ISSN 2278-3091
Volume 9 No.2, March -April 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse117922020.pdf
https://doi.org/10.30534/ijatcse/2020/117922020

Blockchain-based Net Asset Value (NAV) calculation for Mutual Funds

Vijaya Killu Manda[1], Vedavathi Katneni[2], VijayaramarajuPoosapati[3], Vijaya Kittu Manda[4]
[1]Department of Computer Science, GITAM Deemed to be University, mvkillu@gmail.com
[2]Department of Computer Science, GITAM Deemed to be University, vkatneni@gitam.edu
[3]Department of Computer Science, GITAM Deemed to be University, vijaramaraju.poosapati@gmail.com
[4]GITAM Institute of Management, GITAM Deemed to be University, vijaykittu@hotmail.com

ABSTRACT

A model that uses a blockchain-based decentralized ledger system that combines sharing financial security data feeds sourced from a data feed provider and to compute the Net Asset Value (NAV) of a mutual fund scheme by an Asset management company.

Blockchain emerged as a disruptive technology for various fintech areas. Traditional financial services such as the Asset Management industry can use this blockchain-based architecture for mutual fund management taking advantage of features like distributed ledger, immutability, smart contracts, amongst others. The paper discusses the architecture of a mutual fund system to share the Net Asset Values of mutual funds and the last traded prices of securities. The Linux Foundation manages Hyperledger Fabric. The Hyperledger project is an open-source model that can be cost-effective for the stakeholders. The proposed model involves stakeholders such as the data feed provider, regulator, registrar, and transfer agents (RTA/registrar), and the asset management company.

Key words: Blockchain, Mutual Fund, Asset Management Company, Net Asset Value, Fintech

1. INTRODUCTION

Asset Management Companies (AMC) pool investor funds and manage the capital by taking investment decisions related to various capital assets such as equity, bond, and debt instruments, real estate, and commodities. [13]Investors are issued units for their investments. Investors transact in terms of units in mutual fund schemes (including passive funds such as index funds) and Portfolio Management Services (PMS), Investment Trusts such as Real Estate Investment Trust (REIT) and Infrastructure Investment Trusts (InvIT) and Unit Linked Investment Plans (ULIP) of insurance companies amongst others.

Mutual Funds are popular investment tools that carry several advantages over other financial investments. Asset diversification, low costs, managed by professional fund managers, liquidity are some of the attractive features of the mutual fund over investing directly in securities. There are approximately 119,000 regulated open-end funds worldwide, with about 45% of them in the US alone. [11] Increased use of fintech, such as Artificial Intelligence and Blockchain,is seen for making better decisions, achieve higher performance and optimal use of information technology infrastructure. Blockchain is getting increased use in both financial and non-financial domains. [21] Researchers explored the use of blockchain for financial instruments such as peer-to-peer [23] and compliance areas such as halal product assurances. [22]

The Net Asset Value (NAV) represents the value of one unit of a scheme. It is the difference between the total value of assets in the portfolio of the fund after deducting all the liabilities incurred in fund management and dividing it by the number of units issued to investors. [16] The NAV is calculated in-house by the AMC or outsourced to an independent accountancy firm. The value of a scheme changes during the transaction day because of both scheme-specific variables (such as price changes of underlying securities) and macro-economic variables. [9]Funds usually calculate the NAV after the market closes for the day by taking into account the closing price of the securities that the fund holds.

The NAV calculated will be used by various stakeholders such as investors, the Registrars, Regulators (such as SEBI), Self-Regulation Organizations (such as AMFI), Financial Data feed providers, and the business media. The Association of Mutual Funds in India (AMFI), for example, in India, has the mandate to curates the NAV values of all mutual funds and disseminate it in a downloadable format. [1]

Traditionally, an AMC manages multiple systems with different characteristics. Further, each scheme would have plans (Direct/Regular), options (Growth/Dividend), and sub-options. Each scheme, plan, option, and sub-option will have its NAV value. The stock exchange disseminates market quotes and data for various segments such as cash, derivatives, currencies, and commodities. These are fetched by the AMC either directly or through a data feed provider. A different system uses the market data feed and uses it to update the scheme portfolio and then compute the current NAV. Stakeholders such as regulators, registrars, and the investors will then use these values for further usage through their application interfaces. Before saving the data and sharing the values, there may be checks in the system to check the new NAV value to the historical NAVs for that fund.[12]

To make the system robust and straightforward, we propose a blockchain-based system that will not only eliminate some of these systems and make the process flow smoother and straightforward, but also make it immutable, transparent, decentralized and secure.

