AN APPLICABILITY OF BLOCKCHAIN MODEL IN BUSINESS USE CASE - A TECHNICAL APPROACH

Anitha Premkumar

Department of Computer Science and Engineering, Presidency University
Rajankunde, Bangalore, Karnataka, India

ABSTRACT

Business network brings many organizations close together to achieve their desired goals and profit from it. People from different organizations may or may not know each other but still can be part of a business network. A major challenge with these business networks is how to provide trust among people and data security. Blockchain is another means through which many organizations in the current digital age are overcoming these problems with ease. Blockchains have also changed the way the business transactions with clients take place. Blockchain is a decentralized distributed ledger in a peer to peer network which can be public or private, and it enables individuals or companies to collaborate with each other to achieve trust and transparency between business and its clients. Many implementations of blockchain technology are widely available today. Each of them have their own strengths for a specific application domain. They can fundamentally alter electronic communications with a potential to affect all sorts of transaction processing systems. However, there are still many challenges of blockchain technology waiting to be solved such as scalability and adoptability. In this paper, we provide the knowledge on Blockchain technology and we present the applicability of blockchain in the business models and also discuss the relevant use cases for Banking and Supply Chain models.·

KEYWORDS

Blockchain, Secure Web Transaction, Decentralized Distributed Ledger, Peer to Peer Network.

1. INTRODUCTION

Blockchain is primarily defined as a shared immutable ledger, or just an “unchangeable record of who owns what”. It can be used to transfer and permanently records any changes to the assets like money, crypto currency, real estate, records of any kind, identities, personal property etc., between two or more parties without the need of intermediaries. Blockchain uses combination of existing technologies like Ledger, Cryptography, and Network Technology. Internet was a major milestone in technological evolution and it led to newer business models, distributed computing and many more changes to human lifestyle over the past 25 years. Experts believe that Blockchain [6][10] will become the next wave in Internet technology as it eliminates the need of intermediaries and provides trust between various business parties.

In cryptocurrencies, we have observed how Blockchain has enabled an online payment system without central authority unlike in Internet Banking. Blockchain-based system receives data, encrypts it and stores it as digital leger called a software leger in every node of the network. The software ledger is a collection of records which are immutable in nature. The key characteristic of Blockchain is that it provides trust between different parties who are part of the business and who

David C. Wyld et al. (Eds): BIoT, DKMP, CCSEA, EMSA - 2021
pp. 19-29, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.110802

may or may not have known each other prior to the business transaction. This is the one of the reasons why Blockchain is making its entry into business world at a faster rate than other emerging technologies post 2016. In a typical business environment, multiple parities are involved and they communicate with each other to share data and perform business transactions. The business data between various parties needs to keep it in secured place and maintained for future purposes. Earlier generation of business systems kept all their data in central repository where it was being monitored and secured by a central authority. Malicious attack, data breach and data stealing could happen easily with central system. Hence security became a major concern to centralized systems in business environment. To address the above challenge, in Blockchain-based solutions all business data is stored at secured place that is on every node's location in the network. This makes it almost impossible for malicious attacker to hack the data.

2. BLOCKCHAIN TECHNOLOGY

Blockchain technology [4] [6] [16] is a decentralized digital ledger stored across all the nodes in the peer-to-peer network (P2P). P2P network is a computer network where nodes will be directly connected to each other without intermediaries. Digital ledger is a software ledger that holds encrypted data which is immutable and shared between nodes in the Blockchain network without a middleman. The structure of Blockchain technology is such that it contains series of blocks that hold business data in them. All nodes in the network holds a copy of the Blockchain records. Any changes in the data requires permission from all nodes in the network which means verification and validation is done by every node in the network. Every node should work cooperatively to achieve the business goal with help of consensus algorithm. Consensus algorithm is an algorithm embedded into every node in Blockchain network to help the network to achieve the agreement between the nodes on data sharing and new block creation. Decentralized application (DAPP) shown in figure 1, is an application model in which all the nodes are connected to each other to share a data and store it across the blockchain network without central server.

