Proposed Workflow and Conceptual Implementation for Logistics Automation Using Block Chain Technology

Muhammad Jawad Hamid Mughal¹, M.Nawaz Brohi²

¹Department of Computing and Engineering Sciences, SZABIST, UAE
²Faculty of Computer Science, Bath SPA University, UAE

¹jawadhamid242@gmail.com,²mnbrohi@bathspa.ae

Corresponding Author: Muhammad Jawad Hamid Mughal
Email: jawadhamid242@gmail.com

https://doi.org/10.26782/jmcms.2019.08.00033

Abstract

Digital currency a well-known term in past few years that grabbed the attention all over specially in financial sectors. Bit coin is a modern name use for digital currency in today’s world. Many names can be found in the market but Bit coin was first to show trust in digital currency and adopting it as a legal currency. Transactions made using block chain are well secure and transparent to user for monitoring. All signatures are stored in a distributed ledger that keeps the record for transactions happened. Decentralized network is use in block chain technology that connects all the nodes in a network. In this paper, the concept of block chain technology has been incorporated to improve the logistics process using secure digital currency and automate the payment process using bit coins and eliminating third parties interactions. Proposed workflow and conceptual model will help the supply chain management for secure and monitored delivery of goods to end customers. Model will provide advantages for logistics department that includes tracking, transactions updates, transparency, less documentation, on time delivery etc. SHA 256 is used in hashing for data encryption. Customer can also monitor their ordered material status. Proposed conceptual model can be used for all kind of shipment methods i.e. by air, by road, by sea. Paper includes comparison table that will highlight importance of block chain technology.

Keywords: Bit coin, Distributed Ledger, Logistics, Signatures, Hash.

I. Introduction

Block chain word is very well known now days in both academic and industry domain. It is basically a concept and famous technology that is attracting organizations towards its self-due to very secure architecture, crypto currency, decentralized network etc. Traditionally money transactions were made through different third parties (mostly through bank) who were costly as well as time consuming. Process was lengthy and huge documentations work was involved and for storing file big space is required. Block chain is implemented but it will take time for
people and organization to gain trust into this and move to this technology. There are many crypto currencies in market like Litecoin (LTC), Ethereum (ETH) but most famous one is bit coin. Block chain technology use decentralized open ledger that provides visibility to each party or can say to each block in block chain in secure manners. All transaction records made between parties are stored permanently in data base and once record is entered in chain it cannot be erased. Block chain eliminates third party concept and transactions are made directly from one source to another that allows participating parties to access and monitor there transaction.

Bit coin network helps transaction to be happening without any third party involvement and main technique behind this is known as block chain. In 2016 bit coin succeed to hit ten billion dollars[XII]. Block chain consist of multiple block which creates a chain. Each block is link to previous and the next block in the chain but the first block is a special block. Every block has information stored of the previous and the next block. Chain grows with the creating of new blocks and that is how chain continues. It can be applied in different domains like; IOT, smart contracts, security services etc. Public ledger is a collection of all financial transaction record. Traditionally, when multiple companies used to interact with each other and save record of transactions made between them, they used centralized ledger. Centralized ledge is managed by trusted third party that keeps record of transactions, avoid double counting / spending and create valid entries. Distributed ledger stores all the transactions at different geographical locations securely. Databases are not physically location at a single location but distributed over the network. Databases are shared and synchronized throughout the network which make it more effective and provide protection from hacker. Peer to peer architecture is used by distributed ledger. Some of block chain features includes decentralization, public access and encryption. Any kind of request in advertised out to each computer system connected in chain network. New transaction or any change made will update all blocks in chain in ten minutes. Miners are certain group of people that validate transactions and miner which validates first get paid in digital currency.

Nature of digital currency in block chain is that, if any two participants in a network do transaction they will broadcast it to all other members in the network to record the transaction in the blocks. Proof of work is an operation (mathematical) that is performed by nodes simultaneously once block is full. Decentralized process in block chain is totally dependent on proof of work and voting by nodes to make blocks valid. Validity for transaction is not done by any organization but through general agreement of network participants with greater number of CPU. Within eight years bit coin have perfectly recorded 140+ millions [X] of transactions.

