Statistical Assessment of Hybrid Blockchain for SME Sector

SAUGATA DUTTA
Research Scholar, Galgotias University,
Greater Noida, Uttar Pradesh, INDIA

KAVITA SAINI
Associate Professor, Galgotias University,
Greater Noida, Uttar Pradesh, INDIA

***Abstract**:* Blockchain innovation with its property of immutable data isn't just limited to digital cryptographic forms of money yet in addition for various domains like healthcare, logistics, rentals, entertainment, social media and so on. Ventures are investigating this innovation to adopt in main line of business, which will give certainty on security ceasing data breach. This research paper has built up a hybrid blockchain framework which can be utilized on premise or over the cloud or a combination of both and can be utilized by various departments for protecting transactions in small and medium scale businesses with an uprightness of high security, transparency, remote devices, accessibility and cost adequacy. This created framework compares with the traditional approach model on some significant factors for statistical assessment. The analysis discovers how this hybrid blockchain framework is more productive and secured than the client server approach model and aims to be utilized as platform as a service both in local or hybrid cloud infrastructure.

Keywords—Blockchain; hashing; decentralization; peer to peer; private blockchain; cloud blockchain; Network Security

Received: June 5, 2020. Revised: November 16, 2020. Accepted: December 29, 2020. Published: January 13, 2021.

1. Introduction

Blockchain technology has emerged market in 2008, however the recognition of using this technology has started from 2010 onwards. The blockchain in its primitive form was designed by Ralph Merkle in 1979 which was known as Merkle Tree. The theoretical conceptualization was done on 2008 by Satoshi Nakamoto. The practical implementation came into existence with digital cryptocurrencies in 2009. The technology is decentralized, peer to peer, hashed and without the interference of third party authority. The technology itself is self-sufficient and secured. The blockchain technology works in a chain of blocks which is hashed and distributed to make it more secured and transparent. As each block is hashed and correlated with each other, in case if any of the block is tampered then the entire chain becomes invalid. This also uses a concept known as proof of work which slows the process of creation of block. The combination of proof of work and hashing makes it more secured and tamper free. New node which joins the network gets a copy of the blockchain and also once participated, verifies that none of the block is tampered. The underlying technology of blockchain behind digital cryptocurrencies has more to contribute, precisely on a very large scale. The blockchain technology can be used appropriately on a much secured way to various domains and industries. The security layer of blockchain is so robust and strong and it is nearly impossible to tamper with the system. In order to compromise this technology, one has to tamper with all of its block, recalculate the proof of work and take control of more than half of the nodes in blockchain which is in a peer to peer network.

Transactions systems can be more secure by using this technology where data cannot be tampered as there will be no centralized server. The entire data will be in the form of chain of blocks where the data is decentralized and every nodes has the copy. The entire transaction will be transparent and robust both from the prospective of vendor as well as for organization. From the perspective of an organization, a number of factors needs to be considered including; how the transactions in the organization is managed, what technology will be used, how will results be stored and reported to the management, how will third party access the data, what programming standards should be followed, how secured is the transaction, how the data is tamper free, how

the vendor data is not disclosed, will the security feature be available over the cloud and how data is leak proof. To ensure the underlying technology of blockchain used as a secure transaction preferably for the small and medium scale industries, a framework to be developed and facilitated in a manner that will have decentralization, cloud availability, greater transparency, enhanced security, robust, improved traceability and immutability. Recent technological advancement has created the possibility of using blockchain technology in shared economy, logistics, registration, healthcare, election, IOT, intellectual property and so on and so forth. Developing, experimenting a hybrid blockchain framework for an organization will help in transparency, immutable data, inability of fraudulent, and data loss. The developed framework for transaction entry like access management, material management, finance, operations, sales, vendor management, technical and so on using blockchain technology is not only restricted to a single location but can be used in different multiple geographical location where it will create a platform both for vendors and organization perspective. The chain consists of all transactions and can have a filter view while data is immutable. The management dashboard can give a clear understanding of the recent and retrospective history of transactions in the organization without the need of a central commanding authority. This framework is not only restricted to a private blockchain but can be applied over the cloud. This framework creates a platform as a service infrastructure upon which one can create or develop a blockchain app, smart contracts which can be utilized on the combination of local and cloud network as well as utilizing the combination of traditional database. The research has led to develop hybrid blockchain framework which has better performance, security, hybrid in implementation and technicality, high availability and better manageability.

2. Relevant Work in the Area

Xiwei Xu et al. (2018) applied a Blockchain mechanism in a project called originChain. When this technology is used it provided transparent and tamper proof traceable data which included high availability. There is a large impact on the quality of the system with the structural design of the system [1].

Paula fraga-lamas et al. (2019) investigated and prescribed to use blockchain in vehicle industry. This has set off for another plan of action and model for business in car sharing industry. The exploration was finished with various analysis on quality, weakness, openings, threats, improvements and recommendations. [2].

D Dujak et al. (2018) traces the utilization of blockchain technology in supply chain industry. The paper examines in creation of blockchain applications using distributed ledger for logistics and supply chain management. [3].

Asad Ali et al. (2019) discusses the advent of Blockchain technology in healthcare industry which has changed the model of traditional health care system with effective diagnosis and secure data sharing. This paper also discusses with the Blockchain applications in healthcare domain with challenges and future aspects [4].

Olga Labazova et al. (2018) demonstrates various Blockchain based systems contributing new technical dimensions and linking applications. This paper also presents an overview of current Blockchain based system [5].

Cao, Y et al. (2019) discussed the feasibility of using Blockchain technology in energy industry and also discussed the applied methodology by the pioneers. This paper also discusses the application practices of Blockchain technology in domestic and over-seas and also the challenges [6].