2. BLOCKCHAIN-BASED SYSTEM

Since decentralization and collaboration are the key features of a blockchain network, this paper attempts to build a blockchain solution to achieve the objectives mentioned. An immutable distributed ledger will also help the Mutual Fund industry with the trust issue. Blockchain networks provide a choice between going with permissioned models or public and permissionless models. [15]

The best application of a distributed ledger with immutable ledger characteristics is the Bitcoin cryptocurrency. Both the Bitcoin and Ethereum distributed applications are public and permissionless blockchain technologies. These blockchain networks are open to anyone participating in it. However, when it comes to the financial domain and mutual fund industry, the performance that it needs to deliver cannot be matched by permissionless blockchain technologies. Also, the identity of the participants of the network needs to be known for regulatory purposes like know-your-customer and anti-money-laundering regulations. [5]Data confidentiality and transparency have a tradeoff. When it comes to financial information and portfolio of the client, the former is of utmost importance. The ledger that will save the transaction data will be replicated across all the participants making it distributed, and the participants will collaborate in the maintenance of the network. Since the blockchain network is append-only, any data changes will get recorded automatically, making the system immutable.

The proposed model will use a blockchain network for the Data Feed Provider (DFP) to publish stock-exchange data feeds, which typically contains information such as the name of the security, last traded price, amongst others. The AMC uses this data to calculate the Net Asset Values (NAV) of its funds and post them on the same blockchain network. The main advantage with this set up is that it uses the distributed ledger concepts which are at the core of the blockchain design. The ledger maintains a record of the transactions and is decentralized. It is and replicated across all the members of the network. Commercial grade transaction systems require real-time accounting, continuous monitoring, and permission management, which a blockchain system has to address. [18]

Hyperledger Fabric is used to setup the blockchain network for this research. The blockchain network will assist in the data dissemination of financial security data that is essential for the computation of the scheme NAV.

3. HYPERLEDGER FABRIC

Hyperledger Fabric is an open-source enterprise-grade permissioned distributed ledger technology (DLT) platform. [8]A DLT platform that is permissioned is suitable because the participants are untrusted. For example, there may be participants in the same network who are competitors, and therefore cannot be fully trusted. While several public permissionless blockchain technologies are available for enterprise use, the Hyperledger Fabric has the distinction for being enterprise-oriented right from its inception. [6]

Though our current model is limited to four organizations with one node each, Hyperledger Fabric can scale up to 26 nodes. Also, choosing the same version of Hyperledger Fabric in all the organizations is likely to have better performance. [10]

3.1 Why Hyperledger Fabric?

- Permissioned blockchain network, since the identity of participants, are to be known
- Pluggable consensus protocol, to choose the appropriate consensus depending on the number of organizations in the network
- No native currency for smart contract execution, to increase the transaction
- Tiered policy structure so that organizations manage resources at network-level separate from resources at channel-level throughput and to have the same operational cost as any distributed system
- Smart Contract system to support consistent updates and querying of data in the blockchain.
- Unlike private programs of the participants to update their ledger of transactions, Hyperledger Fabric allows shared programs to update shared ledgers thus reducing cost and time to process data while improving trust
- Tiered policy structure so that resources managed at network-level separate themselves from those at channel-level
- Transaction throughput scaling from 3,000 to 20,000 transactions per second [7]

4. ARCHITECTURE

4.1 Organizations

There are four participants in our blockchain network. The members in the proposed system are the Data Feed Provider (R1), Stock exchange regulator (R2), Registrar (R3), and Asset Management Company (R4). These four organizations collaborate to form a blockchain network and share data between them.

