**Literature Study**

In the present system of outlet database maintenance, usage of a central database would lead to various implications. One highlighting issue of concern is if the centre goes down then that can bring an entire company down in the event of a server crash. Companies spend hundreds of thousands or millions of dollars each year to prevent that and provide for redundant systems to prevent that -- often at a cost that reduces or eliminates the cost effectiveness. In other words, one would need to have offsite redundant servers to use the substitute database as primary database. As organisations often underestimate the demands on database server hence the performance of the database behaves as a severe bottleneck. Further, huge amount of investment is needed to setup the required hardware and the software’s needed to run the complex database applications.  If one part of the database is corrupted or damaged because of the hardware or software failure, since we don’t have many versions of the file, all the application programs which are dependent on this database are implicitly affected.  Extensive conversion costs in moving form a file-based system to a database system If you are currently working on file based system and need to upgrade it to database system, then large amount of cost is incurred in purchasing different tools, adopting different techniques as per the requirement. Large amount of human efforts, the time and cost is needed to train the end users and application programmers in order to get used to the database systems.

On the contrary, blockchain are not vulnerable to single point failure. It uses cryptographic hashes for its network. The security aspect of blockchain has been proven by large scale usage and public deployment of Bitcoin and public Ethereum. Along with this, the maintenance service costs are much lower in Blockchain oriented systems as compared to traditional database oriented systems. Additional advantages due to distributed nature of Blockchain are included below:

1) Scaling of system is easy that is you can add new members without complication in algorithm design and bandwidth consumption.  
2) Failing of an agent would not result in the failure of the system.  
3) Adaptability to environment would be better.  
4) Less memory and processing power for individual agents.  
5) Better options for exception handling.

There are several papers that have explored the likelihood of using smart contracts, licensing, Internet of Things, and smart properties under the umbrella of the Blockchain domain.

Paper [1] answers one of the most basic question: “What is blockchain?” BlockChain is a public ledger having record of all transactions and distributed among network participants where every transactions before being added to the ledger is being verified by the other participants according to the majority consensus mechanism. This records cannot be changed or edited once added to the ledger.

Advantages of using blockchain include following features: Data Security: Since data is shared among all the participants of the network, if in any unfortunate case data is lost, it can be recovered using other participant’s data. Transparency: Everyone has the access to all the history transactions. Decentralization: There is no place for the central authority to control the network.

Disadvantages of using blockchain include High power computation. Mining require expensive hardware. Only one miner wins others resources are wasted. Data replication requires space. Local copies of all transaction are stored on each network node. Adding new information are very slow. Transparency may affect the privacy of the user.

One should use blockchain when there is a requirement for (i) Shared database. (ii) Many writer nodes. (iii) To see the connection between the transactions.

Since the number of users of cloud-based services have used, problems regarding the security and copyright aspects has increased. Most effective way to secure is to encrypt the data before uploading those, which is recommended by the Cloud Security Alliance. There are certain difficulties in imposing the encryption and accessing the data to use them. Some of the tools to encrypt files before sending them to the cloud is BoxCrypt, CryptDB, ARX. To ensure the data integrity and non-repudiation on the distributed cloud system is BigChainDB. One way is to introduce the decentralized scheme to control the access to encrypted data. Mate Horvath proposed in a multi-authority CP-ABE scheme for effective revocation of user’s attributes based on their identities. Most of the functions are performed on the client side because exchanging of the data are mostly private. Remaining functions are performed using the smart contracts in the Ethereum Virtual Machine. Benefits of using the access control system is that it provides the ability to change the accessing policy for the encrypted data without duplicating it; integrity of information about the transactions which includes the granting and changing the access and many more. The entire concept discussed in this paragraph can be vividly studied in paper [2].

Use of blockchain in the field of healthcare to maintain a health ledger, which have all the data of the patients from physician to get the patient’s pertinent medical information, which can be used in future. But challenge here is to get all the data from all physician because a person may consult to many doctors from different for different problems. Blockchain can be useful in the other aspects of healthcare such as insurance claims and other administrative problems of estimating health related population data. Any data once added to blockchaincannot be changed or deleted, property of blockchain, ensure that the data are correct and changed. Mari Greenberger, director of informatics in HIMSS, North America believes that blockchain have immense potential that can help with critical components. HIMSS has started to work in blockchain to dig out the best features of blockchain that can be proved very useful in the field of healthcare. They stated the problems in using blockchain for healthcare is that hesitation to use new technology , privacy and security concerns. Carter of the blockchain research institute says that “*Better outcomes are derived from better data*” and right now if we create blockchain to create commons and individual control their data and other healthcare bodies are allowed to access them, it will help them in long run. Paper [3] provides a detailed study on the above discussed content.

