**IS 651 PROJECT REPORT ON BLOCKCHAIN**

****

**By**

**-Kamlesh Pai**

**-Siddhesh Sawant**

**-Neelesh Suryawanshi**

**-Sulabh Sharma**

**INTRODUCTION**

Bitcoin is an electronic cash form of cryptocurrency. It is a distributed digital currency which can be sent from the user to user on the peer-to-peer Bitcoin blockchain network without the need for intermediaries without a central bank or single administrator. In a relatively short time, bitcoin has come long way. Companies around the world accept their currency from REEDS Jewelers, a big jewelry chain in the USA, to a private hospital in Warsaw, Poland. Worth of Billions dollars businesses are also doing business in bitcoin like Dell, Expedia, PayPal and Microsoft. It is supported by blogs, publications such as Bitcoin Magazine publish their articles, forums discuss different cryptocurrencies and exchange their coins. It has a application programming interface (API), price index and exchange rate.

Many people are dubbing Libra the "Bitcoin killer" in the mainstream press, mistaking the role Libra has in the ecosystem. Libra is a stable currency and is currently centralized with no protection around its codebase and for like 10-year there is no resistance history. Whereas Ethereum is an asset for speculation. As the network's value increases, so does the price of the underlying asset. In addition, Libra has been backed by "real assets" that sounds great to a mainstream people, but this is a bug and not a feature real world assets will require real world auditors. In other words, "real assets" are a chain of holes in security. Bitcoin is the native property of its public blockchain that can be audited at very low cost by anyone in the world or there will be no cost unless you are willing to trust any of the thousands of nodes that are already performing such audits. In this way, Ethereum is close to Bitcoin, and Libra's unexpectedly usurping short-term risk to Ethereum which is also negligible.

The main major difference between Libra and Ethereum is that, unlike Ethereum, Libra is an unregulated blockchain. Everything is more or less equal in Ethereum. Nothing stops you from purchasing a powerful machine and entering the network as a miner, potentially receiving mining fees and taking part in smart contract execution. There are no more powerful groups than others; There seems to be no licensing system dictating who can validate new transactions or deploy new intelligent contracts. Libra will be quite different, at least initially. A team of about 100 founding members (validators) will be chosen. All members will have to be confident and can only validate new transactions. The founding members must run the blockchain in essence. We will only have the requisite permissions to control the blockchain. This is very similar to private blockchains like Hyperledger, which can be used to create a public ledger between parties, so no single node has to be completely trusted.

Hyperledger is a collaborative open source initiative designed to promote cross-industry blockchain technologies. It is a global collaboration coordinated by The Linux Foundation, covering economic, economics, the Internet of Things, supply chains, manufacturing, and technology leaders. Bitcoin or some other cryptocurrency is not funded by Hyperledger. But blockchain technology is thrilling the platform. Now Hyperledger has an impressive list of over 100 leaders. The list covers a wide range of well-known executives in the industry. This includes mobile technology giants such as Airbus and Daimler, This firms such as IBM, Fujitsu, SAP, Huawei, Nokia, Intel and Samsung, financial institutions Including Deutsche Börse, American Express, J.P. Morgan, BBVA, BNP Paribas and Well Fargo, and Blockchain start-ups such as Blockstream, Netki, Lykke, Factom, Bloq and Consensys. Many of the world's largest It and Finance companies are working with some of the biggest blockchain start-ups at Hyperledger.

**Review**

1. **Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains.**

<https://arxiv.org/pdf/1801.10228.pdf>

**Understanding**:Hyperledger is an open source community oriented exertion made to propel cross-industry blockchain technologies.Hyperledger Fabric is a particular blockchain system which goes about as an establishment for creating blockchain-based items, arrangements and applications utilizing attachment and-play segments that are gone for use inside the private undertakings. This paper portrays Fabric, its engineering, the basis be-rear different plan choices, its most conspicuous usage angles, just as its conveyed application programming model. All past blockchain frameworks, permissioned or not, pursue the request execute engineering. This implies the blockchain system orders exchanges first, utilizing an agreement convention, and afterward executes them in a similar request on all friends successively.

The client application uses Hyperledger Fabric SDK or REST web service to interact with the Hyperledger Fabric network. Chaincode (similar to Ethereum Smart Contract) installed in peers causes to initiate transaction invocation request. All the peers maintain their one ledger per channel that they are subscribed to.

**Conclusion:**Fabric is a measured and extensible conveyed working framework for running permissioned blockchains. It presents a novel design that isolates exchange execution from accord and empowers arrangement based underwriting and that is suggestive of middleware-imitated databases.

**Future Work:** Future work will address (1) execution by investigating benchmarks and advancements, (2) adaptability to enormous arrangements, (3) consistency certifications and progressively broad information models, (4) other strength ensures through various accord conventions, (5) protection and classification for exchanges and record information through cryptographic methods, and substantially more.

**2. Bitcoin: A Peer-to-Peer Electronic Cash System**

<https://bitcoin.org/bitcoin.pdf>

**Understanding:** Digital signature give some portion of the arrangement, however the primary advantages are lost if a believed outsider is as yet required to forestall twofold spending. We propose an answer for the twofold spending issue utilizing a shared system. The system timestamps exchanges by hashing them into a continuous chain of hash-based confirmation of-work, shaping a record that can't be changed without re-trying the evidence of-work. The longest chain not just fills in as evidence of the grouping of occasions saw, however verification that it originated from the biggest pool of CPU control.

The solution that is proposed in this paper starts with a timestamp server.

1. A timestamp server works by taking a hash of a square of things to be timestamped and broadly distributing the hash, for example, in a paper.

2.The incentive can likewise be supported with exchange expenses. In the event that the yield estimation of an exchange is not as much as its information esteem, the thing that matters is an exchange charge that is added to the motivator estimation of the square containing the exchange. When a foreordained number of coins have entered flow, the motivating force can change totally to exchange charges and be totally expansion free.

3. It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in.This paper proposes a system for electronic transactions without relying on trust.

**Conclusion and Future Work:**The system is vigorous in its unstructured straightforwardness. Hubs work at the same time with little coordination. They should be recognized, since messages are not steered to a specific spot and just should be conveyed on a best exertion premise. Hubs can leave and rejoin the system freely, tolerating the confirmation of-work chain as evidence of what occurred while they were no more.