Yli-Huumo J et al. (2016) explores different research topics on blockchain for research on technical aspects and future directions and have found that most of the research is based on cryptocurrencies and some small portions of research paper are on blockchain based applications [7].

T. Ahram et al. (2017) discusses about the use of blockchain technology is various line of business applications. Blockchain which may be said to be the fundamental base of cryptocurrency has emerged in different security

mechanism in order to cater in an innovative way for growing demands [8].

K, Biswas et al. (2016) proposed a framework where blockchain can be integrated with various smart devices for creating a secure platform in developing a smart city. This framework will overcome those security challenges that may rise with advancement of different technologies used in association to smart city [9].

W. Meng et al. (2018) reviews blockchain with intrusion detections and its applicability. IDS nodes interact data within themselves, in order to protect the integrity of the data exchange, blockchain technology can be applied to restore the security and tampering attack of data [10].

Dmitry Efanov et al. (2018) explores the huge impact of blockchain technology in day to day life. Blockchain features such as distributed database and consensus algorithm with immutability of data are some of the characteristics and fundamental invention post internet [11]

Miraz, Mahdi H et al. (2018) surveyed various implementation of blockchain and proposed blockchain technology enabled systems in industry applications. Various research papers and articles were studied to assess the benefits of blockchain with its solid security features like proof of work and cryptographic puzzle [12].

D. Vujičić et al. (2018) briefed some introduction on topics like blockchain, bitcoin and ethereum. Ethereum with focus on creation of blockchain based applications like smart contracts which can be used in various business lobby's and are self-executable which can also be used in development of digital currencies. Bitcoin which already has a precedence over all latest digital currencies of its invention continued to be the market leader [13].

Saugata Dutta et al. (2019) reviewed use of blockchain technology being used in social media which prohibits fake news, maintains privacy of data, induce rewards for postings and controlled advertisements [14].

Saugata Dutta et al. (2019) explored opportunities in the field of blockchain technology in different industries where this technology is extended to diverse domains [15].

Kavita Kumari et al. (2019) designed a blockchain system with keyless signature infrastructure which can be used to stop counterfeit drugs in health care system [16].
Kavita Saini (2018) explored opportunities in the field of blockchain, its use in currencies, its benefits and effectiveness and future prospect [17].

Kavita Saini et al. (2018) discusses algorithms and encryption techniques in hybrid cloud environment. It discusses the functionality and drawbacks of various encryption algorithm and concludes the benefits of end to end encryption [18].

3. Traditional Model

In this section, a common place technology one would encounter for centralized (client-server) transactions systems.

Data Security: Data in traditional model can be accessed/edited/deleted at any point of time and has control by a central authority, which can result in fraudulent, corruption and portraying wrong information.

Hardware, maintenance and license cost: Traditional model incurs expensive hardware costs, along with the operating system, database software and maintenance cost. Creation of fault tolerance and disaster recovery is pretty much higher.

Transparency: Data on a traditional model can be used in a wrong way. The ownership of data lye on the central authority. The integrity of information is kept within the organization itself.

Cyber threat: The data can be vulnerable to various cyber-attacks like ransomwares, malwares, SQL injection, cross-site scripting and other virus attacks

Interoperability: there may be a challenge in operating on various devices irrespective of the firmware or operating software.

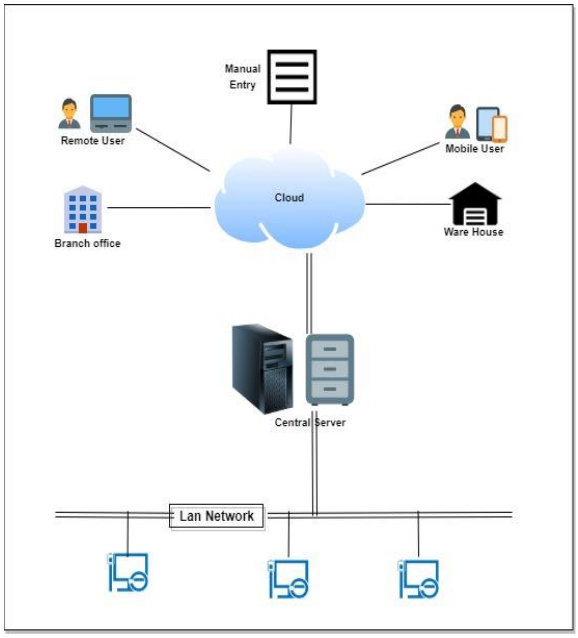

Fig 1: Traditional approach model

4. Problem Definition

The traditional transactional model have potential security and transparency problems. The problems are bulleted as follows:

- The manual register can be altered or modified for financial benefits
- The data stored in the central server can be edited or removed from the backend database.
- High license and maintenance cost
- If entries are registered on a central software, then the record is vulnerable for modifications and deletions
- Vulnerable for corruption and fraud
- Back dated modification of data
- Data can be removed/modified/deleted for personal grudges, criminal activities, fake or mock entries and theft.
- Vendor/Suppliers doesn't have the transparency of goods supplied unless he checks his record or acknowledgement of the receipt.
- History of records are not transparent to the vendor
- Prone to hacking attacks such as SQL injections and Cross-site scripting (XSS).

These are some of major potential loop holes in the traditional transactional model in small and medium size business sector. Holistically, the demerits of using client server approach is less secured, alterable, data leak and prone to cyber-attacks.