1. R1, the Data feed provider, provides the instrument names and their last traded prices. The feed is provided by the stock exchange directly, or any data feed provider that is authorized by the stock exchange.

2. R2 is the Stock exchange regulator like SEBI. The regulator will read the Net Asset Values published by the AMC and can use this data for auditing purposes.
3. R3 is the Registrar and Transfer Agents (RTA). Also called "Registrar," these intermediary service providers are organizations who use the NAV values to determine unit allocation for investors, generating reports, provide customer support, and other services. Computer Age Management Services (CAMS), Karvy Mutual Fund Services (Karvy MFS), and others come under this category. (Vijaya Killu, Vedavathi, & Satya Prakash, 2019)
4. R4 is the Asset Management Company (AMC), which generates units of the mutual fund scheme. They calculate the net asset values of the mutual fund they organize and publishes them onto the blockchain

4.2 Consensus Protocol

The pluggable consensus protocol of Hyperledger Fabric means that we can choose a consensus protocol that fits the requirements of our use case. [2] System architects have a choice of using either choosing a fully Byzantine fault-tolerant protocol or a simple crash fault-tolerant protocol when deployed within a single organization. In our network that features four organizations, we use the Byzantine fault-tolerant consensus protocol.

4.3 Ordering

Hyperledger Fabric ordering service will help achieve consensus on the blocks of transactions in our blockchain network and their order.Unlike permissionless blockchains like Ethereum and Bitcoin, our blockchain network uses a deterministic consensus than the probabilistic consensus model.

We use an execute-order-validate paradigm rather than order-execute that most existing smart-contracts follow. The advantage ofan execute-order-validate is that we gain scalability and performance. An endorsement policy specifies which subset of peers needs to execute or endorse the transaction before ordering them.

Transactions are endorsed by endorsing peers and are eventually sent to the Orderer, which orders the block of transactions to their peers. Any transaction that is ordered by the Orderer and validated by the peers is guaranteed to be correct. This execute-order-validate structure helps in achieving high performance and scalability in the network.

In our network, the ordering service comprises of a single node O4, configured according to network configuration NC4. The Node O4 runs on the infrastructure provided by organization R4. In a multi-node setup, there could be several ordering service nodes that run on other organizations, but for the model that we are building, we use a single ordering service node.