**3. Libra Blockchain**

<https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf>

**Understanding:** The Libra Blockchain is a decentralized, programmable database expected to help a low-precariousness advanced cash that will have the option to fill in as a beneficial vehicle of exchange for billions of people far and wide. The Libra convention permits a lot of copies — alluded to as validators — from various specialists to together keep up a database of programmable resources.Validators process exchanges and associate with one another to arrive at agreement on the condition of the database. The Libra Blockchain is a cryptographically validated database kept up utilizing the Libra convention. The database stores a record of programmable assets, for example, Libra coins. An asset sticks to custom guidelines indicated by its proclaiming module, which is likewise put away in the database.

This paper discusses the components of the Libra protocol:

1. Logical Data Model describes the logical data model that organizes the decentralized database visible to validators and clients.
2. Executing Transactions describes the use of Move , a new programming language that is used to define and execute database transactions.
3. Authenticated Data Structures and Storage describes the mapping of the logical model into authenticated data structures based on Merkle trees .
4. Byzantine Fault Tolerant Consensus describes the LibraBFT variant of the HotStuff protocol , which allows a network with potentially malicious validators to maintain a single, consistent database by executing transactions with Move and coming to agreement on their execution using the authenticated data structures.
5. Networking describes the protocol that enables validators to communicate with each other securely, as required for consensus.

**Future Work:**This is a proposal for the Libra protocol, which permits a lot of validators to give a decentralized database to following programmable assets. We have examined an open-source model — Libra Core — of the Libra convention and indicated how the presentation of the Move programming language for shrewd agreements enables the protocol to execute the one of a kind plan of the Libra biological system.

**4. Hyperledger Sawtooth: An Introduction**

https://www.hyperledger.org/wpcontent/uploads/2018/01/Hyperledger\_Sawtooth\_WhitePaper.pdf

**Understanding :**The present business forms for data sharing are troubled with go-betweens, wasteful aspects, and security concerns. Using conveyed record innovation (or blockchains), business forms between organizations can be streamlined, and records can be kept in sync without the need for a central authority or manual reconciliation processes. This can help enterprises to decrease their expenses and empower them to make totally better approaches for working together. Sawtooth is a system for building dispersed records for big business use, with an emphasis on measured quality and extensibility. Sawtooth tons of state machine replication inquire about and is intended to help any accord component or 'brilliant agreement' language.

Hyperledger Sawtooth:Hyperledger Sawtooth is an enterprise blockchain platform for building distributed ledger applications and networks. The design philosophy targets keeping ledgers distributed and making smart contracts safe, particularly for enterprise use. Sawtooth intends to keep disseminated records circulated and to make savvy contracts alright for big business use.

Sawtooth architecture compromise has five core components:A peer-to-peer network Nodes on the Sawtooth network communicate by sending messages to each other over TCP.

A distributed log which contains an ordered list of transactions

A state machine / smart contract logic layer for processing the content of those transactions

A distributed state storage for storing the resulting state after processing transactions

A consensus algorithm for achieving consensus across the network on the ordering of transactions and the resulting state

Specialized INNOVATIONS IN SAWTOOTH

Sawtooth contains a few specialized advancements, including:

• Dynamic accord—Going past order time pluggable agreement, this enables a consortium to change accord calculations on a running blockchain basically by giving an exchange.

Proof of slipped by time — An agreement calculation with the versatility of evidence of work yet without the downside of high power utilization.

• Transaction families—A keen agreement deliberation that empowers clients to compose brilliant agreement rationale in the language based on their personal preference.

• Compatibility with Ethereum contracts—Sawtooth highlights like permissioning and un-pluggable agreement empower Ethereum to be designed properly for an endeavor.

• Parallel exchange execution—Most blockchains expect exchanges to be executed in arrangement to ensure predictable requesting at each friend. Sawtooth incorporates a propelled parallel scheduler that parts hinders into parallel streams. Parallelism considers quicker square handling to somewhat address the exhibition downside of blockchains contrasted with customary databases.

• Private exchanges—Clusters of Sawtooth hubs can be effectively sent with discrete permissioning. This gives security and classification among members of that unmistakable chain. No unified help spill exchange designs or other secret data. In any case, a middle person, for example, Hyperledger Quilt is required to associate separate chains. Later on, Sawtooth intends to give extra security

**Conclusion and future work :-**

Sawtooth platform is built for enterprise usage. It is built with a focus on modularity and extensibility with learning based from bitcoin and ethereum. This technology helps developers to develop smart contracts in different programming languages. Future developments in sawtooth would be based on privacy with focus on increasing the privacy of transactions and throughput.

1. **Hyperledger Architecture**

https://www.hyperledger.org/wpcontent/uploads/2017/08/Hyperledger\_Arch\_WG\_Paper\_1\_Consensus.pdf

**Understanding :**

This paper describes a generalized reference architecture for consensus.

Business blockchain requirements vary. Some uses require rapid network consensus systems and short block confirmation times before being added to the chain. Scalability, confidentiality, compliance, workflow complexity, and even security requirements differ drastically across industries and uses.

This paper also describes safety and liveness , in which safety means that each node is guaranteed the same sequence of inputs and results in the same output on each node and Liveness means that each non-faulty node will eventually receive every submitted transaction, assuming that communication does not fail.

Hyperledger Consensus:Consensus is the process by which a network of nodes provides a guaranteed ordering of transactions and validates the block of transactions.

What is a Consensus algorithm?

In general, a consensus algorithm is a process in computer science used to achieve agreement on a single data value among distributed processes or systems.There are two main types of Consensus. Hyperledger makes use of the consensus from the pool of other consensus named the consensus. The operating assumption for Hyperledger developers is that business blockchain networks will operate in an environment of partial trust. Thus, the voting-based algorithms are advantageous in that they provide low-latency finality.

**Conclusion & future scope:**

The larger Hyperledger plan theory for permissioned blockchain systems pursues a particular methodology that empowers extensibility and adaptability. Inside this particular methodology, Hyperledger characterizes normal useful segments and the interfaces between them, which enables any segment to be adjusted autonomously without influencing the remainder of the framework.