5. Objectives

In order to solve the above mentioned problems, research has been carried out by setting following objectives:

1. To identify and work-out an efficient strategy for a secure technology platform.
2. To study the pertinent issues with respect to efficiency of secure transactions using Blockchain technology with specific reference to security and immutability.
3. To identify the essential attributes that contributes towards efficiency of secure transaction entry using Blockchain technology.
4. To review and critically examine the available theoretical bases, research findings and practical citation leading to fruitful inferences.
5. To develop a conceptual /theoretical framework for efficient secure transaction entry using Blockchain technology
6. To design an authoring framework for efficient secure transaction using Blockchain technology.
7. To experiment and test the validity of the framework-leading to asset of critical inferences.
8. To review, modify and formulate the framework for secure transaction entry using Blockchain technology

6. Siginificance of Study

This blockchain framework will be of significant to the organization for secure, transparent and robust process for secure transaction entry. This will fulfill the problem statement with the given framework.

Study has covered the following points:

- A decentralized hybrid blockchain application framework to be developed
- Can be deployed on premise as well as on cloud or both which will have affordability with enhanced security.
- Data will be on a distributed P2P network
- Can be accessed from different geographical location
- Vendor, customers and organization details transparency
- Transactions are secured on blockchain and can be adopt by any industries.
- Low infrastructure and maintenance cost.
- The data inserted in block can never be edited or deleted and have probabilistic immutability
- Provision of adding new nodes which exchanges the blockchain information and transactions are validated.

The study will be able to satisfy the need of the problem statement with the blockchain framework.

7. Methodology

The developed blockchain framework platform as a service not only addresses security issue, but also seizes the data tampering at any level. The data is transparent both to the organization, customer and vendor. Since the data is stored in chain of blocks and are correlated with hash which is immutable.

The developed framework consists of following main components:

- *A hybrid blockchain.*
- *An application platform that takes the input of data and creates a blockchain in context to secure transaction system.*
- *Provision of adding new nodes which holds the copy of the chain*
- *A private TCP / IP network connected with internet*
- *A cloud subscription*

The hybrid blockchain model have all transaction entries in the chain which is immutable. The lite copy of the chain will reside in the blockchain app for all stake holders in blockchain. The full copy of the blockchain will reside in the full nodes situated in the cloud and on premise server to sustain the continuity of the chain. Records will be transparent and non-editable for all. The mining will work as an approval from departmental head, may not be a cryptographic puzzle but an authorization to add the data in blockchain with multifactor authentication.

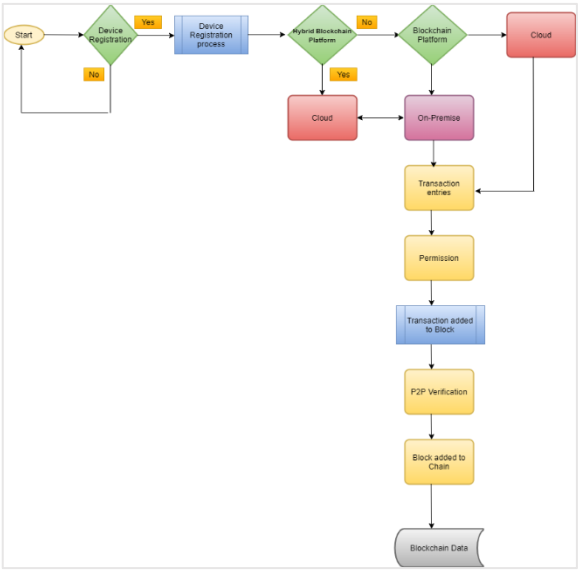

Fig 2: Transaction flow chart

The framework has been created in python as the coding language and flask/Django to create endpoints for blockchain.

First a block is created which includes items in the class namely Id of the block, timestamp, transactions and previous hash.

```
class my_block:
    def __init__(self, block_id, transactions, time_stamp, hash_previous, nonce=0):
        self.block_id = block_id
        self.transactions = transactions
        self.time_stamp = time_stamp
        self.hash_previous = hash_previous
        self.nonce = nonce
```

Fig 3: Block class declaration

Hashing is used in blocks, which takes any size of input and produces a fixed size of output. Blake2b 512 bit hashing is used in this framework.

Genesis block is known to be the first block which has its own hash without the previous hash. Blocks are chained with hash. This will help to stop the risk of changing the contents of the block and make it immutable. If any of the block is changed then the hash of the block also changes, as a result all the corresponding blocks will be invalid.

```
def make_genesis_block(self):
    genesis_block = my_block(0, [], time.time(), "0")
    genesis_block.hash = genesis_block.calc_block_hash()
    self.chain.append(genesis_block)
```

Fig 4: Genesis block

In this framework, a proof of work has been applied although, but for a private blockchain transactions are permissioned to add to the block. Usually a nonce number is required to guess in order mine the block. A difficulty level can be set that generates hash and must end with two zeroes. This will delay the process of generating new blocks, even if someone tries to change the hash of the block, the new hash generation will be required to match this protocol which is nearly impossible to compromise the chain.