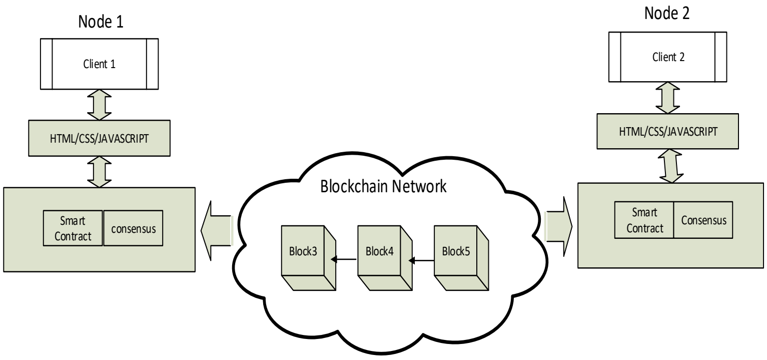


Figure 1. DAPP Model

Every blockchain node in DAPP model has front-end design for interacting with blockchain back-end network via web service calls. Commonly the front-end design is built using a programming languages like HTML, CSS and JAVASCRIPT via which user can access the back-end network. The back-end network consists of smart contract, consensus, and blockchain database. The Browser will initiate the transaction proposal, notify the result of transaction proposal. Blockchain contains a series of blocks attached together in a chain-like structure. The current block contains the address of previous block and previous block contains the address of its previous block and so on. Thus block integrity is maintained. The very first block in the blockchain is called genius block which does not contain address of the previous block. The actual block chain starts with genius block. Each block contains immutable and tamper proof record of transaction data. Data blocks are time stamped and stored in the order of transaction fashion strictly thereby supporting integrity, data transparency and data security. Indeed, blockchain provides immutable and tamper proof data, it is suitable for business to keep their data in secure manner and access by all nodes in the network. A data which is stored in blockchain is secured with help of cryptographic algorithms. Cryptographic algorithm [25][26] uses pair of keys for encryption and authenticate the data. They are namely public key and private key. For instance, in a crypto-currency blockchain, when a person purchases a blockchain wallet, he/she gets a private key. In addition to the private key, there is also a public key. As and when the person sends a transaction from blockchain wallet, the software checks and verifies the transaction and then signs it with his/her private key. This activity sends a message to entire blockchain network that the person has an account in the blockchain wallet and has the authority to transfer the fund on the public key that the person is sending from. Every asset can be converted into electronic asset and given a unique identifier to track, control, buy and sell on the blockchain. The system permits decentralized transactions of all types of e-assets between peers. Blockchain allows users to access the single version of truth to exist across the network as shown in the figure 2.

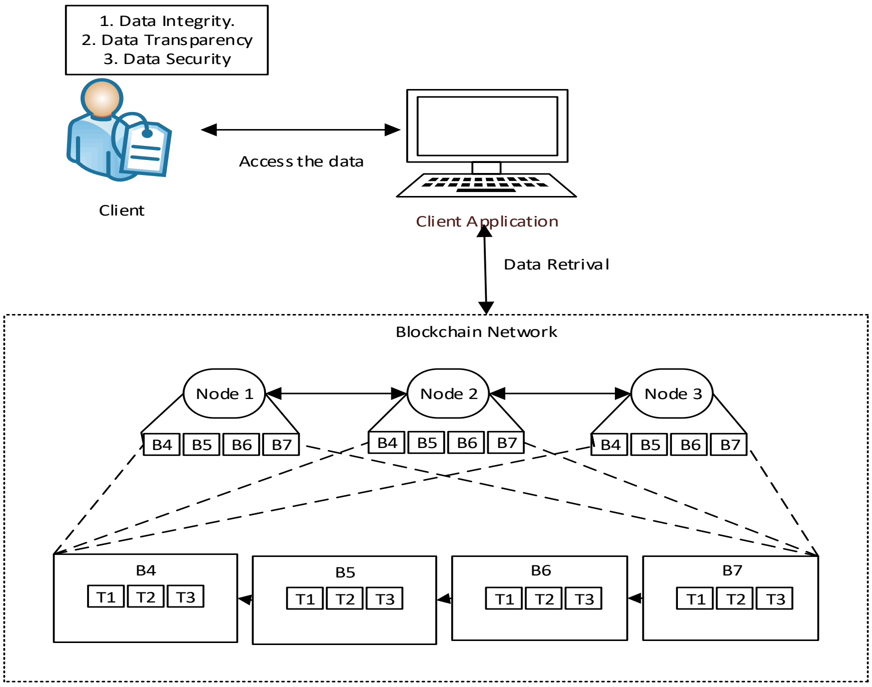


Figure 2. Accessing Single Version of Truth via Blockchain Network.