Supply Chain Management

Supply chain management is a process that manages all activities in production and distribution. It is a network that enables companies and its supplier’s communication for moving products. Supply chain of an organization is a system that includes people, resources, actions, information; which helps in moving product from supplier to customer. Supply chain includes purchasing, inventory, logistics, warehouse management, workshop and marketing. After 1980s the concept of SCM started slowly to increase and organizations showed their interest in this area [IX].
II. Materials and Methods

Zibin Zheng and et al [XII] have intensively discussed about block chain in their work. Ledger allows transactions in decentralized way. Block chain applications quickly start covering different areas like IOT, financial services, health care (medical) etc. Authors mentioned some challenges (scalability etc.) that can overcome, also summarize block chain architecture and compare consensus algorithms. Main block chain characteristics are described like; Persistency: when transactions are validated and invalid are not considered by miners. Blocks having invalid exchange are quickly exposed. Decentralization: traditionally centralized systems were used for transaction where validation goes through central trusted parties (banks etc.). In block chain no central validation is needed and consensus algorithms are used for data consistency. Anonymity: any participant can interact with block chain and user data will not reveal. Auditability: UTXO is a model on the base of which block chain keep user balance in record. Every transaction made in block chain will refers to earlier unspent transactions. Referred unspent will modify to spent transaction when recent transaction will be recorded. Zibin Zheng and et al had shown comparison between three roughly categories (Table. 1) of block chain in the paper. Categories include, Public: is a type of block chain is which all the participants have access to the record and are allowed to take part in decision process. Private: is a type which has centralized networks and nodes from a specific organization would be able to join decision making process. Consortium: is grouping or several organizations and is partially decentralized where some preselected nodes can take part in decision process. No node in block chain can confirm that ledger in all decentralized nodes are same. For this reason some protocols are described that can ensure consistency of ledgers in different nodes. One of the consensus approaches includes proof of work used in bit coin structure. Any node from decentralized network should be selected for keeping transactions records. One ways is random selection but it leads to risk of attacks. Lot of work (computer calculations) needs to prove that if node if publishing (block) transactions it should be save and not harm the network. Each node in a block chain network calculates block header hash value. Header consists of nonce and miner. Hash values changes frequently with the change in nonce. Calculate value should be less or equal to certain provided value. When any node values hits the mark value it should broadcast block to other nodes for confirming hash values. Once it’s confirmed, block is added in a block chain as a new block. Second is proof of stack approach, which is consider as more effective and energy saver approach.
Table 1: Public, Consortium and Private Block chain Comparison [XII]

| Property       | Public blockchain | Consortium blockchain | Private blockchain |
|----------------|-------------------|-----------------------|--------------------|
| Consensus determination | All miners        | Selected set of nodes | One organization   |
| Read permission | Public            | Could be public or restricted | Could be public or restricted |
| Immutability   | Nearly impossible to tamper | Could be tampered | Could be tampered |
| Efficiency     | Low               | High                  | High               |
| Centralized    | No                | Partial               | Yes                |
| Consensus process | Permissionless   | Permissioned          | Permissioned       |

**Bit Coin Protocol**

Transactions are made between senders and receivers. Bit coin is a chain where transactions are made from one owner to another and public key is used to identify valid owner. Each transactions includes previous owner sign (secret singing through private key), transaction hash number through which he received bit coin and next owner address. After the transaction is end it then can be added to set off bit coin transactions because to tracking and security purpose. Each signature refers to pervious bit coin transaction in a chain, owner has right to check from where bit coin came from and all the signatures in chain[XII]. Double spending is a terminology used is bit coin signature where user tries to send a bit coin which he already did before. User should be aware with all transactions that a previously made to avoid double spending. As block chain is publically for all users in a network, so to decide which transaction was made before (first). That is why signatures (transactions) are grouped together in a blocks and are easy to validate. Bit coin is decentralized and no centralized authority that can generate bit coin. Bit coin at first place is generated, in the process of making blocks. All accepted blocks in a large block chain and data stored inside is hashed where hash value start from zeroes. Blocks contain list of transactions a nonce, where user can find specific set of data. Block is broadcasted when someone finds nonce which permits block having correctly organized hash. Fig 1 shows the bit coin transaction procedure. Here user wishes 0.7 bit coin to send to merchant. At point 1 merchant generates mpkas his address and send his address to user at point 2. At point 3, user made tx transaction of 0.7 BTC upk to mpk. At point 4 if transaction is valid so user, flood the transaction made in his network peers and miners will know about the transaction. Point 5 is miner’s point where transaction made and other transactions in chain are considered by verifying hash, either it is targeting any range. Once block is validated, in point 6 miners broadcast this block in network (peers). Following about method merchant will know that signature in global chain is accepted any payment send by user is received.
Block Chain Architecture