After the proof of work process or in case of permissioned process in private blockchain the transactions are appended to the block. Transactions unless not added to the block cannot be termed as confirmed and are unsettled transactions. Once transactions are included in the block, the block is then added to the main chain known as blockchain. During this process, the previous block hash is added to the latest block.

```
# Here a new block is added after veification to the chain
    def add_new_block (self, my_block, proof):
        hashpre = self.lb.hash
        if hashpre != my_block.hashpre:
            return False
```

Fig 5: Add new block

In order to communicate among the nodes with the decentralized applications flask framework is required. A User interface (HTML) is developed for some modules and used REST-API when and where UI could not be created as per experiments on different industries.

```
app = Flask(__name__)

blockchain_nodes = My_Blockchain()
blockchain_nodes.make_genesis_block()

peers = set()
```

Fig 6: Flask and block nodes

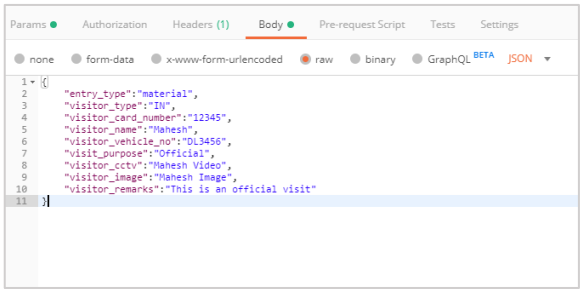

Fig 7: REST-API transaction entry in Blockchain

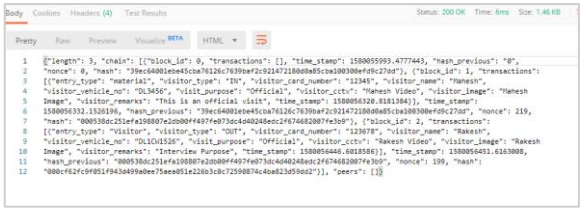

Fig 8: Blockchain displayed in REST-API

Here the copy of the chain is maintained among multiple nodes to maintain the blockchain. Once a block is approved and to be added to the chain, the nodes update the chain with the new block. Here full nodes are used to maintain the consistency of the blockchain. Some full nodes are used over the cloud tested with Azure instances as well as AWS instances. Some full nodes are used on premise for blockchain consistency. The decentralized application can be used over the cloud as well as on premise. The decentralized application will have a choice to connect over the LAN or internet. Once internet is chosen it will verify with the cloud full nodes or if selected over the LAN, it will connect over on premise full nodes. All full nodes and cloud nodes are synced among themselves. Any authorized devices can be used to register with the blockchain framework.

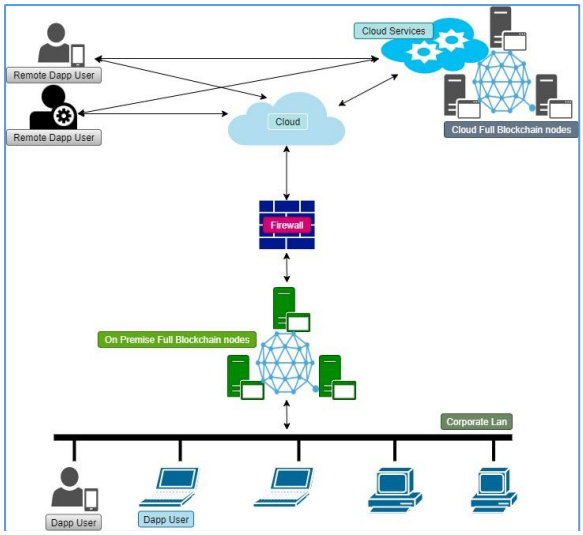

Fig 9: Hybrid blockchain diagram

8. Experiment

The developed framework implementation experiment has been done in 10 organizations with different line of business and with a sample size of 100 information executives, CTO, IT Managers and end users. In this experiment various industries like manufacturing, IT consulting, ISP's, software development, consulting, construction and universities were approached. Blockchain transactions are divided into 4 broad categories like sales call, support call, financial transactions and evaluation transactions. The experiment first started with requirement analysis of putting data in blockchain after analyzing the industry type and transactions related to it. Specific transaction category where fraudulent seems to be maximum were selected. Financial transactions can be changed, modified or deleted for financial gains. Similarly, sales call in any organization are very crucial which too is vulnerable and can be hacked, changed or modified. Support call data is the backbone of a service industry, which can be edited/deleted for portraying a better SLA or a better service capability to its clients missing crucial information which client has the right to know. Holistically, the framework and the architecture were designed for SME while experimenting and installing the framework based upon the requirement. The experiment of framework is divided in three categories namely cloud, hybrid and on premise models. The cloud architecture uses known cloud infrastructure as service platforms like Azure, AWS or Google cloud. On-premise on the other hand is purely installable on local servers and devices in offices. While Hybrid is combination of cloud and on premise architecture. The experimented framework is easy to install without any hassle and OS independent. Apart from this is a cost effective where one does not need to subscribe to cloud for "Blockchain as a service" or install costly computing servers and can run a secured blockchain platform within the organization without any cost and expensive licenses or subscription.

For cloud-based installation, the required decentralized app is installed on devices, systems and cloud servers where the same can be accessed and the continuity of the chain remains permanent. Some of the systems in the cloud contains full copy of the chain. Users can view and add transactions irrespective of locations, which is secure. In case of on premise, installations are done on local systems and servers can be accessed locally from office network. In hybrid blockchain, the framework is installed on cloud servers as well on premise. End users can perform transaction locally or on cloud. The transactions are compared against existing traditional approach industry is following. Samples of hundred executives across ten organization tested the blockchain framework, compared against their existing 2-tier, 3-tier, n-tier, and centralized model. Parameters like security features, foresee benefits, cost-benefit, transparency, execution time and manageability are evaluated.

9. Result and Analysis

The experiment result of the designed framework shows exponential difference on various parameters experimented against the existing traditional approach with the hybrid blockchain framework. Not only it has tended to solve the problem statements but also has an acceptance on the same experimented. Analysis of variance (ANOVA) is used for statistical analysis between the comparative groups to find out that if there are any statistical significant difference.