1. **Ethereum**

<https://ljk.imag.fr/membres/JeanGuillaume.Dumas/Enseignements/ProjetsCrypto/Ethereum/ethereum-yellowpaper.pdf>

**Understanding:**

The Ethereum is a project that trying to build the gene-eralized technology; technology that can be used to build all transaction-based state machine concepts. In addition, it seeks to provide the end-developer with a tightly integrated end-to-end platform for building applications on a traditional computing model that has hitherto not been explored, a trusted computing framework for object messaging. The Blockchain of Ethereum was mainly inspired by the Bitcoin, using the proof of work as a tool to minimize spam. The main difference Ethereum is that it has a global state where data is stored, often referred to as "The World Computer" in Ethereum, Blocks consist of a series of transactions containing sender, recipient, nonce (to avoid double transactions), and the amount sent and gas data.

It consists of two types of accounts, clients and smart contracts, the biggest difference is that smart contracts do not have a private and public key and when they are generated then they will have the data related to their execution. Users or other smart contracts may execute smart contracts to pay an execution fee called Gas, gas is a protective mechanism to reduce the infinite consumption of resources through mistakes or malicious actors, Actor who wants to use a smart contract should pay for a gas with a block cap, which not allowing endless loops and the network to be stalled. It is said that Ethereum is implementing a Quasi Complete Turing Machine because of the implementation of Gas.

The Ethereum was planned from the beginning to be a proof of Stake blockchain, but the software wasn't prepared, to facilitate migration to Proof of Stake, an internal mechanism called a difficulty bomb was introduced to increase the mining difficulty. Just like Bitcoin, with the premise that mining would be a simple swap from electricity to Ether, Ethereum was designed to be as accessible as possible to as many people as possible. Bitcoin has a scourge known as ASICs that mine with advanced hardware to stop ASICs Ethereum implements another proof-of-stake algorithm called Ethash comparison.

In conclusion, overall, the structure of bitcoin is better for storing value, but ethereum is the perfect solution for creating decentralized applications and finances.

Future scope:

The Ethereum is a decentralized machine belonging to all and not owned by anybody. It's available forever, nobody can stop it or filter it. It is highly inefficient because it consists of a multitude of computers connected (in peer-to-peer mode) to each other, each running an open source program. Ethereum is also a secure machine that collaborates with each unit, ensuring reliability, validation, and device protection. If one of the components cheats or fails, the others will ignore it.

**7. Hyperledger Blockchain Performance Metrics**

<https://www.hyperledger.org/wpcontent/uploads/2018/10/HL_Whitepaper_Metrics_PDF_V1.01.pdf>

**Understanding :**

This paper serves as to characterize the fundamental terms and key measurements that ought to be utilized to assess the exhibition of a blockchain technology and afterward impart the outcomes.This paper likewise fills in as a stage freethinker asset for specialized blockchain designers and supervisors keen on utilizing industry standard classification.This paper is focused on blockchain performance evaluation and the associated metrics, rather than on benchmarking.

Blockchain Performance depends on below factors:

Performance Evaluation Terms

Test harness is the hardware and software used to run the performance evaluation.

Client is an entity that can introduce work into a system or invoke system behaviors. In a blockchain system, there are often multiple types of clients at multiple levels. System Under Test (SUT) is defined as the hardware, software, networks, and specific configurations of each required to run and maintain the blockchain. Node is an independent computing entity that communicates with other nodes in a network to work together collectively to complete transactions.

Considerations for Blockchain Performance Evaluation

Test Environment should have Consensus protocol,Geographic distribution of nodes,Hardware environment of all peers,Network model,Number of nodes involved in the test transaction,Software component dependencies,Test tools and framework,Type of data store used for doing performance testing. Workload defines how the SUT is exercised.

Faultloads : All blockchains should be designed to provide ledger immutability, cryptographic authenticity, and tolerance against faults and attacks as core properties. Node In blockchain network, a node is an independent computing entity that communicates with other nodes in a network to work together collectively to complete transactions.

**Conclusion and future scope:**

In this paper, we conducted a comprehensive study to understand the performance metrics of Hyperledger by varying discussing about different metrics , Considerations for Blockchain Performance Evaluation,Definitions of Key Metrics and Blockchain Terms. Further, we plan to quantify the impact of various consensus algorithms and number of nodes in the ordering service on the performance of different workloads. In our study, we assumed that the network is not a bottleneck. However, in the real world setup, nodes can be geographically distributed and hence, the network might play a role. In addition, the arrival rates in real world production system would be following certain distributions.

This archive gives some direction on choosing and assessing remaining tasks at hand. We anticipate that refinements should define blockchain-explicit measurements will warrant future modifications of this report.

**8. Hyperledger Burrow (formerly eris-db)**

https://www.hyperledger.org/wp-content/uploads/2017/06/HIP\_Burrowv2.pdf

**Understanding:**

Hyperledger Burrow is one of the Hyperledger projects which operates as a permissioned Ethereum smart contract blockchain node. Its primary function is to execute the Ethereum smart contract programming code on a permissioned virtual machine. It has been released in December 2014 and was the very first of its kind. The burrow is helpful to continue the existing work of the hyper ledger by proving the strong deterministic contract focused blockchain design to the projects overall efforts. In hyperledger burrow the primary user are aiming a value chain level optimization amongst other blockchains and smart contract benefits. Burrow was intended to be a universally useful savvy agreement machine and isn't advanced for the prerequisites of any single industry; rather Burrow has been upgraded for universally useful, cross-industry shrewd agreement use cases.

Some significant features of Burrow:

• Burrow’s current release is version 0.16.1.

• It has existed under various names since October, 2014.

• Burrow is under active development.

• Burrow is licensed under the Apache License, version 2.

• Burrow is deployable over any cloud platform, currently available on AWS and Azure with further ready-to-deploy cloud solutions already under development. Several tasks for the project are either in progress or on the design table. These can be broken down into “usability improvements” and “code improvements”.

The major components of Burrow are as follows:

• Consensus engine

• Application Blockchain Interface

• Smart contract application engine

• Gateway

Burrow acknowledges customer side detailed and marked exchanges for which we have an interface for remote marking accessible. Further work is in progress to coordinate character the executives to permit existing RSA X.509 confirmation answers for attest substantial elliptic bend open keys on the blockchain. We anticipate contribution from and arrangement with the Hyperledger Identity workgroup on this issue.

**Conclusion and Future scope:**

Outside marking arrangements are pivotal for Burrow's clients as they permit the blockchain hubs to be kept running on ware equipment. We are extremely keen on blending our continuous work to actualize remote marking with other Hyperledger Projects that additionally are trying to use outside marking arrangements as opposed to expecting clients to run their blockchains on exceptionally secure equipment.