Blockchain is divided into categories based on the node's participation into the network. If the network is of public type, then it is called public blockchain where any node can take part into the network at any time. If the network is of private type, then it is called private blockchain in which only certified nodes can be part of the network. Table 1 below highlights the differences between public and private blockchains [8][10].

Table 1: Differences between Public and Private Blockchain

Public Blockchain	Private Blockchain
Any node can participate	Only a certified node can participate
Decentralized such that no one has control over the network. Security enabled by the fact that data cannot be changed once validated by the blockchain.	One or more entities control the network leading to reliance on third-parties to transact. Only participating entities have knowledge of transaction and thereby there is additional security.
Transaction data is visible to all nodes in the network	Transaction data is visible only to the nodes who have got certified to be part of network.
Scalability is an issue	Scalability is not an issue
Speed – transactions per second is lesser due to higher number of nodes	Transactions per second is much higher
More secure since there are higher number of nodes in network and hackers cannot attack it easily and gain control.	More prone to attacks, data breaches and manipulation.
More chances of collusion among majority of participating nodes to gain control of the network.	No chance of collusion since each validator is known and identifiable.

3. First Implementation of Blockchain

Bitcoin [3] was the first Blockchain project that got implemented using Proof of Work consensus algorithm. Consensus algorithm [2] [11] is a software agreement between nodes to work jointly and allows to take common decision to perform the task. Consensus algorithm is the backbone of Blockchain technology. There are many consensus algorithms available to implement Blockchain projects. In this section we discuss about first consensus algorithm PoW [5] [7] used in Bitcoin Blockchain Network. Bitcoin works based on crypto currency transactions. Crypto currencies are a form of electronic cash which can be used to trade assets between business parties that are connected via internet. How Proof of work algorithm works in Bitcoin [1] [3] Blockchain is described below in steps

Step1: Identity of a node is checked with help of membership service of decentralized application
Step 2: Once node's identity is validated, node can perform transactions with other nodes in the network
Step 3: Once node completes the transactions, transactions can be verified and validated by a special node in the network
Step 4: Special node create a new block by solving the complex puzzle to convert valid transactions into blocks
Step 5: Once new block is created, it gets broadcasted to other nodes in the network.
Step 6: Upon receiving a new block, nodes update their existing database called digital ledger with new block.
Step 7: Go to step 1

There are two nodes present in Bitcoin. They are called Peer node and Miner node. Peer nodes are normal nodes that execute the transactions with help of Consensus algorithm. Miner nodes are called special peer nodes that execute transactions and also validate the transactions. Miner nodes will solve complex mathematical puzzle in-order to validate the transaction and create new block. To solve complex puzzle, Miner nodes require heavy electricity and computing power. There can be many miner nodes in the Blockchain network who can compete with each other to solve the complex puzzle. The time duration to solve puzzle and create new block in Bitcoin is 10 minutes. Miners who completes task first within the duration, will be the winner of that round. He will be rewarded with some Bitcoin. He will then propagate a new block to whole network. All the nodes in the network receive a new block and update digital ledger stored at their location.

3.1. A Fork in Blockchain

What if two miners solve puzzle nearly at the same time and try to add new block into the previous chain of blocks in the network? This situation creates fork [9] in the network and it is described in Figure 3. Fork means deviation from previous history of records or suddenly a new rule is framed and followed by nodes at particular point. It means that two branches of chain will be created in the network by nodes who solves puzzle at the same time. This can happen with valid miners coincidentally who solves puzzle at same time or malicious attacker who purposefully wants to create a fork to take control over the network and hack the transaction data.