In this analysis, null hypothesis (H_0) is considered true when there are no significant differences between the parameters of developed hybrid framework method and traditional approach method whereas alternate hypothesis (H_1) is considered true with significant difference between the parameters of

developed hybrid framework method and traditional approach method. Factors like security features, foresee benefits, cost/benefit, transparency and manageability had a significant difference except a factor "execution time" where the null hypothesis holds true and is not rejected.

A. 100% of the samples size accepts that the cross blockchain framework has better security features as compared to the traditional approach.

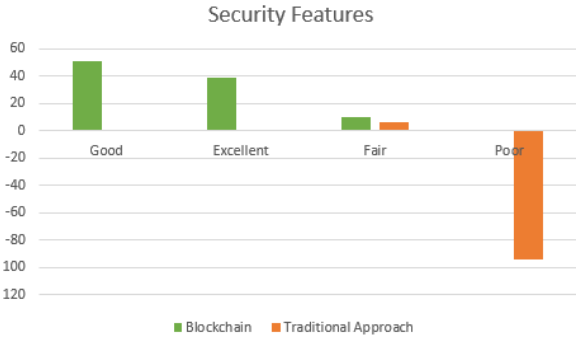

Fig 10: Comparative graph on Security features

ANOVA analysis based on result for security features shows F > F Crit and P < 0.05 where the significance level is 0.05. This analysis shows the result has significant difference and null hypothesis (H_0) is rejected and result holds true for alternate hypothesis (H_1).

Fig 11: F distribution on Security features

Null hypothesis
Null Hypothesis is rejected to the fact that p-value<α while the difference of means is high between the two groups and shows the result is significant statistically.

p value
p value equals 0.00000, [$p(x \leq F) = 1.000000$] means probability of type1 error is small and stronger it supports alternate hypothesis.

Statistics
F = 1064.931432 doesn't fall in the accepted range of critical value [-∞: 3.8889]

Effect size
The effect size f is large which shows the scale difference is high between the means. $\eta 2 = 0.84$ means that the group explains 84.3% of the variance from the mean.

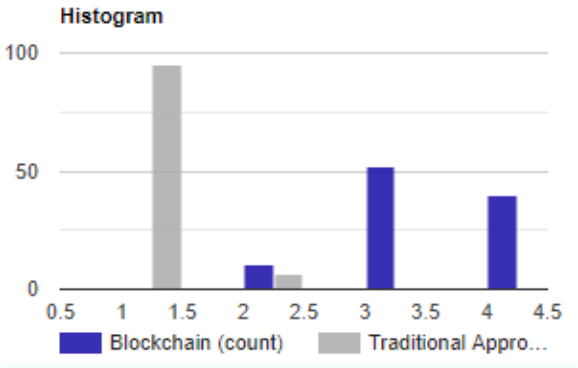

Fig 12: Histogram on Security Features

B. Majority of the sample size foresee benefits in adopting the hybrid blockchain framework as compared to the traditional model.

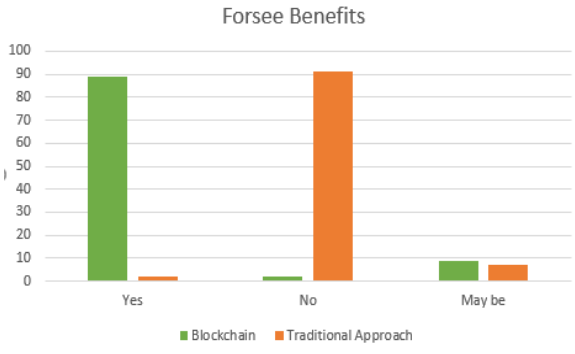

Fig 13: Comparative graph on Foresee benefit features

Statistical analysis based on result for foresee benefits shows F > F crit and P < 0.05 where the significance level is 0.05. This analysis shows the result has significant difference and null hypothesis (H_0) is rejected and result holds true for alternate hypothesis (H_1).

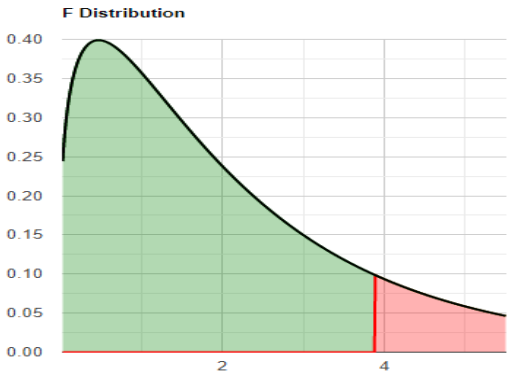

Fig 14: F distribution on Foresee benefit features

Null hypothesis
Null Hypothesis is rejected to the fact that p-value<α while the difference of means is high between the two groups and shows the result is significant statistically

p value
p value equals 2.22045e-16, [p(x ≤ F) = 1.00000] means probability of type1 error is small and stronger it supports alternate hypothesis.

Statistics
F = 1053.822238, doesn't fall in the accepted range of critical value [-∞: 3.8889]

Effect size
The effect size f is large which shows the scale difference is high between the means. η2 = 0.84 means that the group explains 84.3% of the variance from the mean.

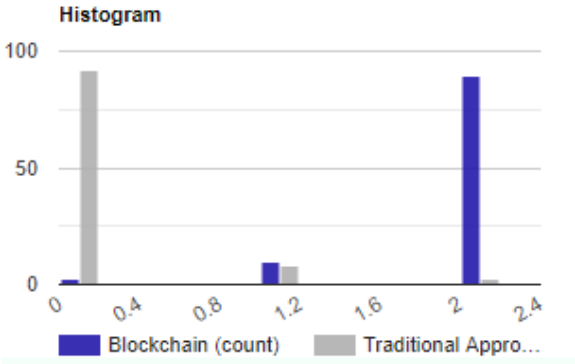

Fig 15: Histogram on Foresee benefits

C. Majority of the sample size finds positive for cost/benefit adopting the hybrid blockchain framework as compared to the traditional model.