The Burrow is ongoing project and its success is highly depends on the involvement of the developers. Once this project will complete it will bring many changes in the above mentioned areas.

**9. Hyperledger Indy Public Blockchain**

file:///C:/Users//Desktop/Understanding%20Hyperledger%20Indy%20Ledger.pdf

**Understanding:** Hyperledger Indy is a distributed ledger, purpose-built for decentralized identity. In particular, Privacy by Design and privacy-preserving technologies are critically important for a public identity ledger where correlation can take place on a global scale. It has its own implementation of Distributed Ledger and it is not dependent on any other blockchain platform. Hyperledger Indy provides tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other silo.

The architecture of hyperledger Indy can be understand by comparing bitcoin, ethereum and Indy. Bitcoin is decentralize money, Ethereum is decentralize application and on the other hand Indy is decentralize identity. There are two nodes: Validator; which handles writes and reads and these nodes come to consensus, Observer; it handles reads and keep their state in sync with the validators.

Indy has multiple Ledger which includes:

• Audit Ledger

• Config Ledger

• Pool Ledger

• Domain Ledger

**Conclusion and future scope:** The Hyperledger Indy is purpose-built for identity. I has its own Ledger and consensus protocol implementation, it is in production (Sovrin network) for more than 2 years, Authentication, Authorization and dynamic validation is based on the information from the Ledger ○ Audit Ledger synchronizes the ledgers and introduces blocks. Hyperledger Indy is a distributed ledger, purpose-built for decentralized identity. Developers can use the tools and libraries from Hyperledger Indy to create identity solutions that are interoperable across jurisdictions and agencies.

**10. REINFORCING THE LINKS OF THE BLOCKCHAIN**

<https://blockchain.ieee.org/images/files/pdf/ieee-future-directions-blockchain-white-paper.pdf>

**Understanding :**

Blockchain innovation is ready to change about each aspect of our advanced lives, from the manner in which we send cash to the manner in which we heat our homes. By hindering outsiders, blockchains guarantee to make our frameworks progressively effective. By bypassing restriction, they guarantee to make our frameworks progressively fair. What's more, if appropriately actualized, they could make our frameworks increasingly dependable and secure.

The plan for a blockchain system and least necessities for an overseeing understanding among an advantaged subset of the hubs' administrators to guarantee that touchy and private information can be taken care of and safely erased upon request.

Blockchain technology is set to change the finance market like blockchains may also increase efficiencies behind the scenes at financial institutions especially in the process of interbank settlement, Energy sector : Blockchain platforms will also likely take some role in replacing the systems that now manage the distribution of electricity. As a smarter grid is built, blockchains may aid in facilitating dynamic signaling between producers and consumers, especially as the line between those roles continues to blur.

**Conclusion:**

Blockchain-based applications profit by a few extraordinary highlights that are not found in applications worked with standard databases. The vast majority of these highlights can be condensed in the accompanying articulation: it doesn't make a difference who runs a blockchain on the grounds that so single element "possesses" it. What this implies practically is that information and projects put away on a blockchain will be protected against evacuation, and will perform precisely (as composed), paying little heed to who is taking every necessary step of including new passages and documenting past ones. This is a portrayal of an admired blockchain framework, one in which the motivations of the members have been appropriately adjusted. In any case, it precisely depicts the most well known blockchain stages in activity today

Future scope of application :

Blockchain-based applications profit by a few extraordinary highlights that are not found in applications worked with standard databases. The vast majority of these highlights can be condensed in the accompanying articulation: it doesn't make a difference who runs a blockchain

on the grounds that so single element "possesses" it. What this means functionally is that data and programs stored on a blockchain will be safe against removal, and will perform accurately (as written), regardless of who is doing the work of adding new entries and archiving past ones. Identity,in the future people who use blockchain identity management systems, may be able to more easily recover their records in the case of emergencies. Supply chain : Blockchains have been proposed as a replacement for documentation processes in the shipping industry, due to the many geographical regions and jurisdictions that a product moves through on its way to the consumer. Telemedicine Individuals receive their healthcare from a diverse collection of providers all of whom need access to the same patient information. Furthermore, these records must be up to date and authenticated by reliable sources.

**11. Blockchain**

https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf

**Understanding :**

Blockchain technology is a database that is consensually shared , replicated and synchronized.The replication and storage of transactional data by each part or node on a blockchain network is called as distributed ledger. Blockchain while similar to database are not used to store general storage but rather than hold information about transactions .

Blockchain is distributed into three parts :

Block: A rundown of recorded exchanges over some stretch of time. Exchanges can speak to for all intents and purposes any sort of action from enlisting a land deed to a solitary buy. Any standards identifying with the square itself are set up when the system is first made. For instance, the most extreme number of exchanges in a square or the size of each square can be constrained.

Chain: When the square arrives at its greatest size of exchanges, it is fastened or connected to the first square through a hash as portrayed in the segment underneath. The hash estimation of one square is embedded into the following square. This makes a connection between the new square and the past square. Rehashing a hash work on an unaltered square of information will consistently create the equivalent fixed-length esteem. On the off chance that a square of information is changed, the subsequent hash yield will be unique. A client would then be able to see the hashes are unique and will realize the first square has been changed and may never again be dependable.

Network: The system is comprised of hubs each containing a total record of all exchanges on a blockchain. No concentrated "official" duplicate exists and no hub is "trusted" more than another. The information respectability is kept up by the blockchain being recreated on the entirety of the hubs.

Each blockchain has its own rules or algorithms governing how nodes validate transactions intended for entry into the blockchain.

**Conclusion :**

Blockchain is of three types : Public : Large disseminated blockchains are accessible for anybody to take an interest in and are commonly publicly released with the code kept up by an expansive network. Permissioned: Large conveyed blockchain coordinate with set up jobs that people can fill when utilizing the blockchain.Private: Oftentimes a littler blockchain is firmly controlled and is set up between confided in elements that desire to share data. Bitcoin is spread into four platform : Bitcoin , Ripple, Hyperledger and Ethereum

**Future scope :**

Developing policies to address the records management implications of blockchain. Implementing systems that can execute those policies, Ensuring blockchain records/transactional data can be accessed over time. Executing the disposition of blockchain records/transactional data by deleting them or transferring them to the National Archives.

