# Blockchain Technologies for Fund Release as Finality in Financial Transaction

**M.V.Ranjith Kumar, Swathi Singh, Mueen Ahmed, Bhandarkar Prasad Prashant, N.Bhalaji**

***Abstract:*** ***We think about that the primary standard of blockchain is changelessness; legitimate and secure exchanges that can never be deleted or overlooked and altered [2].Each party in the process such as broker, custodian or the settlement manager keeps their own record which creates room for error. P2P lending is growing enormously in personal finance. Now both borrowers and lenders are connected to each other via Block chain. A secure, modern, digital system is required to overcome the errors and to prevent them from re-occurring. This project tries to provide a solution to this problem by drawing inspiration from Blockchain Technology. Utilizing blockchain in exercises identified with exchange can kill the requirement for middle people; diminish operational dangers, while giving the framework to quicker exchange settlement. We are organizing the utilization of blockchain based innovation since they have inbuilt attributes to track, square and report ill-conceived endeavors made by anybody on the system, and can give a stage to actualize the security strategy and gauges. This paper aims at establishing a secure private trade network where the exchange of assets between parties takes place.***

***Keywords: Block chain, Multi chain, Transaction Finality, Digital signature, Decentralized Governance, Asset Exchange***

## I. INTRODUCTION

Blockchain technology influenced transforming the current internet from "The internet of information Sharing" to "Internet of value exchange"[1, 9].A requirement for applying blockchain innovation to exchange exercises as it dispenses with the requirement for intermediates and operational dangers while giving a stage to quicker exchange settlements. Money related organizations can settle every one of the necessities in minutes rather than days, with the significant advantages being intended for ongoing repayments, improved movement of business sectors, supply chains, enhancements, and expanded straight forwardness. The blockchain record is structured so that every single existing member have a full record of exchanges which is permanent and it can acquire total straightforwardness and trust in the market which is extremely essential to do additionally exchanges.

**Revised Manuscript Received on May 05, 2019.**

**M.V.Ranjith Kumar,** Assistant Professor, Department of Computer Science and Engineering SRM Institute of Science and Technology, Kattankulathur Chennai, India

**Swathi Singh,** Research scholar, Department of Computer Science and Engineering, SKR Engineering College, Nazarathpettai, Poonamallee, Chennai, Tamil Nadu

**Mueen Ahmed,** Student, Department of Computer Science and Engineering SRM Institute of Science and Technology, Kattankulathur Chennai, India

**Bhandarkar Prasad Prashant,** Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur Chennai, India

**N.Bhalaji,** Associate Professor, Department of Information Technology SSN College of Engineering, Kalavakkam, Tamil Nadu, India

Blockchain can offer a solution to the trade events processing to maintain existing unreliable systems owned by all participants in the system. The innovation can have a decent effect from its utilization in clearing settlements, while safely computerizing the post-exchange process, facilitating desk work of exchange and lawful proprietorship[10].

## II. BACKGROUND

Whenever there is an exchange in a trade, there should exist a private secure network that will ensure privacy and provide more security to the process. Usually, when the assets are being traded in an agricultural network there are minimum chances to achieve that level of security. Due to lack of security, the result is in huge losses, hence these types of supply chain require private and secure networks. To achieve such a level we use blockchain in such processes.

### A. Block chain

Private Blockchain systems are at the other end of the spectrums as they allow only some nodes to be part of the process and only the subset of a particular node can generate a next block[4]. The problems such as mining, privacy and access through the permissions granted by the users are solved by Multichain. The main purposes are: (a) that the work process in blockchain can be seen by only known participants, (b) to supervise the behavior of transactions by giving permissions, and (c) to authorize mining securely without any proof of work and related amount. Problems can be easily resolved when the blockchain size is controlled by the participants once the blockchain is private. Only the transactions which are of interest to the participants of the private network are carried in the blockchain since it is a closed system. To understand permissions in Multichain, we begin by observing that all crypto-currencies manage its identity and security using public keys[11]. The keys are the only way of decrypting the data and the participants can generate their own private keys and should not reveal them to anyone. The identification of funds on the receiving end represents an address having a particular private key. Each private key has its own address which represents an identity for receiving funds. Once the private key is distributed to a public end point, then the fund transaction can only be carried out using the distributed key. It means access to a particular private key is similar to ownership of any funds which it protects. Due to this fact the participant can prove his ownership of the address as the funds associated with it, by providing any message as a proof which has been signed by that particular private key.