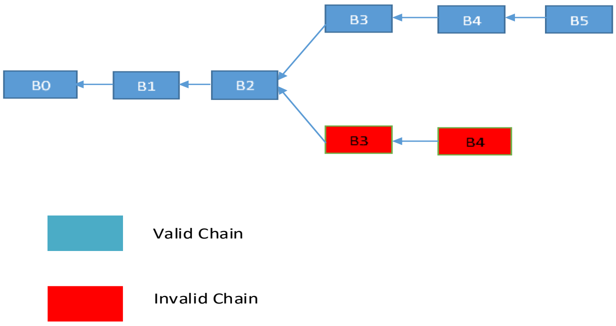


Figure 3: Fork situation in Blockchain Network

Solution: When nodes are encountered fork in the Blockchain network, the process of creating new blocks will not be stopped. Consensus algorithm allows miner to keep solving the complex puzzle and add new blocks into the branches of chain of Blocks. This process will continue and some more blocks will get added into the chain of blocks at every interval of time or each round of an algorithm executes. After some time, the longest branch of chain will be considered as valid chain and that will be considered for further processing and continued and smaller chain will be discarded.

4. Blockchain-Enabled Digital Business Models

Blockchain technology [17][18] [19][20] is becoming more and more popular in various business applications for healthcare , supply chain, education, government and banking. The reason behind this popularity is the ability to cater to constantly growing data in the distributed, decentralized digital ledger while providing ability to seamlessly share the data with all the nodes /peers in the organization network, shown in figure 4.

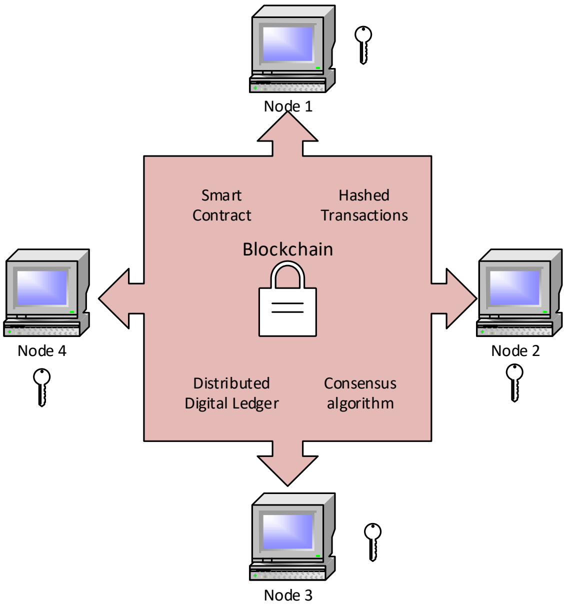


Figure 4. Seamless and Controlled data sharing between nodes within Blockchain Network

In case of healthcare system, the healthcare data is highly sensitive and it needs to be stored at a secured place with limited access. Operational/transactional data will be created and entered by authorized persons within the organization. Private Blockchain system is well suited for such an environment. In Pharma supply chain, manufacturer, distributor, retailer, transporter are the authorized people who are responsible for correctness and completeness of data. Once the drugs are manufactured and shifted to the distributor, drug details are recorded in the blockchain network. Thus every block in the network contains drug transaction details in it. Any authorized member can check for the authenticity of the drug at any time. Blockchain framework supports many platforms to provide a solution to business needs. A few popular platforms such as Ethereum, R3Corda, Ripple, Quorum are listed in Figure 5.

