	Execution cost (INR)
1.	Supply chain Contract deployment	2109599	1564487	1279.87	949.15
2.	Adding item to Supply chain	189960	167664	115.246	101.72
3.	Buy Item	123922	117522	75.18	71.299
4.	Shipment of item	29988	8588	18.19	5.21
5.	Receiving item	35235	13835	21.37	8.39
6	Deposit 100 wei Into supply Chain contract	44331	21459	26.89	13.01
7	Replace item 0	35378	12890	21.46	97.82
8	Cancel item1	44769	51897	27.16	31.48
9	Send amount to Buyer	19073	12801	11.57	7.766
10	Quality of item 3	22910	1638	13.89	0.993

Licensed Under Creative Commons Attribution CC BY



Graph: Transaction cost in JVM environment

4.3 Vulnerabilities In Scm Smart Contract

In previous context we addressed SCM smart contract implementation, mode of operations and its functionality using blockchain. Even though we created SCM successfully there may arise a lot of security concerns. Here focuses on different vulnerabilities and threats involved with SCM model.

Attacks on blockchain: In spite of, the level of security employed in blockchain applications the possibility of the attacker's entrance could not be reduced. The number of potential attacks and heists performed on the blockchain, grabbed the attention of the developers and users. In context to SCM the possible attacks include Re-entrancy attack, Arithmetic Overflow and Underflow attack, Delegate Call attack, Parity Multi Sign Wallet attack, Locked Ether attack, Transaction Order Dependency attack, Time Stamp Dependency attacks.

Re-entrancy attack is a very harmful attack as it capable of completely draining the smart contract of its ether, and can even snitch its way into the smart contract code. A re-entrancy attack occurs when a function in the source code makes an external call to another untrusted contract before it resolves any effects. If the attacker is capable of controlling the untrusted contract, he makes a recursive call back to the original function, thereby repeating the number of interactions between them [23]. This can be better understood by taking a glance of the code snippet where an attack can occur.

There are two counter measures for resolving the re-entrancy attack.

Solution 1: Preventing the usage of *call()* - There are no restrictions imposed on the withdraw limit for *call()* function. So it drains of the contracts funds, making it to halt the contracts execution. Hence this *call()*function should be replaced with *transfer()*function or *send()*function as these functions can only withdraw 2300 units of gas thereby restricting expensive function calls.

Solution 2: The owner places a lock on the state of the source smart contract thereby restricting user's permissions to modify the smart contract's state information.

Arithmetic Overflow/ Underflow attack: These attacks occur as a consequence of integer overflow or underflow. For example, in many of the available software programs four-digit year is represented with the last two digits i.e. 1998 is stored as 98, 1999 is stored as 99.Thus making it problematic for the year2000, as the system will save it as 00 reverting it back to 1900.

Overflow attack is caused by storing the number that is exceeding the integer range. Solidity programming language can handle uint (unsigned integer) range up to 255 bits. When it gets incremented by 1 it leads to overflow. Storing 256th bit into uint leads to a problematic scenario storing a 0 in that location.

The scenario of Underflow attack occurs as a consequence of subtraction over a 0. As a result of this operation the value to be stored in that location instead of turning to be negative, will be stored as 255 i.e. the highest possible value into that location [23].

Locked Ether attack: These attacks were most prone on parity wallets where the vulnerability arises when the users deposit money to their contract accounts but later due to the attack, they fail to spend their money from those accounts. These accounts effectively freeze their account making inaccessible for the users to access their money. The vulnerability is caused by (i) the contracts that do not provide any function for spending money depending on the expenditure function of another contract that implemented a library. (ii) The called contract i.e., the library, being killed accidentally or willingly.

Transaction Order Dependency attack: This attack is equivalent to race condition in smart contracts. This attack takes place with the prior knowledge possessed by the attacker about the memory pool.

This attack takes place when the transactions are placed in the memory pool, waiting for the mining operation. The legitimate miners set the price of items in their transactions. Before they are mined and updated to a block the value set by the legitimate miners gets modified by the attacker. The attacker sends a transaction to the memory pool with a higher gas fee than the legitimate miner. The order in which the transactions arrive is irrelevant for their execution. The gas sent with the transaction is vital in this scenario as it determines which transaction has to be mined first. Hence the new price value will be updated to the blockchain. This entire process can be made by the attacker with his prior knowledge [22].

This entire operation creates a problem in Smart Contracts that rely on the state of storage variables to remain at certain value according to the order of transactions.

The counter measure for this attack is the usage of transaction counter. The price accepted for mining the transaction is stored in a static variable and is locked with the help of a transaction counter. However, when any transaction is performed on the locked variable the price gets compared. If both of them are same the operation gets executed, otherwise it is reverted back.