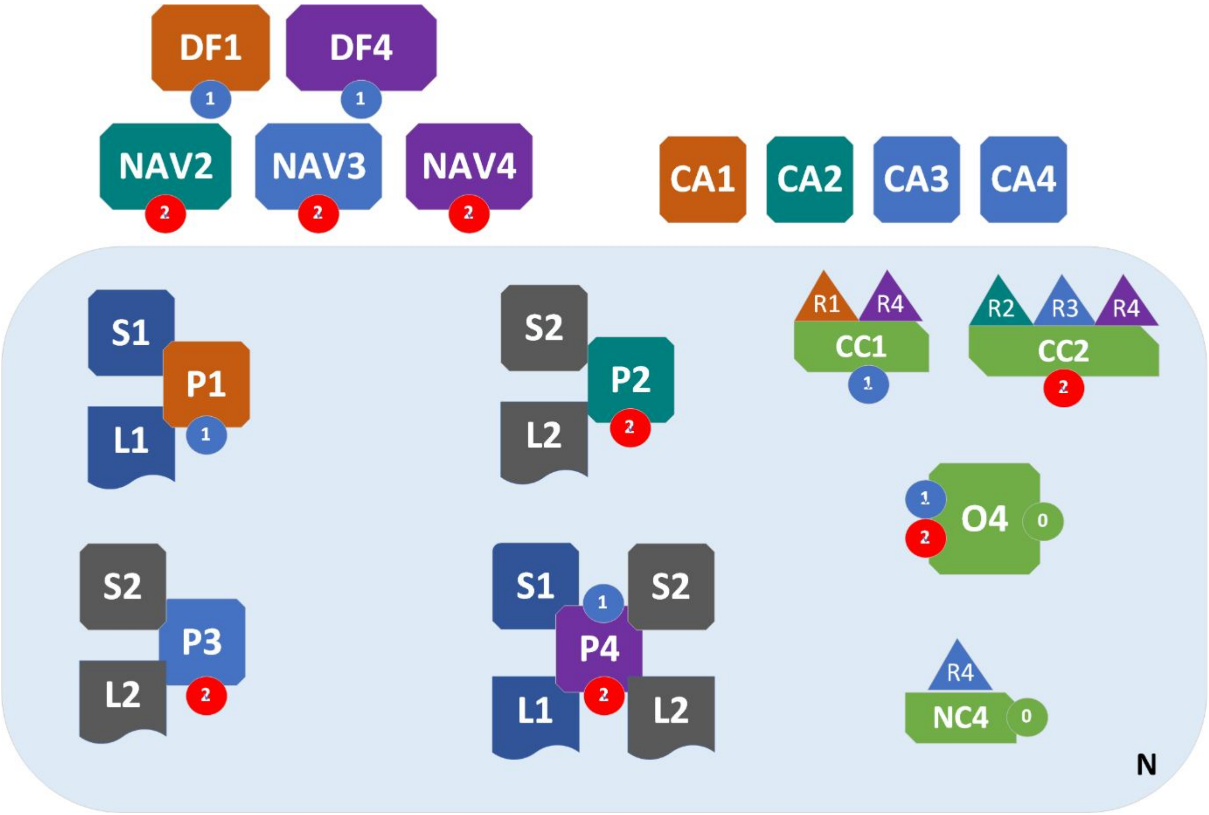

Figure 1: Architecture of the Blockchain model

4.4 Configurations

The blockchain network defines its policies in Network Configuration NC4, which describes the administrative capabilities. The policies define which participants can control access to network resources. The network starts with the ordering service O4, which makes it the initial administration point of the network. NC4 lists the administrators of the network, which in our model is only the Asset Management Company R4. Being a tiered structure, we can configure the network in such a way that the network configuration is different from channel configurations. Organizations defined in the network configuration will manage resources at the network level, while participants defined in the channel configuration will manage their respective channels. The network and channel configurations are replicated and kept in sync by every node in the network. So, O4 has a copy of the network configuration, while R1 has a copy of CC1, R2, R3, and R4 have copies of CC1 and CC2 application channel configurations.

4.5 Certificate Authorities

The certificate authorities in the network generate X.509 certificates, which identify the components of the network, such as administrators and network nodes. These certificates can also be used to sign transactions, thus marking endorsement of a transaction. In our network, we will use four certificate authorities (CA1, CA2, CA3, CA4), one for each organization, to identify components belonging to the four 6organizations, respectively.

4.6 Consortium

Consortiums define the organizations which transact with each other on our network. Administrators of the R4 organization create Consortia.

The first consortium that we create (X1) consists of two members - R1 and R4 organizations. A channel C1, with members of the consortium, is then created to share the data feed of the instruments and their last traded prices in the network. R1 shares the data feed on channel C1, which is read by R4 to calculate the NAV values of its funds. Network Configuration NC4 saves the configuration of the consortium. We use the first consortia to create channel C1, which shares the Last Traded Prices between the Data Feed Provider and the Asset Management Company.

In the second consortium (X2), participants in the network include the asset management company R4, regulator R2, and registrar R3. The AMC can share the latest Net Asset Value of its mutual funds to both the regulator and the registrar by creating a Channel C2. Like the first consortium, an administrator from R4 will create the consortium definition for X2.

4.7 Channels

In our model where some data on the network needs to be private, we make use of a channel system where a set of peers on the network form a sub-network called a Channel. A channel shares data in the form of transactions between organizations defined in a consortium. Those members in the channel have visibility to a set of transactions, thus preserving confidentiality and privacy of transactions. [3] The confidentiality and privacy of the smart-contracts and transaction data are protected. [20] This aspect of privacy-preserving architecture contrasts with the public permissionless blockchain networks which host the data in every node in the peer. The channel configuration is saved in a file that is separate from the network configuration, and only the members mentioned in the channel configuration will have permissions on the channel.