It is a chain consists of sequence of blocks that holds record list of all transactions in standard public ledger. A block should have one parent block in chain, if it contains previous block hash number in its header. First block with no parent (no referring to any block hash) block in block chain is known as Genesis block. Single block architecture as shown in Fig 2 consists of header and body. Header contains follow detail in it, a block version specify validation rules to be followed. Merkle tree is a hash value of all block transactions. Timestamp, nBits, nonce is 4 byte field which increase (start =0) for hash calculation. Parent hash (256 bit) indicate previous block. Block body is a combination of transactions made any transactions counter. Number of transactions that a single block can holds depends on size of a block and each transaction. Private and public keys are hold by each user. Private key is confidential and is used for sign transaction. Signing and verification are two phases includes in digital signature. For example A wants to send data to B, in signing phase data will be encrypted using private key and send to B. In verification phase B will validate send data with A’s public key. This method will insure the data is tampered or not[XII]. ECDSA is an algorithm used for digital signature in block chain. Block chain has various characteristics i.e. decentralization, persistency, anonymity, auditability.
Distributed Ledger

This ledger group was initiated in Sept, 2015 with the contribution of group of different banks around world. Nine banks were involved in distributed group at the beginning and after time passes more banks were becoming to joining distributed ledger; now 50 financial organizations are part of ledger group. Osuuspankki, Danske bank, SEB and Nordea are four well known Finnish banks that are the part of distributed ledger. Purpose is to enhance and fasten development and operations of block chain in financial domain. They are trying to work together to achieve shared standards. Shared standards are complex and rare. It is a challenging task in banking sector but it is a requirement for the block chain implementation in banking area[VII]. Sharing standard may have security problems like commercial secrets etc. banks mostly looks for an application that can be operate manually. Having a unique system for all the banks that they can use, rather than each bank uses an individual expensive system. Possible that owns block chain for a bank will be not that much benefit as the entire amount comes from users. Hence, if more banks uses block chain technology it will give more profit to them. There are many companies in the market that are trying to make development in financial sector by using bit coin block chain or some are trying to create their own new block chains for doing business . Ripple is an organization which is in touch with few banks and working together for reduction of international payments cost. NASDAQ planned to launch e-voting service in Estonia using block chain technology.

Hash function

Hash function is a domain of values. Each hash value refers to an item that needs to be processed. In programming, storage and retrieval issues mostly arise. Collection of items are given in random order, requested to store and retrieve on demand by matching item key values with provided key values. Preferred method or approach for storing and retrieval problem is hash table technique [IV]. Quality of this method is that it uses items key value and calculates an address for storage and retrieval of that specific item. Key values that are computed and as a result addresses are same such addresses are known as synonyms. Occurrence of synonyms may cause collision. Area where items are stored is called hash table and for accessing tables multiple hash algorithms are used i.e. Storage Algorithm. This technique determines randomly the number of single labels when they are accessing in large group of events that are labeled in a network. Label consists of addresses (source and destination). Promising participants for hash function include CRCs and hashing produces statistical hash address[VIII].

Algorithms

Ripple

It is consensus algorithm that brings trusted sub networks together in larger network. In this approach network nodes are separated in two i.e. server and client type. Server is used for consensus processes and client for funds transferring. Every server have list of unique node (UNL) and is important for server to used node list. It helps server to determine where to insert a transaction in ledger. In UNL server will
find the nodes, in case of agreements received reaches 80% so transaction will be added to the ledger. Ledger will be considered as correct as long as in UNL faulty nodes are less the 20%. For maintain correctness RPCA is functional to each node in a network after few seconds. Ripple components include: server, ledger, open ledger, closed ledger, proposer and UNL[III].

Tendermint
It also lies under consensus (byzantine) algorithm. New block is found in a round and unconfirmed block (in round) will be broadcast by proposer. It included three steps: prevote, precommit and commit. In the first step (prevote), decision is taken by validators. In case t proposed block, validator is locked in previous round it broadcast locked block for prevote. All validators mark their decision in the second step (precommit). Precommit any block to broadcast and sign if the node received 2/3 of prevote for specific block. Commit is the third step in which block is validated by node and do broadcast for block. 2/3 is the receiving ratio of commit for the acceptance of block[V].