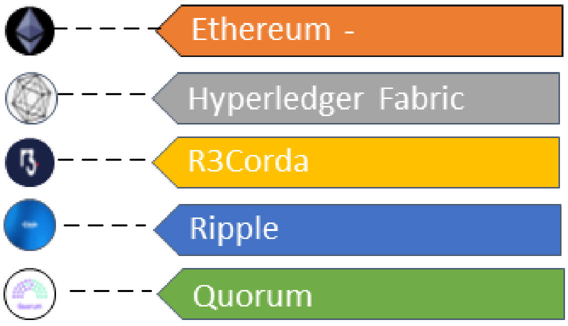


Figure 5. Popular Blockchain Platforms

When it comes to asset tracking with trust, transparency and more security, Hyperledger Fabric is most convincing framework among all. Hyperledger [21-24] from Linux foundation, is an open source permissioned distributed ledger technology platform for business enterprises. It is designed to support pluggable implementations of various components and helps us to solve variety of use cases. Hyperledger serves as a greenhouse that collaborates with the customer, developer, different vendors from various sectors to achieve its goal. It provides different consensus models that enable performance at larger scale while achieving data privacy. As mentioned previously, Consensus is an agreement between nodes in the network in-order to verify and validate the transactions and achieve the correctness of the set of transactions in the block. Blockchains can have different consensus models based on the requirements for different use cases. Use of Blockchain technology [14] [15] can provide enormous competitive advantage to businesses even though at present significant challenges are there in leveraging it in digital business models. In Figure 6, the key dimensions of Blockchain usage in business models is depicted.

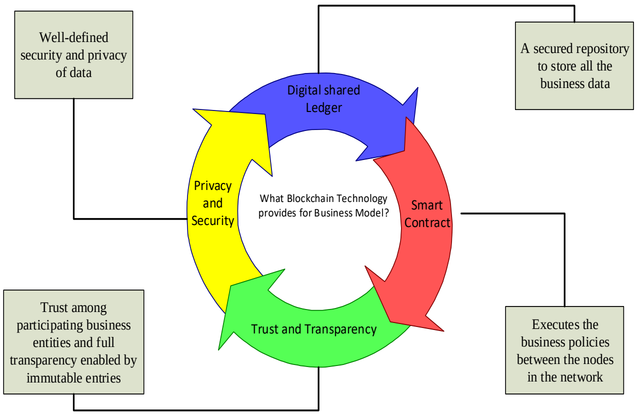

Well-defined security and privacy of data
A secured repository to store all the business data
Digital shared Ledger
Privacy and Security
What Blockchain Technology provides for Business Model?
Smart Contract
Trust and Transparency
Trust among participating business entities and full transparency enabled by immutable entries
Executes the business policies between the nodes in the network

Figure 6. Key Dimensions of Blockchain Usage in Digital Business models

4.1. Banking System [10] [12] [13]

Banking sector has been among the top to adapt blockchain to support their digital banking needs. Millions of customer transactions are processed via banking systems and it is very important to securely store this data in a secured place. Who gathers the data, who has access to the data and where it is stored are aspects critical to the banking system. In traditional systems, the transaction data gets stored in a central server for verifications, validations and maintenance. Consider a scenario where, Bob wants to sell his car to John. Bob sends his public key to John to transfer amount to his account using bank application. John uses Bob's public and his own private key of the bank application and transfers the required amount to Bob's account. Bob uses his public and private key to check the transaction account. In this scenario, Bob and John are connected via bank central system.so every transaction which is taking place via bank application, goes to the server which is maintained by bank's central authority. This server will capture all the data and stores on it. It is also responsibility of central server to maintain the data in proper way. Table 2, shows how Banks registers transaction data in their central databases.

Table 2: Bank Database without Blockchain

Sender Name	**Sender Account**	**Receiver Name**	**Receiver Account**	**Transfer Amount**	**Date & Time**
John	000XXXX20280	Bob	000XXXX08765	5,00,000	31/12/2019 18-00-30

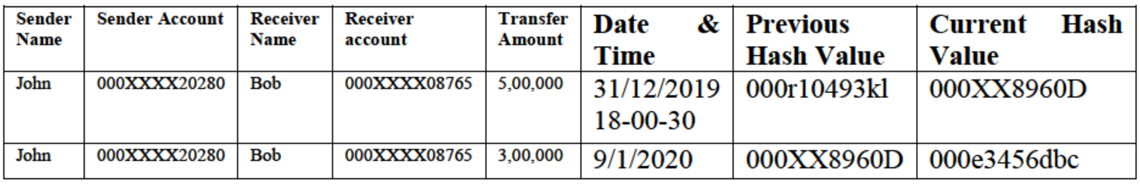
There are a few problems that are associated with centralized system –