**12. Bitcoin: A Peer-to-Peer Electronic Cash System**

[**http://blockchainlab.com/pdf/bitcoin.pdf**](http://blockchainlab.com/pdf/bitcoin.pdf)

**Understanding :**

A simply shared form i.e Peer to Peer version of electronic money would enable online installments to be sent legitimately starting with one party then onto the next without experiencing a budgetary foundation. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not just fills in proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Transactions: Electronic coin is defined as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority that checks every transaction for double spending. After each transaction, the coin must be returned to the central authority to issue a new coin and only coins issued directly from the central authority are trusted .The problem with this solution is that the fate of the entire money system depends on the company running the central authority i.e. with every transaction having to go through them, just like a bank

Calculations: We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain

p = probability an honest node finds the next block

q = probability the attacker finds the next block

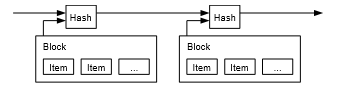
qz = probability the attacker will ever catch up from z blocks behind

qz={ 1 if p≤q q/ pz if pq}

Given our assumption that p > q, the probability drops exponentially as the number of blocks the attacker has to catch up with increases

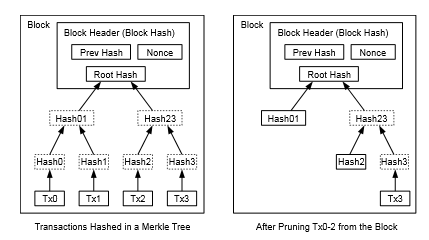
Conclusion: We have proposed a system for electronic transactions without relying on trust which depends on below events:-

Timestamp Server: A timestamp server works by taking a hash of a block of items to be time stamped and widely publishing the hash. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



Network : New transactions should be broadcasted to all nodes. Each node shall collect new transactions into a block. Each node shall works on finding a difficult proof-of-work for its block. When a node finds a proof-of-work, it shall broadcasts the block to all nodes. Nodes shall accept the block only if all transactions in it are valid and not already spent. Nodes shall express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Reclaiming Disk Space: Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space.



Future scope : Bitcoin may change the world more than the Internet did. The hope is that this new technology will turn digital divide, among and within countries, into digital opportunities. The reduction of transaction costs and the elimination of costly and sometimes obscure layers of intermediation have the potential to favour financial inclusion for the benefit of society.

**13. ChainDB: A Peer-to-Peer Database System**

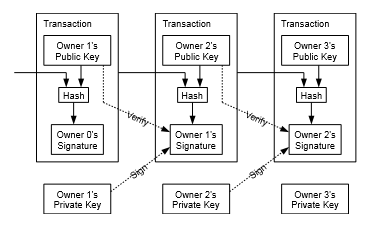
[**https://bitpay.com/chaindb.pdf**](https://bitpay.com/chaindb.pdf)

**Understanding:**

Chain DB is new approach to securely store data related to bitcoin in the cloud. The Bitcoin has identified itself to be safe and host large number of database administration of clients around the planet. ChainDB seeks to apply that same approach to securing arbitrary sets of data in the cloud. ChainDB uses the existing Bitcoin mining network rather than creating another Bitcoin clone which requires its own mining network. The Bitcoin database services millions of users around the planet and has thus far shown itself to be essentially invulnerable to attack. ChainDB seeks to apply that same approach to securing arbitrary sets of data in the cloud. However, rather than create yet another Bitcoin clone that requires its own mining network, ChainDB uses the existing Bitcoin mining network.

Validation rules speciﬁc to a ChainDB govern whether a given chain of blocks and transactions is valid. Participants in a chain create blocks and append them to the chain by competing to get their block deﬁning transaction into the Bitcoin block chain.

Transactions: A chainDB transaction mutates the state of database. When it is financial database related transaction , that transaction might look very similar to a bitcoin transaction. The rules of a ChainDB transaction can be ﬁxed and they might employ a scripting system similar or identical to that of Bitcoin. Transactions in a ChainDB are a set of transaction validation rules that are speciﬁc to the chain. The structure and composition of transactions in a ChainDB is unrelated to the consensus process that organizes the transactions into a semantically consistent history.



Block: ChainDB transactions are organized into blocks. ChainDB blocks are linked to the Bitcoin block chain by embedding the hash of the ChainDB block in a Bitcoin transaction. By rule, no more than one ChainDB block can be deﬁned in a Bitcoin block.Timestamping ChainDB blocks with less frequency will incur less cost. Below diagram

A comprehensive ordering of all transactions also makes it possible to select a block even when some blocks are being withheld.

Bidding:Nodes that produce ChainDB blocks are called builders. A chain builder organizes valid transactions into blocks and creates a Bitcoin transaction that references the chain and ChainDB block. The Bitcoin transaction includes a miner fee that reﬂects the value of deﬁning a ChainDB block to the bidder

**Conclusion:** A ChainDB organize works a lot of like the Bitcoin arrange Like Bitcoin, ChainDB hubs communicate ChainDB exchanges and squares to all hubs, every one of which performs free approval. New exchanges are communicated to all hubs . Every hub gathers new exchanges into a square. Every hub delivers a Bitcoin "offer" exchange to deﬁne the square (utilizing an unspent yield that it endeavored to facilitate with different hubs. The offer exchange is communicated to Bitcoin excavators and other ChainDB hubs. While ChainDB is structured with open interest, open databases as a primary concern, private or shared private databases can likewise beneﬁt. An individual or association could store basic data on machines that are promptly available on the web and beneﬁt from the fake safe properties of ChainDB.

**Future scope:**

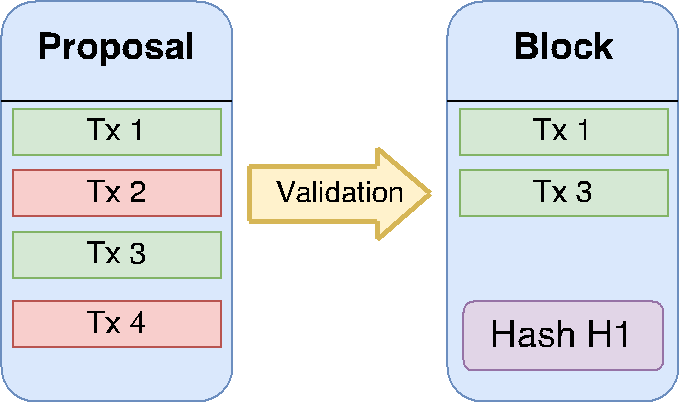
A ChainDB organize works a lot like the Bitcoin arrange Like Bitcoin, ChainDB hubs communicate ChainDB exchanges and squares to all hubs, every one of which performs free approval. New exchanges are communicated to all hubs . Every hub gathers new exchanges into a square. Every hub creates a Bitcoin "offer" exchange to deﬁne the square . The offer exchange is communicated to Bitcoin diggers and other ChainDB hubs. While ChainDB is planned with open support, open databases at the top of the priority list, private or shared private databases can likewise beneﬁt. An individual or association could store basic data on machines that are promptly open on the web and beneﬁt from the fake safe properties of ChainDB.