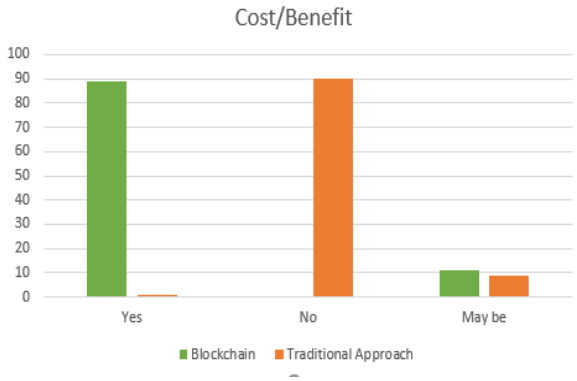

Fig 16: Comparative graph on cost/benefit features

ANOVA analysis based on result for cost benefits shows F > F crit and P < 0.05 where the significance level is 0.05. This analysis shows the result has significant difference and null hypothesis (H_0) is rejected and result holds true for alternate hypothesis (H_1).

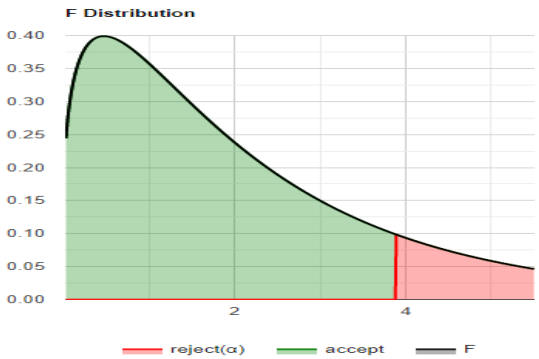

Fig 17: F distribution on Cost/benefit analysis

Null hypothesis
Null Hypothesis is rejected to the fact that p-value<α while the difference of means is high between the two groups and shows the result is significant statistically

p value
p value equals 2.22045e-16, [p(x ≤ F) = 1.00000] means probability of type1 error is small and stronger it supports alternate hypothesis.

Statistics
F = 1453.527084, doesn't fall in the accepted range of critical value [-∞: 3.8889]

Effect size
The effect size f is large which shows the scale difference is high between the means. η2 = 0.88 means that the group explains 88.0% of the variance from the mean.

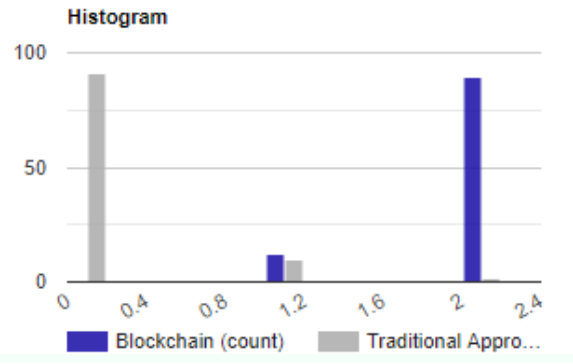

Fig 18: Histogram on Cost/benefit analysis

D. 100% of the samples size accepts that the hybrid blockchain framework has better transparency features as compared to the traditional approach.

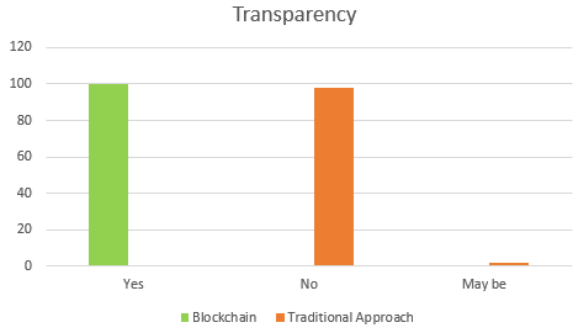

Fig 19: Comparative graph on transparency features

ANOVA analysis based on result for transparency shows F > F crit and P < 0.05 where the significance level is 0.05. This analysis shows the result has significant difference and null hypothesis (H_0) is rejected and result holds true for alternate hypothesis (H_1).

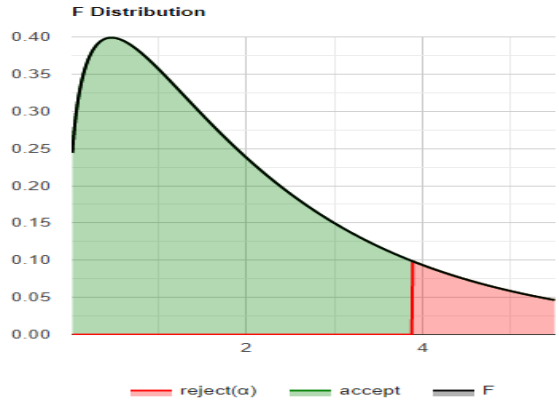

Fig 20: F distribution on transparency analysis

Null hypothesis
Null Hypothesis is rejected to the fact that p-value<α while the difference of means is high between the two groups and shows the result is significant statistically

p value
p value equals 1.11022e-16, [p(x ≤ F) = 1.00000] means probability of type1 error is small and stronger it supports alternate hypothesis.