Time Stamp Dependency attacks: Smart contracts often need access to time values to perform certain type of functionalities. Values such as block. timestamp, block. number can give you a sense of the cursrent time or the change in time. However they are not safe to use for most of the purposes. In case the of block. Timestamp developers often attempt to use it to trigger time-dependent events. As Ethereum is decentralized, nodes can synchronize time only to some degree. More over malicious miners can alter the timestamp of their blocks, especially if they can gain advantage by doing so.

However miners cannot set a timestamp smaller than the previous one as the block will get rejected, nor can they set a timestamp too far ahead in the future. So one cannot rely on the preciseness of the provided timestamp.

As a counter measure the block time on the ethereum is generally about 14s, its possible to predict the time delta between the blocks [22]. However, the blocktimes are not constant and are subject to change for a variety of reasons like fork reorganizations and solving the mathematical puzzle. Due to variable block times, block. Number should also not be relied on for precise calculations of time.

6. Results

Experimental Setup

Secure SCM (SSCM) implements various functionalities of Supply Chain Management System in a more secure way. Here various security parameters and functions are combinedly implemented with our SCM models discussed above. In our SSCM model we implemented various kinds of attacks like Re-entrancy attack, Arithmetic overflow/ underflow attack, Delegate call attack, Parity multi sign wallet attack, locked ether attack, Transactional order Dependency attack, Timestamp dependency attack and proposed their counter measures in an effective way on how to overcome and safeguard from attacks in SCM. The operations performed in SSCM are validated by SSCM smart contracts. The prototype of the proposed system is implemented to study the performance and also to check the attainment of security levels. The experimental setup of SSCM is same as discussed.

The following results as shown in table 2 were produced on executing our SSCM model in JVM environment.

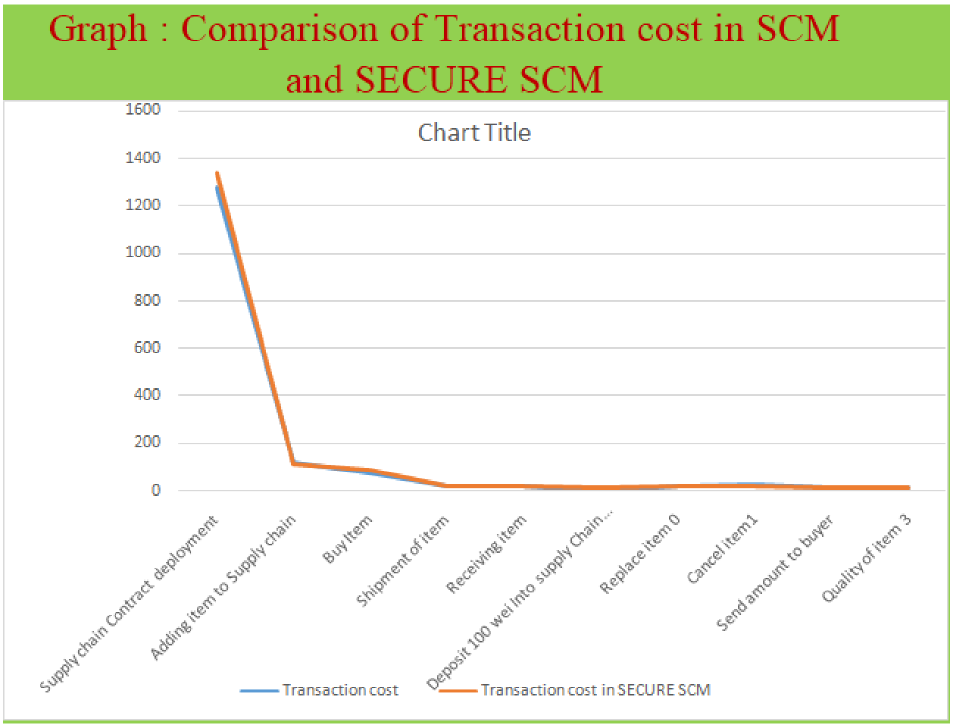
Table 2: Results Produced by deploying in JVM Environment

S. No.	Operation performed	Transaction cost (GAS)	Execution cost (GAS)	Transaction Cost (INR)	Execution Cost (INR)
1	Supply chain Contract deployment	2205711	1638763	1338.18	994.22
2	Adding item to Supply chain	189960	167664	115.28	101.72
3	Buy Item	144176	137776	87.47	83.58
4	Shipment of item	30074	8610	18.24	5.23
5	Receiving item	35235	13835	21.37	8.39
6	Deposit 100 wei Into supply Chain contract	26987	5715	16.37	3.46
7	Replace item 0	35400	12912	21.47	7.83
8	Cancel item1	29885	36897	18.13	22.38
9	Send amount to Buyer	25624	18968	15.54	11.50
10	Quality of item 3	22910	1638	13.899	0.993