**14. YAC: BFT Consensus Algorithm for Blockchain**

<https://arxiv.org/abs/1809.00554>

**Understanding:**

Consensus in decentralized systems that asynchronously receive events and which are subject to Byzantine faults is a common problem with many real-life applications. Advances in decentralized systems, such as distributed ledger (i.e., blockchain) technology, has only increased the importance of finding performant and secure solutions to consensus of state machine replication in decentralized systems.  
YAC is a practical decentralized consensus algorithm, that solves the problems of inefficient message passing and strong leaders that occur in classical Byzantine fault tolerant consensus algorithms. The algorithm is open source and currently is used to provide Byzantine fault tolerant consensus for the Hyperledger Iroha blockchain project. We provide proofs of safety and liveness, as well as empirical results showing that our algorithm can scale to dozens of validating peers.

****

**Fig. 1. Validation process.** Alice removes invalid transactions.

**Alice’s validation process**

Alice is a ‘validator” who validates a proposal P1. Alice tries to apply each transaction in the proposal to her local state. A transaction is considered valid if it is not ill-formed according to validation rules, and its application does not vio-late rules about global state (e.g., no account can have negative balances). The validation process is shown in Figure 1. Alice creates a block from all valid transactions and calculates hash of block H1.

**Vote step delay:** The purpose of this experiment was to deduce an optimal value for the vote step delay, which is the period of time for each peer to decide on the proposal to become the next block in the chain by voting. We tested several values in different network configurations to discover the relationship between the number of peers in the network, vote step delay parameter, and the number of proposals processed per second (system throughput).

**Conclusion and Future Work:** We presented YAC, a novel Byzantine fault tolerant con-sensus algorithm for blockchain systems. Using voting on block proposals, YAC is able to guarantee safety and liveness for transaction processing, given that not more than f faulty validating peers are present out of at least 3f + 1 peers on the network. This paper provides an overall description of the algorithm execution in different cases. Also, we followed the steps of a YAC execution example where peers have different states. Empirical results using the open source implementation of YAC in Hyperledger Iroha show that the algorithm can scale to dozens of validating peers, however the delay at the vote step must be adjusted for the number of validating peers in order to reduce exhibited faults by peers.

**15. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends**

<https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends>

**Understanding** :Blockchain, the establishment of Bitcoin, has gotten broad considerations as of late. Blockchain fills in as a permanent record which permits exchanges occur in a decentralized way. Blockchain-based applications are jumping up, covering various fields including monetary administrations, notoriety framework and Internet of Things (IoT, etc. Be that as it may, there are as yet numerous difficulties of blockchain innovation such as adaptability and security issues standing by to be survived.

This paper exhibits a complete outline on blockchain innovation. We give a review of blockchain architechture right off the bat and think about some run of the mill accord calculations utilized in various blockchains. Besides, specialized difficulties and late progresses are quickly recorded. We likewise spread out conceivable future patterns for blockchain.

Comparisons among public blockchain, consortium blockchain and private blockchain

|  |  |  |  |
| --- | --- | --- | --- |
| Property | Public blockchain | Consortium blockchain | Private blockchain |
| Consensus determination | All miners | Selected set of nodes | One organization |
| Read permission | Public | Could be public or restricted | Could be public or restricted |
| Immutability | Nearly impossible to tamper | Could be tampered | Could be tampered |
| Efficiency | Low | High | High |
| Centralized | No | Partial | Yes |
| Consensus process | Permissionless | Permissioned | Permissioned |

TABLE II: Typical Consensus Algorithms Comparison

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Property | PoW | PoS | PBFT | DPOS | Ripple | Tendermint |
| Node identity management | open | open | Permissioned | open | open | permissioned |
| Energy saving | No | partial | Yes | partial | yes | yes |
| Tolerated power | < 25% | < 51% | < 33.3% | < 51% | < 20% | < 33.3% |
| of adversary | computing | stake | faulty replicas | validators | faulty nodes in | byzantine voting |
|  | power |  |  |  | UNL | power |
| Example | Bitcoin | Peercoin | Hyperledger | Bitshares | Ripple | Tendermint |
|  |  |  | Fabric |  |  |  |

Key Characteristics of Blockchain: In summary, blockchain has following key characteristics.

Decentralization. In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), in-evitably resulting to the cost and the performance bottle-necks at the central servers. Contrast to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.

Persistency. Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discov-ered immediately.

Anonymity. Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user.

**Conclusion and FutureWork:**

Blockchain has demonstrated its potential for changing customary industry with its key qualities: decentralization, persistency, secrecy and auditability. In this paper, we present an exhaustive outline on blockchain. This paper first gives a review of blockchain innovations including blockchain design and key attributes of blockchain. We at that point talk about the run of the mill accord calculations utilized in blockchain. We examined and thought about these conventions in various regards. Besides, we recorded a few difficulties and issues that would ruin blockchain advancement and abridged a few existing approaches for taking care of these issues. Some conceivable future headings are likewise proposed. These days blockchainbased applications are jumping up and we intend to lead inside and out examinations on blockchain-based applications in the future.

**16. Introduction to Libra blockchain.**

<https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf>

**Understanding:**

The Libra Blockchain, on which the currency runs, is pseudonymous, which will be allowing users to contain one or more addresses that are not linked with their real-world identity. It is also open source, so it can be used by any user, developer or company, create products on top of it, and add value through its services. It will start as a "permission blockchain," meaning that Facebook must determine what entities will serve as validator nodes for processing transactions. Anyone who meets the technical requirements can run a validator node in permission less blockchains such as Bitcoin's. Facebook says that while its aim is to see the Libra network become illegal, it is currently not possible to accomplish what they are trying to achieve through such a network. One of the Libra Association's aims is to study and introduce the transition to a permission-free network and continue this work "within five years of the Libra Blockchain and ecosystem's public release."