According to the Taiwan Ministry of Education statistics, many students travel to other countries for further studies or change states due to several reasons or due to some work requirements. Due to unavailability of any anti forging methods, there have many cases which have seen forged certificates cases. To counter this problem, blockchain can be used to create digital certificate. By the property of non-modification, digital certificate having anti-counterfeit and verifiability can be made. Procedure of creating the digital certificate is , generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries. Paper [4] quite illustratively explains this notion.

Paper [5] presents a research article on the present state of research and development in blockchain technology. The major usage of blockchain is seen in bitcoins- a popular digital payment system. Every block in the bitcoin is of the size of 1 MB. Hence each block can roughly store approximately 500 records of transactions. With each block piling over the other makes it even more difficult to alter the blocks and also gives a certain degree of confirmation. In general, greater the confirmation greater is the security of the blocks. The blockchain implementation in bitcoin technology majorly experiences challenges in throughput, latency, security, size and bandwidth. In the current scenario the length of the blockchain in the bitcoin can extend up to 50,000 MB which clearly indicates the necessity of expanding this capacity to incorporate larger chains of growing list of records with increase in number of users and transaction frequencies that can match the order of frequencies in VISA and twitter.

The development of distributed ledger technology that is, blockchain has led to the emergence of essential operations in clearance and business in the wholesale markets. The responsibility of banking establishments being mediators in making purchases and settling customer bills can be minimised to zero using the blockchain technology potentially decreasing waiting time of huge transactions from days to minutes. The ease of the process of transferring digital currency like Bitcoin and transparency in record maintenance is facilitated by means of peer –to-peer network, cryptography and distributed data storage[6].

There are numerous advantages of applying blockchain to market investments. The efficient transfer and administration of transaction details between the seller and the buyer is quite simple and safe with the blockchain technology. However there are issues related to reliability and isolated utilization of blockchain technology. Some major concerns pertaining to blockchain are 51% attack, latency of the network and network bandwidth. The solutions corresponding to such problems have been effectively discovered and enlisted [7].

The blockchain can be employed to provide solutions to problems pertaining to domains that may seem totally irrelevant. Some these domains could include services in government sector, businesses, secure authentication and validation.Decentralised applications called ‘DApps’ can run ob both client side and on the blockchain. There are various crypto currencies like ethereum, bitcoin, journalcoin, learncoin, healthcoin and many more whose distinct characteristics and forte is presented in paper [8].

Bitcoin mining is truly essential to improve security of the transactions. As the number of bitcoin miners increases the difficulty of the math problem to be solved also increases. There are various methods of performing Bitcoin mining. The significant operations of SHA-256(Secure Hash Algorith-256) hashing of values to convert the input data into a safe and secure fingerprint of that data has been effectively elaborated in the paper [9].

There is an intensive wastage of resources when it comes to the usage of blockchain especially the process involving the mining of the blockchain. Blockchain mining wastes a lot of energy. Mining in blockchain is prone to the very famous 51% attack which can easily happen in smaller blockchains. The idea behind the acceptance of a particular blockchain from the different versions of the blockchain is choosing the chain of longest length. This means that for a malicious miner to take advantage of double spending must have a computation power greater than most of the miners in the blockchain so that it can add more blocks than the other true miners and hence get the false blockchain into acceptance by the other miners as soon as length of blockchain created by the miner is greater than the length of the original blockchain. Considering the fact that there are thousands of miners available on the blockchain, a malicious miner would have to spend enormous amounts of money on mining hardware to compete with the rest of the network. Even the strongest computers on earth are not directly competitive with the total computational power on this network. Thus the size of the network plays a key factor in preventing 51% attack. Faster throughput and lesser latency are what the blockchain technology demands for its efficient functioning. There are certain challenges regarding the scalability of the blockchain that also needs to be dealt with [10].

Blockchain also suffers from multiple broadcasting of the same transaction over the network. Each transaction is first verified before adding into the block. So prior to the verification every transaction is a part of the unverified pool of transactions. In order to avoid redundancy in the blocks a protocol called first-leader-then-block consensus protocol is used. This proposal reduces the communication cost by almost 97% as compared to the real communication standards which are in effect today. The paper [11] exclusively discusses on the rewarding or the incentive mechanisms adopted for transaction fee propagation which is independent of the network topology. The various concepts highlighted here are I-connected networks, Eclipse and partitioning, propagation lemma and the equity lemma.