Channels can further help in communication between various components in the organization and the network. For example, a client application can use the channel to connect to a peer that is hosted in the organization and the Orderer that is hosted in the network on another organization.

4.7.1 Data Feed Channel

To share the instrument names and their latest traded prices, we create a channel C1 with members of consortium X1, i.e., R1 and R4. Any data shared on the C1 channel is visible to only members of the channel. The channel configuration is defined in CC1, which is managed by data feed provider R1. The channel configuration CC1 is separate from Network Configuration NC4, such that even administrators defined in network NC4 have no rights on the channel C1 unless they are also members in CC1.

4.7.2 Mutual Fund NAV Channel

A second channel C2 is created so that the asset management company can share the Net Asset Value (NAV) of its mutual funds. The configuration of channel C2 is defined in CC2. This configuration is entirely different from network configuration NC4 and data feed channel configuration CC1.

4.8 Peers

Peer nodes physically host a copy of the ledger within an organization. The current state of the application, apart from the ledger, is also maintained in the peers. [14] The present model defines four peer nodes P1, P2, P3, and P4,which are hosted by organizations R1, R2, R3, and R4, respectively. Peer nodes communicate with Orderer O4. Peer Nodes P1 and P4 host ledger L1 for channel C1. Each peer node can be recognized by the X.509 identity issued by the certificate authority. A peer node, once started, will send a join request to the Orderer, which checks for its permissions on the channel configuration file. In our model, all peer nodes carry a copy of the smart contract.

4.9 Client Applications

Client Applications communicate with the blockchain network using channels. All communication between a client application and a peer is done through the use of smart contracts via channels. Whenever a client application access the smart contract chaincode peer nodes, the peer will use its copy of channel configuration to determine the access rights of the application. For example, the application could be allowed only to read or write data from the ledger.

4.9.1 Client Application DF1, used by DFP

In our model, the data feed provider R1 uses a client application DF1 to publish the last traded prices of instruments. The application DF1 can communicate with Peer P1 and orderer O4 using the communication capabilities mentioned in channel C1. Application DF1 can be identified by the certificate provided by CA4. So, in order to update the last traded price of an instrument, the DFP will invoke a function on application A1, which interacts with the smart contract S1 on node P1. Since the node P1 hosts a copy of smart contract S1, it can take part in the transaction endorsement and generate an LTP update transaction.

4.9.2 Client Application DF4, used by AMC

The Asset Management company can read the last traded prices published to smart contract S1 through application DF4. The X.509 certificate for application A4 is generated by CA4, which generates certificates for all components in organization R4. The DF4 application is configured to only read data from the ledger L1.

4.9.3 Client Applications NAV2, NAV3, and NAV4

The second set of applications NAV2, NAV3, and NAV4 deal with the transfer of Net Asset values between Asset Management Company, Registrar, and Regulator. NAV4 is accessed by AMC R4 to update the NAV values on the blockchain network with write access. NAV2 and NAV3 have only read access to the L2 ledger. All these three applications interact with the S2 smart contract and ledger L2.

4.10 Smart Contracts / Chaincode

Smart Contracts define the business process for the consistent update of data in the blockchain network as well as for querying it.(Christopher, Vikram, & Lee, 2016) They are used to generate transactions that are subsequently distributed to the peers in the network by the Orderer. While a smart contract defines the transaction logic, the chaincode packages these smart contracts for deployment.

The Data feed provider (R1) will use a smart contract S1 for publishing the last traded prices of the instruments which can be read by the other participants in the network. Rules can be stipulated to ensure that only the DFP will have access to update the LTP ledger. In contrast, the other participants, like the Asset Management Company,are limited to reading them. The AMC will use another smart contract which will read the data published by the data feed provider and use it to, in turn, calculate and publish the Net Asset Values daily.