The use of this characteristic feature in Multichain is to restrict access to a list of participants that are permitted, by the "handshaking" process that takes place when two block chain nodes connect:

1. On the permission list, the identity of each node is represented as a public address.
2. On the permission list, other's addresses are verified by each node.
3. Messages to the other party are sent by each node.

Signature of the message is sent by each node which proves the authenticity of their ownership of the private key associated with the public address they present. If any of the two nodes is not satisfied with the results, it terminates the end to end connection. Therefore, ensuring the safety and authenticity of the carried transactions. The right to send and receive transactions in a given list of addresses can be restricted. There can be numerous senders and receivers due to which only those transactions are allowed in which the senders and receivers are given permissions. At some instances the blockchain maybe public and restrictions can be applied on transactions. In Multichain, using network transactions all the rights are granted and even revoked containing special metadata. The rights of administrator to grant the rights of other participants is received the initial miner "genesis" block. These rights to other participants in transaction processes whose result matches with the other participant's addresses are granted by the administrator. A constraint is introduced by changing the administration and mining rights of other participants. To make any change, the existing administrators must vote. Each administrator registers these votes in a separate transaction. Once a consensus is reached, the changes will be applied. A single administrator can bypass the initial blocks of a chain known as "setup phase". The modifications to particular rights are attached to the metadata of transactions, they communicate to each nodes in the network swiftly. The network is decentralized causes different nodes to receive permissions for the transactions either before or after other transactions. Depending on the changes in the privileges that were broadcasted before, the validity of the payment transaction may change. The payment being accepted and rejected simultaneously by some nodes, the differences can prove critical. Upon confirmation of these transactions, then only such problems can be resolved on the blockchain. The transactions are always 'replayed' in blockchain order and each node follows this rule to ensure the validity of the transactions in a block as per the permissions granted by the user. The rejection of a transaction in a block makes the whole block invalid.

### B. Multi chain

Multichain is a platform for creating and deploying private blockchains [2]. It aims for the deployment of blockchain technology by providing privacy and control. Compared to the blockchain, Multichain is better as it provides extra functions and support to private blockchains. The internal database is located in one place while in a blockchain, it is distributed. Multichain supports all types of operating systems and provides application program interface and command line interface [3]. In the next few sections, we describe the features on the Multichain and how we can use it for establishing a private trade network.

## III. SYSTEM IMPLEMENTATION

Multichain provides a remote procedure call protocol encoded in JSON(JSON-RPC) application programming interface(API) for the application.[3]. Savoir is a module which enables us to use the API based on Python3. It is very important that we keep on storing information in admin block so procedural nodes i.e. Manufacturer (admin), Distributor and retailer nodes to proceed the request (fig 1). We need functions related to the blockchain, database, and user interface for all the processes.

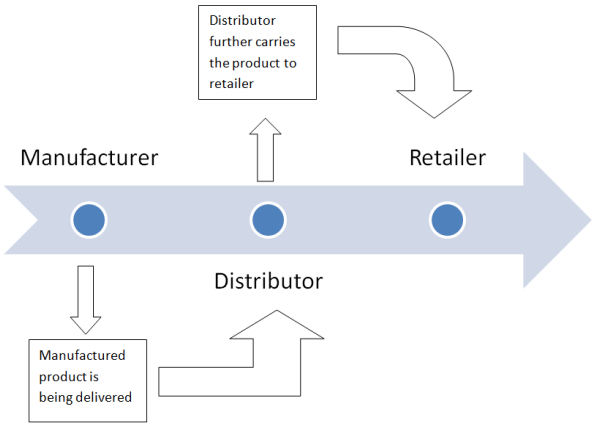


**Fig. 1 System Architecture for Trade system**

### A. Asset Exchange

To start a trade process using a blockchain, we need to create a blockchain first and connect the procedure nodes and it is important to grant these nodes the authority from the admin [3]. The admin can provide authority or permission like sending, receiving, issuing and even mining. All the nodes connected can review the procedure and further continue their process.