Paper [12] describes the solution to achieve scale-out throughput maintaining an equivalent level of decentralisation and security. Namely, there are three conditions to be met for any consensus protocol to work effectively. They are correctness, consistency and liveness. It explains the features of value-transfers in blockchain. The solution comprises of key concepts like Communication cost Per Transaction and spontaneous Sharding. A blockchain is partitioned into various shards on the basis of the domain. Sharding is of two types: local and global shards. A transaction that can be completed in a single shard is referred to as a local shard and the transaction that is completed using two shards is known as a global shard. There are two types of consensus algorithms Nakamoto consensus algorithms and byzantine fault tolerance (BFT). The Practical Byzantine Fault Tolerance (PBFT) algorithm is implemented with a message complexity of O(n2). Each transaction pattern is divided into shards so as to reduce the size of proof in every transaction.

Blockchain is a decentralized ledger used to securely exchange digital currency, perform deals and transactions. Each member of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction. Blockchain ledger is a collection of all Bitcoin transactions executed in the past. Basically, it’s a distributed database which maintains a continuously growing tamper proof data structure blocks which holds batches of individual transactions. The completed blocks are added in a linear and chronological order. Each block contains a timestamp and information link which points to a previous block. Bitcoin is peer-to-peer permission-less network which allows every user to connect to the network and send new transaction to verify and create new blocks [13].

Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA) cryptographic algorithm to make sure only rightful owners have the access to funds .When Bitcoin is sent, it creates a transaction message and attaches new owner's public ECDSA key. Each Bitcoin is associated with public ECDSA key of its current owner. A new transaction is broadcasted over Bitcoin network to inform everyone that new owner of these coins is the owner of the new key.

The significant advantage of blockchain is the method of transactions which are verified and traceable. Instead of having a trusted third-party or a central bank, the technology is based on consensus among a peer-to-peer network of computers that run on complex algorithms. Instead of storing in one database, time-stamped transactions in blocks are stored in different systems across a value chain. This helps in achieving a decentralization of trust which has helped realizing cross-border payments, trading and faster settlements in a reliable and cost efficient way.

The blocks of data are stored in linear chain. The blocks that contain data are cryptographically hashed. The hashed blocks are dependent on previous blocks so as to prevent tampering of data in blockchain. Distributed Ledger is a peer-to-peer network prevents modification of ordered series of records that have been stamped by using a defined consensus mechanism. It is built upon a series of networks of databases where participants can create, separate and keep information in an efficient and secure manner [14].

Several research papers have been published analysing the security of blockchain. Paper [15] is one such paper which ensures integrity, authenticity, immutability and credibility of data in a data-sharing communication software-development oriented platform. It addresses the challenge of data leakage and how it can be effectively detected and resolved by adopting a distributed storage approach. What makes blockchain so impressive is that it allows controlling and tracking of data for sharing purposes among different levels of security domains. It allows non-repudiation of data. The data can be stored in an asymmetrically encrypted form with an only the fly generated key based on the available resources, software bundle and authentication codes. The data can be shared and accessed by following a control policy as governed by the smart contract.

Paper [16] analyses the suitability of blockchain in building a smart city. The blockchain is mainly categorised into 3 classes: Blcockahin 1.0, Blockchain 2.0, Blockchain 3.0. Blockchain 1.0 deals with cryptographic currency like the bitcoin. Blockchain 2.0 delas with financial settlements like equities, debt, insurance, smart contracts, etc. Blockchain 3.0 deals with the making of a decentralised cooperative society in terms of health, science, culture and arts. Big Data is the heart of the Smart City implementation. Hence privacy and security of information is a serious threat to be acknowledged.

Blockchains allow us to have a distributed peer-to-peer network where non-trusting members can interact with each other without a trusted intermediary, blockchain-IoT combination facilitates the sharing of services and resources which forms a connection between different devices, and we can verify using different cryptography technique. Blockchain enables trust less network i.e. the parties can transit even though they don’t trust each other, as there is no trust issue between the parties which means that the interaction between the two parties will be much faster. This functionality of blockchain is very useful for researchers and developers who are working in hot domain as it is secure and fast to obtain data.

All the IoT devices of a manufacturer operate on the same blockchain network. The manufacturer deploys a smart contract that allows them to store the hash of the latest firmware update on the network .The devices either ship with the smart contract’s address baked into their blockchain client, or they find out about it via a discovery service. They can then query the contract, find out about the new firmware, and request it by its hash via a distributed peer to peer file system [17].

In the original design, Bitcoin’s blockchain stores coins as the system states. For this application, Bitcoin nodes implement a simple replicated state machine model which moves coins from one address to another. Since then, block-chain has grown beyond crypto-currencies to support user-defined states and Turing complete state machine models.For example, Ethereum  enables any decentralized, replicated applications known as smart contracts.