i) Time to validate the user account and verify the account details is longer. This impacts the overall transaction time.
ii) Network is vulnerable to malicious attackers who can try to steal data or deny service to other users. Such attacks reduce the credibility of the bank in the eyes of the customers.
iii) Centralized systems are mostly monolithic in nature and require proprietary knowledge for maintenance. Thereby the time to make change is longer. Blockchain technology addresses these issues by eliminating completely a central server system and allows all the nodes to have all the transactional data in their computer in the form of a distributed digital ledger. The above mentioned example can be explained as below in a scenario where Blockchain is used.

Transaction: Bob is selling his car to John

Bob and John login to blockchain applications that are designed to work on a Peer-To-Peer network. Peer-to-Peer network means, Bob and John are connected directly without any intermediaries. Both uses their public and private key to perform transactions. Once transaction is completed, it is verified and validated by other nodes in the network and transaction data gets saved into a digital ledger. The data which is entered into ledger is immutable and is called as tamper proof data. This digital ledger will be shared with every node in the network. It is almost impossible to hack the data for network attacker as the data is stored at every single node in the network. Blockchain Digital ledger will contain the record of transaction data with hash value. Hash value is an unique value for each record of blocks in the digital ledger and shown in Table 3. In digital ledger, every record will contain two hash values.one is previous hash value and other one is current hash value. Previous hash value will have data about previous record details. Current hash value will have current transaction details.

Table 3.Bank Database with Blockchain



Sender Name	Sender Account	Receiver Name	Receiver account	Transfer Amount	Date & Time	Previous Hash Value	Current Hash Value
John	000XXXX20280	Bob	000XXXX08765	5,00,000	31/12/2019 18-00-30	000r10493kl	000XX8960D
John	000XXXX20280	Bob	000XXXX08765	3,00,000	9/1/2020	000XX8960D	000e3456dbc

4.2. Blockchain-Enabled Supply Chain [10][12]

Supply chain is at the heart of many businesses for effective product delivery. This is where the business models should have trust between different business parties and helps to supply the goods from suppliers to manufacturers to consumers. Supply chain is a complex connected network through which manufacturing companies source their raw materials and get their products to market, to sell and profit from them. It encompasses planning, controlling and execution of product flow from raw materials to finished goods. The goal of an efficient supply chain is to function in most effective and streamlined manner possible in order to achieve better performance throughout the network. The main parts of a Supply chain are

- **Planning-** Plan for resources that are required to satisfy the consumer needs
- **Sourcing-** Identify the supplier who provides goods and services needed for product
- **Manufacturing-** Activities including for manufacturing the product and testing it for quality and plan for delivery schedule
- **Delivery(Logistics)-** Collecting consumer orders, plan for safe storage and delivery, dispatching the load and receiving payments
- **Returning –** Providing return policy for goods in case of damage or unwanted product

Physical flows and information flows are two types of flow by which many organizations are linked together to form a supply chain which are i) Physical flow in supply chain deals with transportation, movement and storage of goods. It is actual flow of goods from manufacturing unit to marketplace. This is most visible flow in supply chain. ii) Information flow in supply chain allows organizations to share data about planning, controlling and execution of goods delivery. Here the information is stored in computer systems or in paper documents. In traditional supply chain models, multiple business partners are involved to supply the goods to consumers at right place and time. This scenario is given in figure 7. The business partners have to organize complex, trust-based systems to exchange and store such data with adequate security measures.