Smart contracts S1 are installed on peer nodes P1 and P4 to allow applications A1 to interact with the peer ledger. In the first organization, the application A1 is connected to Orderer O4 and peer P1 using the communication facilities provided by channel C1. Before a smart contract can be used in a peer, the administrator of the organization where the peer is hosted has to approve the chain code definition. Approval from a sufficient number of organizations is required before the smart contract interface can be committed on the channel and can be used by the client applications. In our model, the chaincode definition is approved by both R1 and R4.

Smart contract S2 shares the NAV by the AMC. S2 is accessed by applications NAV2, NAV3, and NAV4 of R2, R3, and R4 organizations, respectively.

Chaincode definition has a critical configuration called an endorsement policy that defines which organizations should approve transactions before they can be accepted.(Androulaki, Angelo, Neugschwandtner, & Sorniotti, 2019)In the present model, DFP R1 should endorse the latest traded price and update transactions since they are the ones generating it. Peers P1 and P4 can commit all transactions that are validated by R1 in smart contract S1.If the DFP needs to change the chaincode definition, then the change should be approved by both the DFP and AMC. The DFP will then commit the new definition onto the channel.

Developers coding smart contractsneed not have to learn a new programming language that is specific to the blockchain technology.This is one of the crucial advantages of Hyperledger Fabric and is an important consideration for its usage in this model [17] The smart contracts S1 and S2 can be written in programming languages such as Go, Java, or Javascript.For organizations that run Ethereum, the existing business logic in smart contracts that are coded in Solidity can be converted to Javascript smart contracts for Hyperledger Fabric using open source-to-source translation tools like Sol2js. [19]

5.SCOPE FOR FURTHER STUDY

The current model limits to a single peer node per organization that connects and communicates with the larger blockchain. The organization node, in turn, can have internal connectivity with other nodes of the organization, thereby increasing the blockchain scalability and resiliency. Increased peers can reduce system outage and network downtimes. The architecture is flexible and extensible by adding several peer nodes per organization hosting a copy of the Ledger L1. Some of these peers could further host a copy of the smart contract. In such a setup, the possibility of leader peerstake up the responsibility of distributing transactions to other peers in the organization can be explored.

Even though the channel concept in our model supports private communication between organizations, we can further encrypt the data that is shared in a channel using secure multiparty computation (MPC). [4]

6.CONCLUSION

Blockchain applications are making increased inroads into fintech areas. This paper builds an architecture using blockchain features such as decentralized, immutable ledger, smart contracts, using Hyperledger Fabric for use by the mutual fund industry. The system shares the last traded prices of instruments, computes the latest net asset values of various mutual fund schemes, and distributes it to the stakeholders using the blockchain network. The system shows several advantages such as efficient data transfer and sharing between stakeholders, maintain immutable that is not only distributed but also immutable.