The blockchain can be classified as public blockchain and private blockchain.

Public blockchain:

Bitcoin is the most well known example of public block-chains. In Bitcoin the states are digital coins (crypto-currencies), and a transaction moves coins from one set of addresses to another. Each node broadcasts a set of transactions it wants to perform. Special nodes called miners collect transactions into blocks, check for their validity, and start a consensus protocol to append the blocks onto the blockchain. Bitcoin uses proof-of-work (PoW) for consensus, only a miner which has successfully solved a computationally hard function can append to the blockchain. Bitcoin transaction speed remains very low as it takes high computation to validate the block it is nearly 7 transactions per second.

Private blockchain:

Hyperledger  is among the most popular private blockchains.Three phase protocol is used in this blockchain to validate the transaction.In the pre-prepare phase, a leader broadcast a value to be commit by other nodes. Next, in the prepare phase, the nodes broadcast the values they are about to commit. Finally, the commit phase confirms the committed value when more than two third of the nodes agree in the previous phase [18].

References

1. Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda, Víctor Santamaría , “ To Blockchain or Not to Blockchain: That Is the Question”, IEEE Computer Society On March/April 2018
2. Ilya Sukhodolskiy, Sergey Zapechnikov, “A Blockchain-Based Access Control System for Cloud Storage”, IEEE Computer Society On 2018 Issue No. :978-1-5386-4340-2/18
3. Leslie Mertz, “(Block) Chain Reaction”, IEEE Pulse Issue No.2154-2287, 15 May 2018
4. Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen, “ Blockchain and Smart Contract for Digital Certificate”**,** IEEE International Conference on Applied System Innovation2018, Issue No. :978-1-5386-4342-6
5. Where is current reearch in bockchain Technology?-A systematic Review(Jesse Yli Hummo,Deokyoon Ko, Sujin Choi, Kari smolander)
6. Lael Brainard:”The Use Of Distributed Ledger Technologies in Payment, Clearing and Settlement, Board Of Governors Of The Federal Reserve System at Institute Of International Finance Blockchain Roundtable, Washington D.C. in April 14, 2016
7. Harry Halpin and Marta Piekarska: Introduction to Security and Privacy on the Blockchain, 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)
8. Ujan Mukhopadhyay, Anthony Skjellum, Oluwekemi Hambolu, Jon Oakley, Lu Yu and Richard Brooks: A Brief Survey of Cryptocurrency Systems, available at: http://ieeexplore.ieee.org/ iel7/7899233/7906913/07906988.pdf
9. Swan M. Blockchain: Blueprint for a New Economy. “O’Reilly Media, Inc.”;2015
10. “Bitcoin mining acceleration and performance quantification”, Published in: Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on 4-7 May 2014, INSPEC Accession Number:14599397
11. O˘guzhan Ersoy, Zhijie Ren, Zekeriya Erkin and Reginald L. Lagendijk ,”Transaction Propagation on Permissionless Blockchains: Incentive and Routing Mechanisms”-2018 Crypto Valley Conference on Blockchain Technology
12. Zhijie Ren, Kelong Cong, Taico V. Aerts, Bart. A.P. de Jonge, Alejandro F. Morais and Zekeriya Erkin, ”A Scale-out Blockchain for Value Transfer with Spontaneous Sharding”, 978-1-5386-7204-4/18 IEEE
13. Sachchidanand Singh, Nirmala Singh,” Blockchain: Future of Financial and Cyber Security”,2016 2nd International Conference on Contemporary Computing and Informatics (ic3i)
14. Arpita Nayak, Kaustubh Dutta, “Blockchain: The Perfect Data Protection Tool”, 2017 International Conference on Intelligent Computing and Control (I2C2)
15. Miguel Villarreal-Vasque, Denis Ulybyshe, Bharat Bhargava, Ganapathy Mani, Jason Kobes Northrop Grumman, Paul Conoval, Robert Pike, Steve Seaberg, “ ‘Blockhub’: Blockchain-based Software Development System for Untrusted Environments”, 2018 IEEE 11th International Conference on Cloud Computing, 2159-6190/18
16. Li Shuling , “Application of Blockchain Technology in Smart City Infrastructure”, 2018 IEEE International Conference on Smart Internet of Things, 978-1-5386-8543-3
17. Konstantinos Christidis, Michael Devetsikiotis, K. Christidis, “Blockchains and Smart Contracts for the Internet of Things “
18. Tien Tuan Anh Dinh , Rui Liu, Meihui Zhang , Gang Chen, Beng Chin Ooi, and Ji Wang, ”Untangling Blockchain: A Data Processing View of Blockchain Systems”