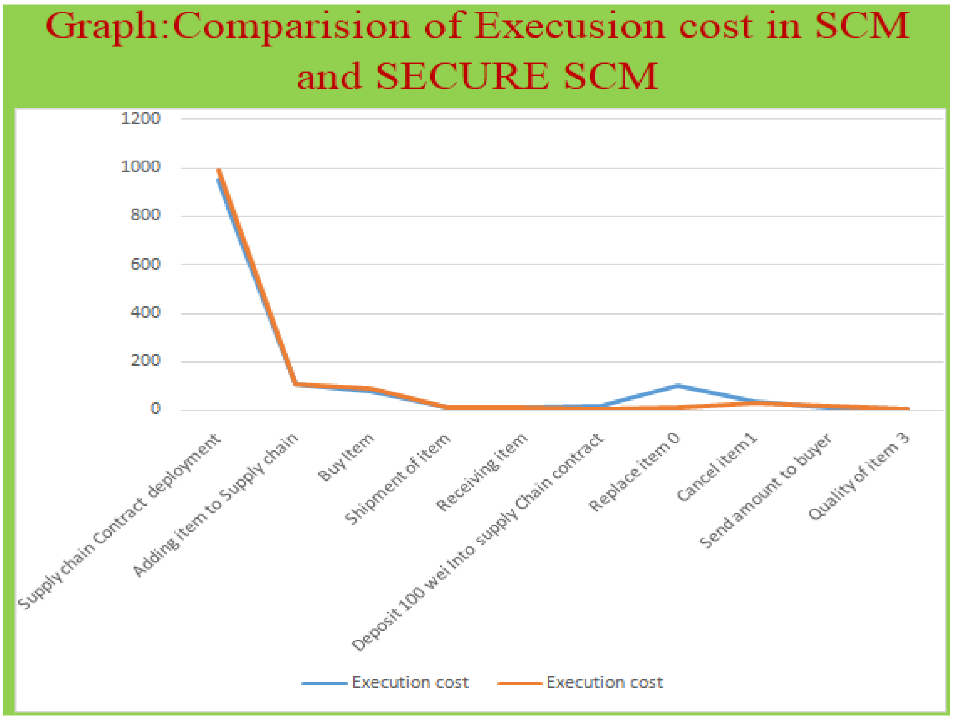
Licensed Under Creative Commons Attribution CC BY

Table 3: Comparison of Transaction cost and Execution cost using JVM

S. No.	Operation performed	Transaction cost In SCM (INR)	Transaction cost in SECURE SCM (INR)	Execution Cost In (SCM)	Execution cost in SECURE (SCM)
1	Supply chain Contract deployment	1279.87	1338.18	949.15	994.22
2	Adding item to Supply chain	115.246	115.28	101.72	101.72
3	Buy Item	75.18	87.47	71.299	83.58
s4	Shipment of item	18.19	18.24	5.21	5.23
5	Receiving item	21.37	21.37	8.39	8.39
6	Deposit 100 wei into supply Chain contract	26.89s	16.37	13.01	3.46
7	Replace item 0	21.46	21.47	97.82	7.83
8	Cancel item1	27.16	18.13	31.48	22.38
9	Send amount to Buyer	11.57	15.54	7.766	11.50
10	Quality of item 3	13.89	13.899	0.993	0.993



Graph 1: Comparision of Transaction cost inSCM and Secure SCM



Graph 2: Comparision of Execution cost in SCM and Secure SCM

Licensed Under Creative Commons Attribution CC BY

7. Conclusion and Future Work

We have discussed about design of proposed supplychain management framework, which is having advance features, which provides the customer with easy way of buying and delivery of products to their home without much afford, at an original product cost and quickly reach to customer at door step. Although, blockchain technology is having security features, because of transparency, smart contract byte code open to the participants. The attacker make use of smart contract vulnerabilities, he could be able to attack the SCM smart contract. In this paper we have discussed about possible attacks on SCM smart contract like Re-entrancy attack, Arithmetic Overflow and Underflow attack, Delegate Call attack, Parity Multi Sign Wallet attack, Locked Ether attack, Transaction Order Dependency attack, Time Stamp Dependency attacks. Finally, we have proposed secured methods and tested to protect SCM from these attacks. So, proposed SCM smart contract able to protect from these attacks. We can conclude that our SCM smartcontract is an easy way of buying and selling product and could be protect from the above attack.