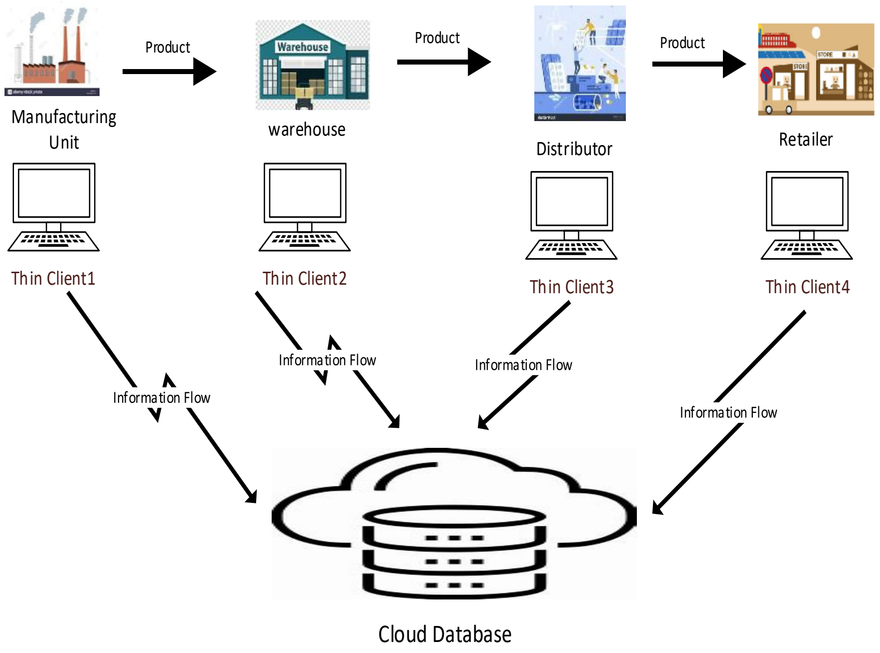


Figure 7. Supply Chain Model without Blockchain

On the other hand, Blockchain helps the business partners not only to exchange data but also have the required visibility throughout the chain. This model helps the business systems to verify the data at any time. This also helps prevent counterfeit products from getting into the supply chain.

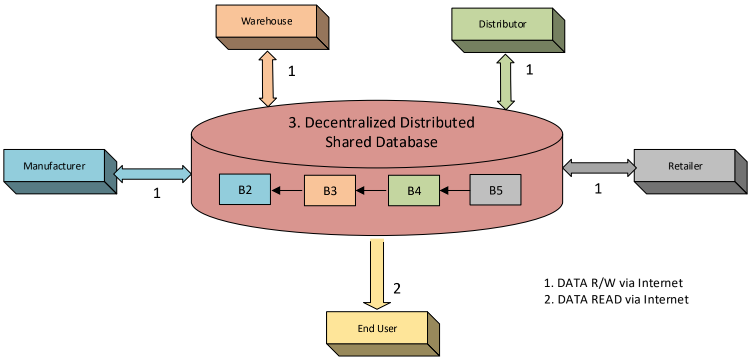


Figure 8. Blockchain Based Supply Chain Model

Blockchain-based supply chain helps businesses to track the product right from manufacturing unit to consumer location as given in Figure 8. Business data at various stages in the supply chain should captured and stored as blocks in the chain of blocks on a network. For example, details like ingredients, date of manufacturing, date of expiry etc., will be captured when goods are getting produced at the manufacturing unit. This information gets validated by other parties in the network, put into blocks and sent to all nodes in the network. When goods move from manufacturing unit to warehouse, warehouse details will be captured and stored as block which will then added into chain of blocks. This will continue till it reaches the consumer. Consumer can check their product simply by reading data from the ledger via a blockchain application. Smart contract, a piece of code embedded into the applications help the nodes to write data into ledger and read from ledgers.

5. Conclusion

Establishing trust and ensuring full transparency is the crux of business to business and business to consumer transactions. Securely storing the data and enabling role-based access to the same is another key goal. In traditional business systems, a complex system design is required to achieve these goals and the same can be quite inflexible and expensive to maintain. Blockchain is a technology that can help overcome these challenges by having a decentralized digital ledger to captures all the valuable data and corresponding transactions. The unique feature of this ledger is that it is immutable in nature which means data and transactions are not modifiable once it is stored in ledger. This helps the businesses to store data permanently in such a manner that it cannot be deleted or modified by other parties without the knowledge of the participants in the blockchain. Data in the blockchain is visible to participants in the network anywhere, anytime. Hence blockchain technology brings trust, transparency, security and visibility to all participants in the business network thereby making it the ideal choice for many businesses to adapt.