**A new ' Move ' programming language**: "Move," a new programming language which is for implementing custom transaction logic and "smart contracts" on the blockchain is at the core of the Libra Blockchain. A smart contract is a contract created using blockchain technology to validate, enable or enforce the fulfillment of contract obligations. Move has the highest priorities of safety and security, Facebook says, and is explicitly designed to prevent the cloning of property. It does so by requiring "resource types" that restrict digital assets to the similar properties such as physical assets, a resource has only single owner, it can be used only once, and the creation of new resources is restricted. Facebook says the Libra blockchain uses a consensus protocol to verify transactions that is designed to work even if one-third of the validator nodes are down, and which is more energy-efficient than consensus by "proof of work" that Bitcoin's blockchain requires. The Libra Blockchain is a single data system which tracks the history of transactions and states over time, unlike previous blockchains, which interpret the blockchain as a series of transaction blocks. This, says Facebooks, would make it easier for apps that use the blockchain to use a single platform to read and validate any information at any time.

The association is regulated by the Association Council of Libra, which consists of one member per node of validator. All decisions on network and reserve governance are brought to the council, and the approval of two-thirds of voters is required for major policy or technical decisions. The association is the only group capable of creating (mint) and killing (burn) libra. Only when licensed resellers purchased these coins from the association with fiat resources to completely back the new coins would coins be minted. These are only burned in return for the underlying assets when the licensed resellers sell Libra coin to the association.

**Conclusion:**

The association's crucial goal is to increase decentralization over time, says Facebook. This will ensure that the entry barriers to building and using the network are small and will boost the durability of the ecosystem over the long term.

**Future Scope:**

Together with WhatsApp's 1.5 billion users, Facebook and its 2.38 billion monthly active users should provide a great starting user base for Libra. Yet past experience has shown that even a giant like Facebook is sometimes not sufficient to push user adoption. Facebook has therefore collaborated with various financial and retail companies, as well as some non-profits, to accelerate user adoption, making Libra less of a Facebook venture and more of a global one in particular.

**17. Hyperledger Architecture vol 2**

<https://www.hyperledger.org/wpcontent/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf>

**Understanding:**

This smart contract paper offers a simplified smart contract reference architecture. The paper also discusses how various blockchain implementations of Hyperledger which are Burrow, Fabric, Indy and Sawtooth, which apply the reference architecture. Here, the blockchain is a decentralized network with lot of nodes that interact with each other. The blockchain runs chaincode programs, keeps the data from state and ledger, and executes transactions. The chaincode is the central element since transactions are chaincode operations. Transactions must be endorsed and only transactions that have been endorsed can be made and have an impact on the state. For control functions and parameters, one or more unique chaincodes can exist, collectively being called system chaincodes.

The blockchain's new state (or, literally, system) is modeled as a versioned key-value store (KVS), where names and values are arbitrary blobs. The chaincodes (applications) are running on the blockchain by put and get KVS operations exploit these entries. The state is permanently registered, and state changes are logged. Please note that versioned KVS is adopted as a state template, an implementation can use actual KVSs, but also RDBMSs or other solution.

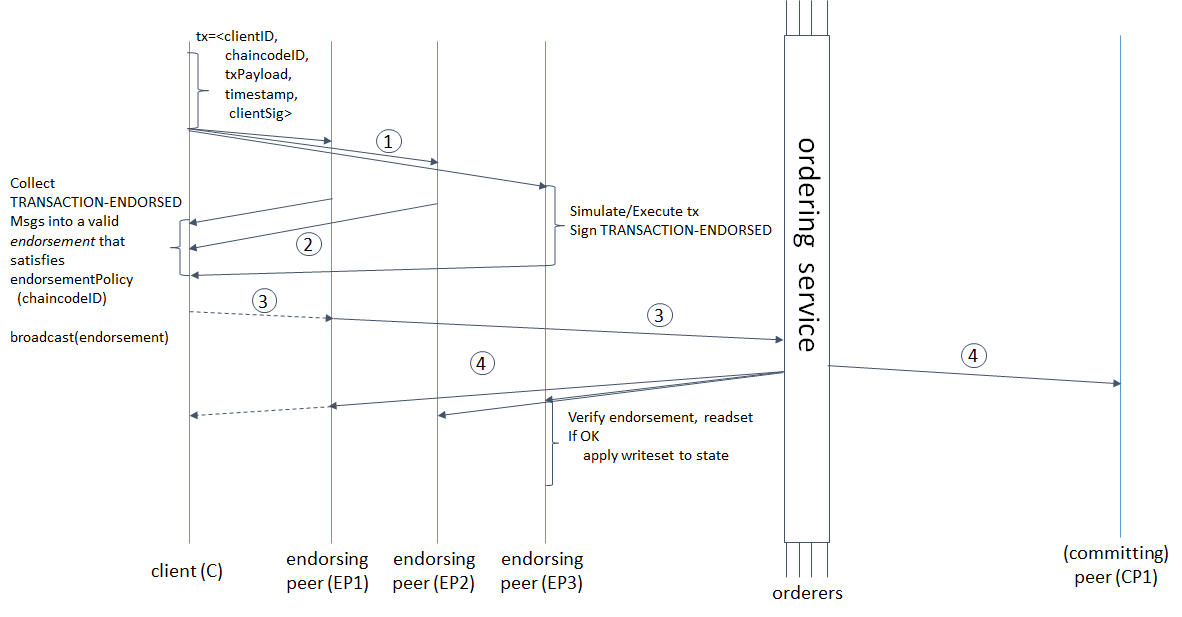
More formally, state s is modeled as a mapping element K-> (V X N),where K is a set of keys and V is a set of values N is an infinite set of numbered versions.

Next injective function: N-> N takes an element of N and returns the number of the next version.

All V and N have a special element (empty type) that is the lowest element in the case of N. At first, all keys are mapped to (⊥, ⊥). We denote v by s(k).value for s(k)=(v, ver) and s(k).version for ver.

KVS operations are being modeled as follows: put(k, v) for k ∈ K  and v ∈ V, now take the blockchain state s and switch it to s'(k)=(v, next(s(k).version)) with s'(k')=s(k ') for all k '! = k. Returns s(k) to get(k). Peers retain the state, but not orders and customers.