Sarah Meiklejohn and et al[XI] have handsomely described about exploring, unique characteristics using algorithm (address clustering) on bit coin wallets and re-identification attacks. Bit coin is purely online currency which trusts on cryptographic protection instead of relying on physicals items. It uses decentralized methodology that was introduced in 2008 and was deployed in 2009. It is an idea of chain transactions where one owner can send to other and owners has public key for identification. Two methods are defined by authors through whom same users can control linking addresses as larger entities in block chain may collapses addresses. In first method different addresses are treated that are used as an input for transaction and same user control them. Method links together those addresses that are being used previously in work. Second method is known as change addresses and its new process. This is different from the first method, it utilizes idiom instead of inherent properties.

Peer to Peer Network
In this form of network each node is loosely connected to equal number of peers with no fixed topology. Communication that includes transactions, blocks is generated by each node towards the connected peers. In p2p network all nodes are equal; they only differ from each other on different roles they are assign with and functionality supporting by them. Nodes are the mixture of different function that are performed with in the network i.e; block chain database, digital wallet and mining etc. In this scenario sender don’t require to trust node used for broadcasting transactions. On the other side node also don’t need to trust sender or create sender’s identity [I]. That’s way transactions can be made over p2p network (insecure network) e.g.; Wi-Fi, NFC, barcodes and Bluetooth etc. IOT devices support this property to interact with each other (devices) for transactions, even devices in secure location or devices connected to a network which is insecure e.g. sensors, RFID etc.
III. Traditional Supply Chain Networks

SCM is a practice of moving goods, assets and other material from one place to other placing keeping the flow information of all the imports/exports, material parts, suppliers etc. Traditional nature of supply chain was liner, with a clear design, planning and source of moving goods from one to other location. Traditionally, SC managers made great efforts to achieve unpredictable changes to improve outcomes, included addition funds, services etc. Most likely these traditional objectives are not going to change easily or may take time to change but presently SC manager should focus to achieve enhanced/improved supply chain technologies, which can help to increase the performance. Supply chain is a combination of many different processes and level that begins with supplier’s information, materials availability and ends on customer. Fig 3 shows the simple process of supply chain for a single product. In below figure raw material is collected and transformed into ready product, then forwarded to distribution hubs and finally reaches to the customer. Modern SC looks into multiple products in whole chain instead for pointing to the next level only and aims to provide more transparency to suppliers and customers. Traditional SC have following limitations: delay in information because of material moving through each organization, limited visibility, multiple planning cycles can also leads to delay[II].

IV. Supply Chain Management Using Block Chain

Supply chain is a term use for flow and methods follow for delivering goods to end customers, it includes different locations and stages. Thus it’s becoming more difficult to trace an event in a whole chain. Transparency is also an issue in supply chain management, buyers and customers have no idea about material needs to be delivery. In SCM investigation of illegal acts are hard to find. There are countless problems that supply chain faces on daily bases, using block chain can reduce these errors with its new technology features of crypto currency, distributed ledgers, transparency and secure infrastructure. Block chain features can be beneficial for many supply chain applications. Public block chain accessibility can help client to see the status of product delivery from place of dispatch to end customer. Decentralized
network infrastructure enables users to participate in supply chain activities (limited access, depend upon restriction level) and immutable behave guarantee the security [X].

V. Commercial Invoice

Commercial invoice is one of the core components in supply chain domain. It contains all the information needed for materials to be delivery. Commercial invoice is basically document that contains the important information of the materials needs to be exported, these information’s also help in custom clearance and assets validation. There is no standard format for commercial invoice, organizations used their own formats but the information the needs to be enter against each individual item like HS code, serial number, quantity etc. are same in every invoice.

VI Results and Discussion

Table 2: Comparison table with and without Block Chain Technology

| Characteristics         | Without Block Chain | With Block Chain |
|-------------------------|---------------------|------------------|
| Documentation           | More                | Less             |
| Transparency            | No / Limited View   | Yes              |
| Security                | No or very less     | Highly Secure    |
| Traceability            | Yes but too difficult | Easy and Accurate |
| Delivery Confirmation   | No or too late      | On Time          |
| Invalid Transaction     | Can be happen       | Hash # changes   |
| Off days Approval       | Wait for working day| Works even on off days |
| Physical Currency       | Yes                 | Digital Payment (Bit Coin) |
| Exchange Rate           | Every time          | Standard for Bit Coin |
| Agents                  | Yes                 | No               |
| Integrated Planning     | Less                | Highly           |
| Information Flow        | Delay per organization | On Time, accurate |
| Toll Payment            | Manual              | Digital / Bit Coins |