References

[1] Sathoshi Nakamoto "Bitcoin: A Peer-To-Peer Electronic Cash System", 2008 [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] Giang-Truong Nguyen and Kyungbaek Kim," A Survey about Consensus Algorithms Used in Blockchain" Journal of Information Processing Systems Vol.14, No.1, pp.101~128, February 2018.

[3] Florian Tschosch and Bjorn Scheuermann, "Bitcoin and Beyound: A Technical survey on Decentralized Digital Currencies" IEEE Communications Surveys and Tutorials,Volume 8, March 2016.

[4] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, " An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE 6th International congress on Big Data.

[5] Shijie Zhang, Jong-Hyouk Lee, "An Analysis of the main consensus protocols of blockchain", ICT Express, August 20129.

[6] A white paper on " Deloitte's 2019 Global Blockchain Survey- Blockchain gets down to business"AvailableOnline[https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

[7] Fan Yang, et.al. "Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism" August 2019, Special section on Emerging Approaches to Cyber security, IEEE Access.

[8] Public-vs–private blockchain , Available online: https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/

[9] Noe Elisa, Longzhi Yang, Fei Chao, Yi Cao. "A framework of blockchain-based secure and privacy-preserving E-government system" Wireless Networks, https://doi.org/10.1007/s11276-018-1883-0

[10] A Study paper on security aspects of a blockchain, TS Division, TEC Available Online: https://www.tec.gov.in/pdf/Studypaper/Security%20aspects%20of%20blockchain.pdf.

[11] Giang-Truong Nguyen and Kyungbaek Kim, " A Survey about Consensus Algorithms Used inBlockchain" J Inf Process Syst, Vol.14, No.1, pp.101~128, February 2018.

[12] Peter Verhoeven , Florian Sinn and Tino T. Herden, "Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology", Logistics 2018, 2, 20; doi:10.3390/logistics2030020.

[13] A white paper on "Blockchain in banking while the interest is huge, challenges remain for large scale adoption "April 18, 2017. Available Online: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-strategy-innovation-blockchain-in-banking-noexp.pdf

[14] A white paper on "Blockchain and Suitability for Government Applications" 2018 PUBLIC-PRIVATE, Analytic Exchange Program", Available Online: https://www.dhs.gov/sites/default/files/publications/2018_AEP_Blockchain_and_Suitability_for_Government_Applications.pdf

[15] A white paper on "\Blockchain Technology in India – Opportunities and Challenges", available Online: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-strategy-innovation-blockchain-technology-india-opportunities-challenges-noexp.pdf

[16] Michael Crosby (Google), Nachiappan (Yahoo), Pradan Pattanayak (Yahoo), Sanjeev Verma (Samsung Research America) ,Vignesh Kalyanaraman (Fairchild Semiconductor), "Blockchain Technology : Beyond Bitcoin" , Applied Innovation Review, Issuse 2, June 2016.

[17] A white paper on "Deloitte's 2019 Global Blockchain Survey". Available Online: www.deloitte.com.

[18] Swan, M. Blockchain: Blueprint for a New Economy; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.

[19] Leila Ismail and Huned Materwala," A Review of Blockchain Architecture and Consensus Protocols : Use cases, Challenges, and Solutions" , Symmetry 2019.

[20] Archana Prashanth Joshi et al, "A survey on security and privacy issues of Blockchain Technology", Mathematical Foundation of Computing, American Institute of Mathematical Sciences, May 2018.

[21] A white paper on "Hyperledger Fabric Framework". Available online: https://hyperledger-fabric.readthedocs.io/.

[22] A White paper on "An Introduction to Hyperledger". Available online: https://www.ibm.com/downloads/cas/0XMOQJNP.

[23] A White paper on "Hyperledger Architecture volume 1", Available on-line: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf.

[24] Sukhwani, H. Performance Modeling & Analysis of Hyperledger Fabric (performance Blockchain Network); Duke University: Duke, UK, 2018.

[25] Anjula Gupta et al, "Cryptography Algorithm: A Review", IJEDR, 2014.

[26] Lukman Adewale Ajao et al, "Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil and Gas Industry", Multidisciplinary Scientific Journal, August 2019