Statistics
F = 19802.10320, doesn't fall in the accepted range of critical value [-∞: 3.8889]

Effect size
The effect size f is large which shows the scale difference is high between the means. η2 = 0.99 means that the group explains 99.0% of the variance from the mean.

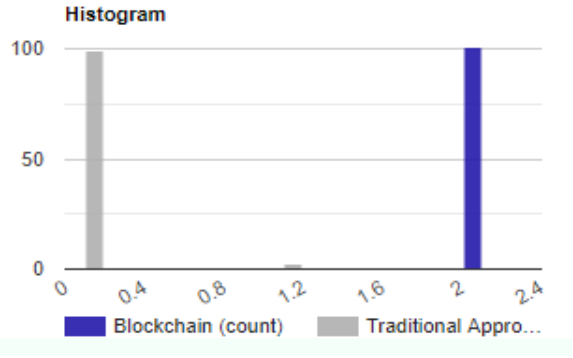

Fig 21: Histogram on Transparency analysis

E. Majority of the samples size accepts that execution time has no major difference between the blockchain framework as compared to the traditional approach.

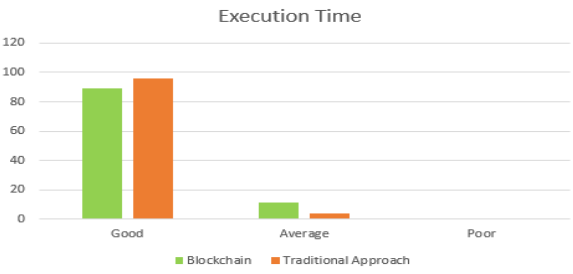

Fig 22: Comparative graph on execution time

ANOVA analysis based on result for execution time shows F < F crit and P > 0.05 where the significance level is 0.05. This analysis shows

the result has No significant difference and alternate hypothesis (H_1) is rejected and result holds true for null hypothesis (H_0).

Fig 23: F distribution on execution time

Null hypothesis
Null Hypothesis is accepted to the fact that p-value>α while the difference of means is less between the two groups and shows the result is not significant statistically

p value
p value equals 0.0606847, [p(x ≤ F) = 0.939315] means probability of type1 error is very high and stronger it supports null hypothesis.

Statistics
F = 3.559065, doesn't fall in the accepted range of critical value [-∞: 3.8889]

Effect size
The effect size f is small which shows the scale difference is low between the means. η2 = 0.018 means that the group explains 1.8% of the variance from the mean.

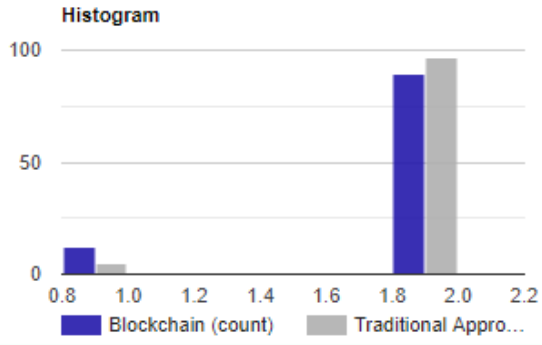

Fig 24: Histogram on execution time

F. Majority of the sample size accepts the blockchain framework has good manageability as compared to the traditional model.

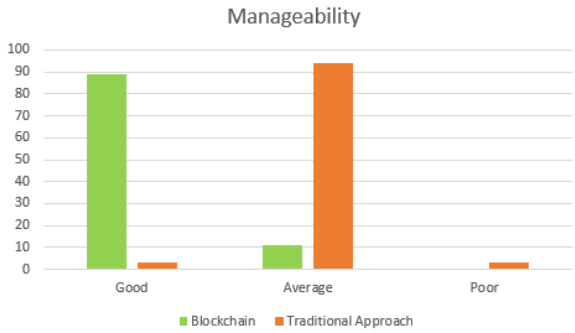

Fig 25: Comparative graph on manageability features

ANOVA analysis based on result for manageability shows F > F crit and P < 0.05 where the significance level is 0.05. This analysis shows the result has significant difference and null hypothesis (H_0) is rejected and result holds true for alternate hypothesis (H_1).

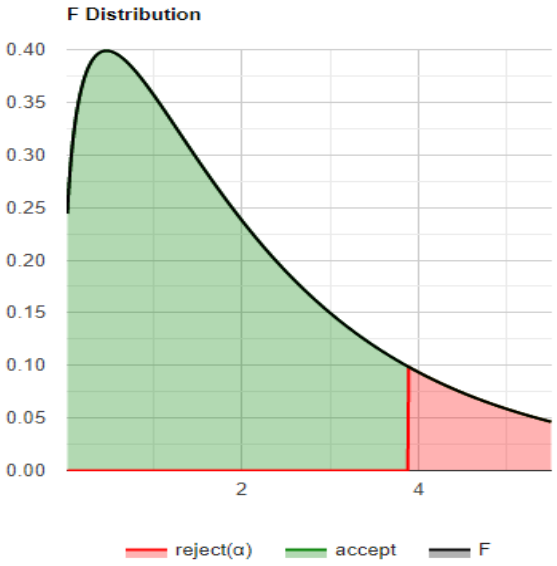

Fig 26: F distribution on manageability features

Null hypothesis
Null Hypothesis is rejected to the fact that p-value<α while the difference of means is high between the two groups and shows the result is significant statistically

p value
p value equals 1.11022e-16, [p(x ≤ F) = 1.00000] means probability of type1 error is small and stronger it supports alternate hypothesis.