REFERENCES

1. AMFI. (2020). **AMFI Net Asset Value (NAV)**. Retrieved from AMFI: https://www.amfiindia.com/net-asset-value
2. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A., . . . Yellick, J. (2018). **Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains**. EuroSys '18. Porto, Portugal. doi:10.1145/3190508.3190538
3. Baliga, A., Solanki, N., Verekar, S., Pednekar, A., Kamat, P., & Chatterjee, S. (2018). **Performance Characterization of Hyperledger Fabric**. 2018 Crypto Valley Conference on Blockchain Technology. doi:10.1109/CVCBT.2018.00013
4. Benhamouda, F., Halevi, S., & Halevi, T. (2019, March/May). **Supporting private data on Hyperledger Fabric with secure multiparty computation**. IBM Journal of Research & Development, 63(2/3). doi:10.1147/JRD.2019.2913621
5. Bogatov, D., Caro, A., Elkhiyaoui, K., &Tackmann, B. (2019). **Anonymous Transactions with Revocation and Auditing in Hyperledger Fabric**. Retrieved from https://eprint.iacr.org/2019/1097.pdf
6. Cachin, C. (2016). **Architecture of the Hyperledger Blockchain Fabric**. Retrieved from https://pdfs.semanticscholar.org/f852/c5f3fe649f8a17ded391df0796677a59927f.pdf
7. Gorenflo, C., Lee, S., Golab, L., & Keshav, S. (2019). **FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second**. IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/8751452/
8. Hyperledger Fabric. (2020). **Hyperledger Fabric Documentation. Retrieved from Hyperledger Fabric**: https://hyperledger-fabric.readthedocs.io/en/release-2.0/whatis.html
9. Komariah, S., Amalia, S., &Suhardi, A. (2020, February). **Macroeconomics and Net Asset Value (NAV) on Equity Mutual Funds**. International Journal of Psychosocial Rehabilitation, 24(2), 3164-3172. doi:10.37200/IJPR/V24I2/PR200623
10. Nasir, Q., Qasse, I., Talib, M., & Nassif, A. (2018). **Performance Analysis of Hyperledger Fabric Platforms**. Hindawi Security and Communication Networks. doi:10.1155/2018/3976093
11. Otten, R., &Bams, D. (2002). **European Mutual Fund Performance**. European Financial Management, 8(1), 75-101. doi:10.1111/1468-036X.00177
12. Parsons, R., & Ray, T. (2001). US Patent No. US7587354B2. Retrieved from https://patentimages.storage.googleapis.com/86/be/4e/714c6b4c81a692/US7587354.pdf
13. Satya Sekhar, G. (2017). **The Management of Mutual Funds**. Palgrave MacMillan. doi:10.1007/978-3-319-34000-5_5
14. Sharma, A., Agrawal, D., Schuhknecht, F., & Dittrich, J. (June 30–July 5, 2019). **Blurring the Lines between Blockchains and Database Systems: the Case of Hyperledger Fabric**. SIGMOD '19. Amsterdam, Netherlands. Retrieved from 10.1145/3299869.3319883
15. Taskinsoy, J. (2019, October). **Blockchain: A Misunderstood Digital Revolution. Things You Need to Know about Blockchain**. SSRN Electronic Journal, 1-25. Retrieved from https://www.researchgate.net/publication/336349583
16. Tripathi, D., & Shukla, A. (2013, December). **Impact of Net Asset Value of Mutual Fund**. IJMRR, 3(12), 3895-3900. Retrieved from http://ijmrr.com/admin/upload_data/journal_Diksha__7dec13mrr.pdf
17. Valenta, M., & Sandner, P. (2017). **Comparison of Ethereum, Hyperledger Fabric and Corda**. FSBC Working Paper. Retrieved from https://www.semanticscholar.org/paper/Comparison-of-Ethereum%2C-Hyperledger-Fabric-and-Valenta-Sandner/9f4f80c8e596b70ec8e2324f44ede15c48c147b5
18. Wang, Y., & Kogan, A. (2018). **Designing confidentiality-preserving Blockchain-based transaction processing systems**. International Journal of Accounting Information Systems. doi:10.1016/j.accinf.2018.06.001
19. Zafar, M., Sher, F., Janjua, M., &Baset, S. (2018). **Sol2js: Translating Solidity Contracts into Javascript for Hyperledger Fabric**. SERIAL'18. Rennes, France
20. Thomas, Monica., Chooralil, Varghese S. (2019). **Security and Privacy via Optimised Blockchain**. International Journal of Advanced Trends in Computer Science and Engineering. Doi: 10.30534/ijatcse/2019/14832019
21. Chaitanya, A. Krishna, et al.,.(2019). **Cryptographic based Message Transfer using Blockchain Technology**. International Journal of Advanced Trends in Computer Science and Engineering, 8(1.3), 2019, 45 – 50. Doi: 10.30534/ijatcse/2019/1081.32019
22. Katuk, Norliza. (2019). **The application of blockchain for halal product assurance: A systematic review of the current developments and future directions**. International Journal of Advanced Trends in Computer Science and Engineering, 8(5), September - October 2019, 1893 – 1902 https://doi.org/10.30534/ijatcse/2019/13852019
23. Vijaya Kittu, Manda., Satya Prakash, Yamijala., (2019). **Peer-to-Peer lending using Blockchain**. International Journal of Advance and Innovative Research, 6(1), January – March 2019, 61-66