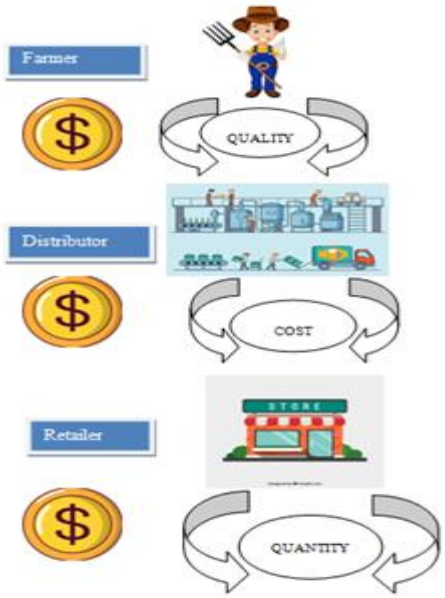


**Fig. 2 Asset Exchange**

### B. Transaction Finality

We think about that the fundamental rule of blockchain is changelessness; legitimate and secure exchanges that can never be deleted or overlooked and altered [2]. Multichain is giving its clients the chance to go into another blockchain based ward where understandings are represented by code. It gives you a confirmation that the system stays nonpartisan. The result of transactions will be spoken to by code you associate with. There are no reversals in the code and transactions are final which means that the applications are unstoppable. Once the manufactured product is delivered, there ceiving asset confirms the delivery and then the only process is completed and the transaction is initiated (fig3).

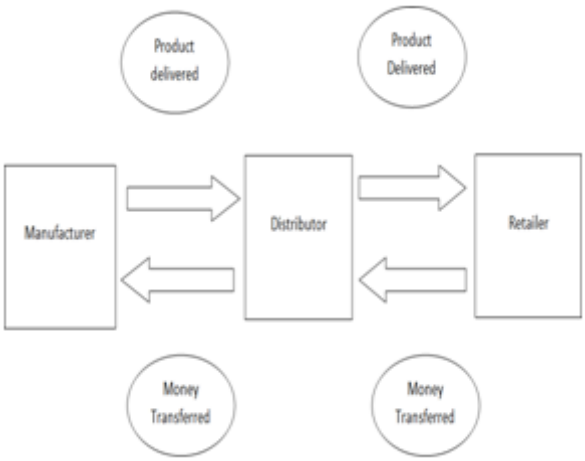


**Fig. 3 Transaction Process**

### C. Decentralized Governance

Blockchain base governance system can offer a range of services traditionally provided by the government all which could be voluntary with user-citizen opting in and out at will [5]. There are various problems that arise due to centralization and opaqueness which leads toward corruption andunaccountability. In comparison to centralized mode, the third party has no need for blockchain [8]. Centralization is fragile and sensitive; so we can predict that decentralized systems can stand the test of time. These problems can be only solved by getting rid of systems that do not rely on a central point of failure. We believe that only decentralized projects can survive in the long run. The needs for decentralized systems are increasing day byday.

### D. Digital Signature

Digital Signatures are designed to guard against tampering and forgery in communications [6]. Every client claims a couple of private key and an public key which they use for getting information. The transactions before being available on open networks are digitally signed using the private key and are then accessible using public keys [6]. Digital Signatures can be broken down into two phases: Signing phase and verification phase[8]. There may arise some cases where we can get an invalid digital signature. Three conceivable reasons can be there for getting an invalid computerized signature:

- Digital mark being corrupted for example not genuine and might be decoded with the public key. The acquired unique hash esteem will be some other esteem and not the accurate unique hash estimation of the message.
- Message or information being changed or altered after its marking. The present hash-esteem determined will vary from the first hash-esteem.
- Public key not relating to the private key is utilized at the ideal opportunity for marking. Unscrambling the mark with an inaccurate key will give wrong unique hash-esteem.

### E. Ensuring Privacy

A fundamental problem that arises in all blockchain transactions in terms of privacy is that the transactions are viewable to all participants [2]. Each user has complete transparency over what data is being collected and how they are being accessed [7]. Each participant can acquire information regarding the total amount of assets being held and traded. This feature is available to the participants due to the basic nature of the blockchain. The transparency may or may not be desired as subjected to the use case. Another prominent problem that arises is that the participants gain knowledge about the public addresses of other participants during transactions which allow them to inspect full balance and trading activity undertaken in the past as well as the ones going to take place in the future.

This problem can be resolved if the participant assigns different addresses for each transaction. Different addresses can be used while sending and receiving the data depending upon the identities of the participants, preventing them from attaining any knowledge of the activities of other participants. Assets can be moved between addresses as per the need of the participants. To ensure no association between the assets deposited and withdrawn, a “coin mixing” service can be employed by a trusted central party. [2]. The transaction asset quantities can be hidden from all the participants other than the sender and the receiver of that particular transaction while allowing all network participants to confirm the authenticity of the transaction.