Statistics
F = 496.630192, doesn't fall in the accepted range of critical value [-∞: 3.8889]

Effect size
The effect size f is large which shows the scale difference is high between the means. η2 = 0.71 means that the group explains 71.5% of the variance from the mean.

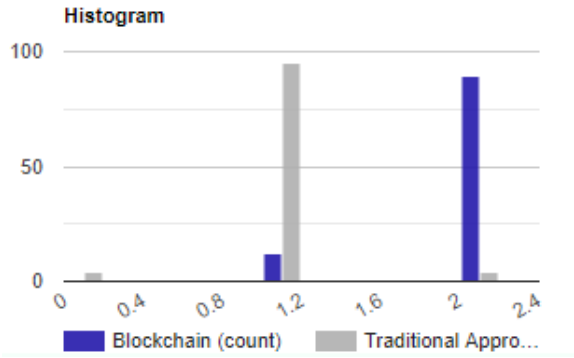

Fig 27: Histogram on manageability features

G. Majority of the sample size can consider the blockchain framework as permanent for adoption. This is the most significant result achieved after the experiment where the table shows that 89% of sample are ready to consider the framework as permanent.

Consider permanent	
Yes	89
No	0
May be	11

Table1: Acceptance table

10. Conclusion

As blockchain now no longer the universe of cryptocurrencies and there is a gradual increase in proposition of its usage in each anteroom of business. This will take the middle stage in coming years in various line of business like governments, healthcare, supply chain, legal and it is constantly evolving [8]. Some organizations has started using blockchain and blockchain as a service. This research paper has experimented the hybrid blockchain framework in different industries where it found a positive feedback on various scaling factors and consider for permanent usage as a superior alternative to client server approach model. The problem statement satisfies issues like data security breach, modification, deletion, transparency, high maintenance, subscription, license cost and hacking attacks, which are major challenges today. This paper highlights the usefulness and contribution of hybrid blockchain framework as a secured, cost effective alternate to client server approach model which can be implemented in various small and medium scale industries with ease. The framework is light weighted and has fast execution process. The energy consumption is less comparatively due to no blockchain mining process. However there are some factors which needs to be taken care and can be alluded for future study like performance issues may arise especially when data grows along with users, which may be solved by sharding. The framework can be incorporated with an Artificial Intelligence handler to monitor the security of the blockchain network.

Acknowledgements

My sincere thanks to my professor and guide who has supported me enormously for accomplishing.

References

[1] Xu, X., Lu, Q., Liu, Y., Zhu, L., Yao, H., & Vasilakos, A. V. (2018). Designing Blockchain-based applications a case study for imported product traceability. *Future Generation Computer Systems*. doi:10.1016/j.future.2018.10.010.

[2] P. Fraga-Lamas and T. M. Fernández-Caramés, "A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry," in *IEEE Access*, vol. 7, pp. 17578-17598, 2019. doi: 10.1109/ACCESS.2019.2895302

[3] Dujak, D., & Sajter, D. (2018). Blockchain Applications in Supply Chain. *Eco Production*, 21–46.doi:10.1007/978-3-319-91668-2_2

[4] Siyal, A., Junejo, A., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography*, 3(1), 3.doi:10.3390/cryptography3010003

[5] Lavazova, Olga and Dehling, Tobias and Sunyaev, Ali, From Hype to Reality: A Taxonomy of Blockchain Applications (2018). *Proceedings of the 52nd Hawaii International Conference on System Sciences* (HICSS 2019), January 8-11, 2019, Wailea, Maui, HI, USA.

[6] Cao, Y. (2019). Energy Internet Blockchain technology. *The Energy Internet*, 45–64. doi:10.1016/b978-0-08-102207-8.00003-5

[7] Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where Is Current Research on Blockchain Technology? —A Systematic Review. *PLoS ONE* 11(10): e0163477https://doi.org/10.1371/journal.pone.0163477

[8] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels and B. Amaba, "Blockchain technology innovations," *2017 IEEE Technology & Engineering Management Conference (TEMSCON),* Santa Clara, CA, 2017, pp. 137-141.

[9] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Sydney, NSW, 2016, pp. 1392-1393.

[10] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," in *IEEE Access*, vol. 6, pp. 10179-10188, 2018.

[11] Dmitry Efanov, Pavel Roschin,The All Pervasiveness of the Blockchain Technology, *Procedia Computer Science*, Volume 123,2018,Pages 116-121,ISSN18770509,https://doi.org/10.1016/j.procs.2018.01.019.

[12] Miraz, Mahdi H., and Maaruf Ali. "Applications of Blockchain Technology Beyond Cryptocurrency." *Annals of Emerging Technologies in Computing* 2.1 (2018): 1–6. Crossref. Web.

[13] D. Vujičić, D. Jagodić and S. Ranđić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo, 2018, pp. 1-6.

[14] Dutta, Saugata, and Kavita Saini. "Blockchain and Social Media." Blockchain Technology and Applications. *Auerbach Publications*, 2020. 101-114.

[15] Dutta, Saugata., & Kavita. (2019). Evolution of blockchain technology in business applications: *Journal of emerging technologies and innovative research*, May, 2019, Vol 6, issue 5, pp. 240-244

[16] Kumari, Kavita, and Kavita Saini. "CFDD (CounterFeit Drug Detection) using Blockchain in the Pharmaceutical Industry."

[17] Saini, Kavita. "A Future's Dominant Technology Blockchain: Digital Transformation." *2018 International Conference on Computing, Power and Communication Technologies (GUCON). IEEE*, 2018.

[18] Saini, Kavita, et al. "E2EE for Data Security for Hybrid Cloud Services: A Novel Approach." *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). IEEE*, 2018