The shipment process flow to automate logistics operations that is dependent on digital currency and follows block chain rules is proposed as below. Fig 4 shows how material delivery flow from source to destination with encrypting data at each stop.
and changes hash number. Proposed idea is to separate the whole process into three sections i.e. export, shipment and import. Each section consists of multiple blocks; last block of one pair will connect to first block of the next pair as shown in Fig 4. Practically all blocks are in a single chain and are not separate into multiple sections but for better understanding blocks in three different domains are presented. Blocks included in export are related to source departments that are involved in different stages i.e. checking material availability, creating commercial invoice, packing list etc. Shipment blocks are related to shipment departments that help delivery items to reach to destination. First block of shipment section will only receive the data from last block the export section, shipment blocks have no concerns with the previous block and cannot made any changes, they are just linked by previous hash numbers. There is no physical payment all the transaction will be automatically done and data will be save in distributed ledger. Any invalid transaction we change the hash number. In Fig 4 all blocks are shown connected with dotted lines mean that only authorized users can view the records of all the blocks others can only have access to only those block which they are located to work for or responsible to monitor.

![Data Flow Design for Proposed Block Chain Logistics Automation](image)

**Figure 4: Data Flow Design for Proposed Block Chain Logistics Automation**

*Copyright reserved © J. Mech. Cont. & Math. Sci.*

*Muhammad Jawad Hamid Mughal et al*

415
Fig 5 is a final outcome of implemented system that shows the data encryption using algorithms. Below figure shows block chain of a specific with inv# ZEB/COM-INV/9838 selected from the list of approved commercial invoices. Each data fields of different blocks are fetched from invoices stored in database and are encrypted using SHA 256 algorithm as presented in hash field. Every block has previous hash field that get the hash value of the previous block which links blocks together and make chain more secure, except first block because there is no previous block so it only contain hash value and known as genesis block.

Figure 5: Block Chain View
VII. Conclusion

Core objective of this study is to automate logistics process, eliminate third parties involvements, delays and secure transaction with digital payment process (bit coin) using block chain technology. Data flow for logistics process and conceptual implementation are proposed that show how goods can be delivery to their destinations through virtual secure blocks of block chain. Each block presents a department inside or outside the organization that performs their tasks and encrypted data is moved to next block for further action. For data security SHA 256 algorithm is used for encryption and hash number for previous block is linked to endorse the invalidate and unethical behavior. Study concludes that the proposed model will provide an easily environment to logistics department for delivering material in secure manner without using physical currencies and depending on other untrusted third parties. All process will be automated that will reduce documentation and delivery time.

VIII. Future Work

As technology is changing rapidly and organizations are relaying on automation systems to ease their work. Data protection is the main concern when it comes to transaction, proposed concept can provide are secure channel of data transfer and payment transaction through bit coin. In addition more features can be integrated i.e. Google map with pre-defined paths, tolls and road tax payments system integration, IOT devices (smart warehouse etc.).

References

I Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," Security and Communication Networks, pp. 5943-5964, February 2017.

II Bushra Mukri, "Blockchain Technology in Supply Chain Management: A Review," International Research Journal of Engineering and Technology (IRJET), vol. 5, no. 6, pp. 2497-2500, June 2018.

III David Schwartz, Noah Youngs, and Arthur Britto, "The Ripple Protocol Consensus Algorithm," Ripple Labs Inc, p. 8, 2014.

IV G.D. Knott, "Hashing Functions," The Computer Journal, vol. 18, no. 3, pp. 265 - 278, March 1975.

V Jae Kwon, "Tendermint: Consensus without Mining," GitHub, vol. 10, 2014.
VI Krystsina Sadouskaya, "Adoption of Blockchain Technology in Supply Chain and Logistics," XAMK, Bachelor's Thesis 2017.

VII Laura Jutila, "The blockchain technology and its applications in the financial sector," Aalto University, Bachelor Thesis 2017.

VIII Ramakrishna M.V, E. Fu, and E. Baheekapili, "A Performance Study of Hashing Functions for Hardware Applications," In Proc. of Int. Conf. on Computing and Information, pp. 1622-1636, 1994.

IX Rhonda R. Lummus and Robert J. Vokurka, "Defining supply chain management: a historical perspective and practical guidelines," Industrial Management & Data Systems, vol. 99, no. 1, pp. 11-17, 1999.

X Saifedean Ammous, "Blockchain Technology: What is it good for?" Social Science Research Network, August 2016.

XI Sarah Meiklejohn et al., "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," Proceedings of the 2013 conference on Internet measurement conference, pp. 127-140, October 2013.

XII Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data, pp. 557-564, June 2017.