### F. Database Synchronization

Blockchain technology is best in a decentralized network where all the participants share the same opinion and vision. However, optimization for answering queries related to past activities on that network is very poor [2]. They represent that activity as a log of valid transactions. This log containing the valid transactions is stored in sequential orders that are grouped by block numbers without any additional indexes.

## IV. CONSUMER FACING REWARD SCHEME

Nowadays, consumers use lightweight wallets that are running as mobile applications connecting several nodes in order to receive and send transactions. The exchange of asset quantities within transaction allows these lightweight wallets to transact safely over the network without tracking the movements of assets. Blockchain provides various privileges to its users and anyone can use this system by installing a mobile wallet which generates its own private and public keys and also the addresses. As we know that these keys and addresses play an important role in decrypting the data so be careful with these keys and do not lose them as they

represent your ownership and if lost then we cannot recover them.

Utilizing Blockchain innovation in an inventory network can give great outcomes a customary store network process inside resource the board can be costly and dangerous especially with regards to exchanges. Each gathering in the process, for example, representative, caretaker or the settlement chief keeps their own record which makes space for blunder. Now both borrowers and lenders are connected to each other via Blockchain. A secure, modern, digital system is required to overcome the errors and to prevent them from re-occurring. Blockchain has inbuilt attributes to track, square and report ill-conceived endeavors made by anybody on the system, and can give a stage to actualize the security strategy and models.

## V. LIMITATIONS

- A private network can only consist of limited participants.
- The multichain platform can only be used for creating and deploying private blockchains.
- The transactions in the blockchain are not confidential and can be seen by other participants until the participant assigns different addresses for each transaction.
- Transparency of the data.
- Smart contracts are not well suited to the majority of blockchain use cases.

## VI. CONCLUSION

Multichain is a stage for overseeing, following, and securing exchange exchanges and to build up a private exchange arrange. It will associate all members engaged with an exchange arrange, including purchaser, purchaser's bank, merchant, vender's bank and transporter in one spot (on the web and through cell phones). The framework enrolls the whole exchange process from request to installment, showing it and guaranteeing installment when every single legally binding understanding have been met. The stage is completely mechanized and accessible 24/7, so the request to-installment process is a lot faster than the customary trade of archives. It additionally requires less office organization. The DTC stage will get strategic organizations utilizing the most recent track-and-follow innovation to check the landing of products in concurred condition at key focuses in the voyage from provider to purchaser that will at that point start installments naturally. Transactions are received and sent to different nodes which are connected to consumers through lightweight wallets that are working as web applications. The lightweight wallets are transacted safely without any need to track the movements of assets separately. Since the blockchain has no confinement on correspondence, anybody can utilize the framework which produces its own private keys after establishment.

## REFERENCES


1. Knezevic, Dusko. "Impact of Blockchain Technology Platform in Changing the Financial Sector and Other Industries." Montenegrin Journal of Economics 14.1 (2018): 109-120.
2. Dr. Gideon Greenspan "Multichain private blockchain" 2015.
3. Oh, Se-Chang, et al. "Implementation of blockchain-based energy trading system." Asia Pacific Journal of Innovation and Entrepreneurship 11.3 (2017): 322-334.
4. Gupta, Suyash, and Mohammad Sadoghi. "Blockchain transaction processing." Encyclopedia of Big Data Technologies, SherifSakr and Albert Zomaya (Eds.). Springer International Publishing, Cham (2018): 1-11.
5. Atzori, Marcella. "Blockchain technology and decentralized governance: Is the state still necessary?." Available at SSRN 2709713 (2015).
6. Thompson, Stephen. "The preservation of digital signatures on the blockchain." See Also (2017)..
7. Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." 2015 IEEE Security and Privacy Workshops. IEEE, 2015.
8. Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, 2017.
9. SINGH, Swathi et al. Survey on Surging Technology: Cryptocurrency. International Journal of Engineering & Technology, [S.l.], v. 7, n. 3.12, p. 296-299, july 2018.
10. Kumar, MV Ranjith, N. Bhalaji, and Swathi Singh. "An augmented approach for pseudo-free groups in smart cyber-physical system." Cluster Computing (2018): 1-20.
11. Prabhakaran, S., and M. V. Ranjithkumar. "Advanced Graphical Passwords Using Captcha." International Journal of Pure and Applied Mathematics 118.22 (2018): 351-357.




*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*