The future scope of this paper is that beyond our proposed SCM and security methods, still there are many challenges in SCM, customer demands more transparency in product cost, because what they are paying for product is not actual price, and there must be trust among the suppliers, stake holders and environment. And one more challenge is that there are vulnerabilities in blockchain, network vulnerability, and major challenge is that cooperation between supplier, manufacturer, logistics, and environments. And risk management is also one of the challenges, as there are different participants involved in SCM. One more challenge is that, since we are using blockchain technology, it is a new technology, people are not much aware of this technology, experts in this technology is very few and moreover, cost is also very high in ethers. It is very challenge to afford for middle class people.

References

[1] Rhonda R Lummus and Robert J Vokurka. Defining supply chain management: a historical perspective and practical guidelines. Industrial management & data systems, 1999.

[2] Ronald H Ballou. The evolution and future of logistics and supply chain management. European business review, 2007.

[3] Mamun Habib. Supply Chain Management (SCM): Theory and Evolution. Supply chain management-applications and simulations, pages 1–14, 2011.

[4] Claudine Antoinette Soosay and Paul Hyland. A decade of supply chain collaboration and directions for future research. Supply Chain Management: An International Journal, 20(16):613–630, 2015.

[5] Togar M Simatupang and Ramaswami Sridharan. The collaborative supply chain. The international journal of logistics management, 13(1):15–30, 2002.

[6] Festus O Olorunniwo and Xiaoming Li. Information sharing and collaboration practices in reverse logistics. Supply Chain Management: An International Journal, 15(6):454–462, 2010.

[7] Judith M Whipple, Daniel F Lynch, and Gilbert N Nyaga. A buyer's perspective on collaborative versus transactional relationships. Industrial marketing management, 39(3):507–518, 2010.

[8] Usha Ramanathan and Angappa Gunasekaran. Supply chain collaboration: Impact of success in long-term partnerships. International Journal of Production Economics, 147:252–259, 2014.

[9] Peter M Ralston, R Glenn Richey, and Scott J Grawe. The past and future of supply chain collaboration: a literature synthesis and call for research. The International Journal of Logistics Management, 28(2):508–530, 2017.

[10] Laura Horvath. Collaboration: the key to value creation in supply chain management. Supply chain management: an international journal, 6(5):205–207, 2001.

[11] Stanley E Fawcett, Amydee M Fawcett, Bradlee J Watson, and Gregory M Magnan. Peeking inside the black box: toward an understanding of supply chain collaboration dynamics. Journal of supply chain management, 48(1):44–72, 2012.

[12] Douglas M Lambert, Margaret A Emmelhainz, and John T Gardner. Building successful logistics partnerships. Journal of business logistics, 20(1):165–181, 1999.

[13] Mark Barratt. Understanding the meaning of collaboration in the supply chain. Supply Chain Management: an international journal, 9(1):30–42, 2004.

[14] Gilbert N Nyaga, Judith M Whipple, and Daniel F Lynch. Examining supply chain relationships: do buyer and supplier perspectives on collaborative relationships differ? Journal of operations management, 28(2):101–114, 2010.

[15] Soonhong Min, Anthony S Roath, Patricia J Daugherty, Stefan E Genchev, Haozhe Chen, Aaron D Arndt, and R Glenn Richey. Supply chain collaboration: what's happening? The international journal of logistics management, 16(2):237–256, 2005.

[16] Kirstin Scholten and Sanne Schilder. The role of collaboration in supply chain resilience. Supply Chain Management: An International Journal, 20(4):471–484, 2015.

[17] Long Wu and Mai-Lun Chiu. Examining supply chain collaboration with determinants and performance impact: Social capital, justice, and technology use perspectives. International Journal of Information Management, 39:5–19, 2018.

[18] Long Wu, Cheng-Hung Chuang, and Chien-Hua Hsu. Information sharing and collaborative behaviors in enabling supply chain performance: A social exchange perspective. International Journal of Production Economics, 148:122–132, 2014.

[19] Andrew Popp. "Swamped in information but starved of data": information and intermediaries in clothing supply chains. Supply C

[20] Robert Frankel, Thomas J Goldsby, and Judith M Whipple. Grocery industry collaboration in the wake of ECR. The International Journal of Logistics Management, 13(1):57–72, 2002. hain Management: An International Journal, 5(3):151–161, 2000.

Licensed Under Creative Commons Attribution CC BY

[21] Keah Choon Tan. A framework of supply chain management literature. European Journal of Purchasing & Supply Management, 7(1):39–48, 2001.

[22] B. Ratnakanth K.VenkataRamana Satchain: Secured Autonomous Transactions in Supply Chain using Block Chain, IJITEE, ISSN: 2278-3075, Volume-9 Issue-6, April 2020.

[23] B. Ratnakanth K.VenkataRamana, M.Sahiti Competent Solutions for Smart Contract Vulnerabilities in SCM Using Block Chain (IJSTR) , VOL 9, ISSUE 6, June 2020.

Licensed Under Creative Commons Attribution CC BY