State partitioning, Keys in the KVS may be identified as belonging to a particular chaincode by their name, in the sense that only a certain chaincode transaction can modify the keys that belong to this chaincode. By theory, the keys of other chaincodes can be read by any chaincode. It is a post-v1 function to allow cross-chaincode transactions that change the state of two or more chaincodes.



**Conclusion and future scope:**

For licensed blockchain networks, the Architecture WG will continue to define the following core components: Consensus Layer, Smart Contract Layer, Communication Layer, Data Store Abstraction, Crypto Abstraction, Identity Services, Policy Services, APIs, and Interoperation.

The Architecture WG published a simplified smart contract reference architecture that any Hyperledger project can use. The concepts of reference architecture are expressed in unique ways by Hyperledger Burrow, Hyperledger Fabric, Hyperledger Iroha, and Hyperledger Sawtooth.

Blockchain technology implementation is not only limited to the finance industry alone. In various sectors such as supply chain management, digital advertising, forecasting, cyber security, Internet of things, networking, etc., it has a fantastic future.

**18. Block chain Technologies: Logical Government Application and Challenges**

<https://icma.org/sites/default/files/2018-Nov%20Blockchain%20White%20Paper.pdf>

**Understanding:**

This paper clarifies the potential utilizations of square chain innovation for neighborhood government use just as the dangers and difficulties related with its usage, as demonstrated for certain situation thinks about performed to date.

Bitcoin is history's first perpetual, decentralized, worldwide, trustless record of records. Since its creation, business people in ventures the world over have come to comprehend the ramifications of this improvement. The idea of block chain innovation has got minds going out of control, on the grounds that the thought would now be able to be applied to any requirement for a dependable record. It is likewise placing the full intensity of cryptography in the hands of people, preventing advanced connections from requiring an exchange expert for what are considered 'pull exchanges'.

The use of block chain innovation, be that as it may, isn't restricted to digital money. There are multitudinous potential uses of block chain beside advanced monetary forms, including guaranteeing information uprightness, principle training auditable records, and making self-executing keen contracts. With regards to neighborhood government, utilization of disseminated records can diminish exchange costs in the conveyance of nearby administrations, while likewise giving more prominent straightforwardness and open door for cooperation by residents. None of these potential employments of block chain innovation require the utilization of digital currency. Block chain innovation can lessen the time and cost related with information the executives, grant preparing, also, implementing administrative consistence, among other things. Self-executing brilliant contracts with programmed triggers can streamline numerous administration capacities.

**Conclusion and future scope:**

By looking all the application of block chain we can say that this technology is innovative and has the potential to improve and change the way we store and process the data. Numerous states have passed enactment identified with block chain innovation, including Arizona, California, Delaware, and Nevada. Some enactment is structured to explicitly perceive understandings went into on the block chain as lawfully restricting agreements. Others are intended to consider block chain innovation and investigate its potential applications. While these administrative activities are a beginning, the most troublesome and revolutionary uses of block chain will require authoritative changes to government-controlled procedures.

Block chain may improve nearby government proficiency and information integrity, and limit cost in the long haul. In spite of the guarantees of unchanging nature and unhackability, there will consistently be a hazard that data in a block chain falls into an inappropriate hands. Neighborhood government pioneers should approach block chain arrangements with incredulous however receptive outlooks, with the understanding that a considerable lot of the mysterious guarantees encompassing block chain are finished blown and not sensible.

**19.Wrapped Tokens: A multi-institutional framework for tokenizing any asset**

<https://www.wbtc.network/assets/wrapped-tokens-whitepaper.pdf>

Understanding:

Wrapped tokens is a multi-institutional resource tokenization system that sticks to the brought together approach. Be that as it may, rather than depending completely on a solitary foundation, it depends on a consortium of organizations performing various jobs in the system. Ethereum based tokens have risen as a significant resource class, on account of the gigantic selection of the ERC20 standard and the inclination of Ethereum as the go to block chain innovation for DeFi (decentralized finance) ventures. Recently, the advantage supported tokens advertise has additionally experienced exponential development and promotion as enthuthiasts endorse them to be the "holy grail" of digital currency. Token on the Ethereum block chain can serve various different functions and in this paper the asset backed or wrapped tokens has been focused.

Wrapped tokens give an approach through which different organizations in the digital currency space can participate to move beyond normal issues looked by current stablecoin executions. Accordingly, clearing path for another age of stablecoins that can tackle Ethereum in a substantially more sans trust way towards empowering: worldwide liquidity, diminished exchange expenses, expanded fragmentary proprietorship and keen agreement programmability.

**Future Scope:**

Smart contract open source and permanent nature empowers permissionless development. With the Wrapped Tokens configuration design, engineers can broaden the capacity of a current crypto asset and make it interoperable with other decentralized applications. With the help of it users could transfer DAI by paying the transaction fee in DAI as well, never needing to possess ETH.

This technology can also be used in atomic swaps can be utilized among traders and clients so as to trade WBTC and BTC. On the off chance that the client might want to get WBTC or BTC all the more rapidly, a believed technique for trade should likewise be possible through the shippers.

**Conclusion:**

In some sense overseers are confided in the wrapped system, as resources could be taken or they probably won't respect the coordinated support. Nonetheless, the wrapped system intends to limit this trust. Through wrapped tokens, we propose an answer for make resources compatible and representable on the Ethereum chain. Worldwide liquidity, expanded fragmentary proprietorship, savvy contract programmability and decrease in exchange expenses are a portion of the key advantages of tokenization. WBTC will be the principal such token, empowering DApps simple access to Bitcoin. All exchanges, agreements and reviews will be freely distinguishable to keep up straightforwardness and empower trust in the system. The structure likewise gives a manner by which numerous foundations in the digital currency space can perform various jobs to move beyond basic issues looked by resource supported tokens.

**Comparing and Contrasting different approaches:**

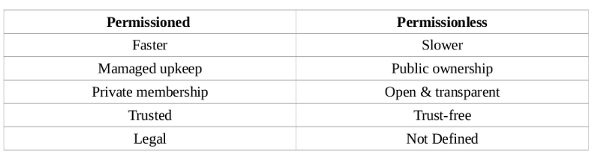
**Types of Ledger:**

**Public Ledger:** Decentralized, anyone can read and send transactions. e.g. Bitcoin, Ethereum, Hyperledger

**Private Ledger:** Centralized under one organization which controls the right to view and sens transactions. e.g. Bank chain, multichain

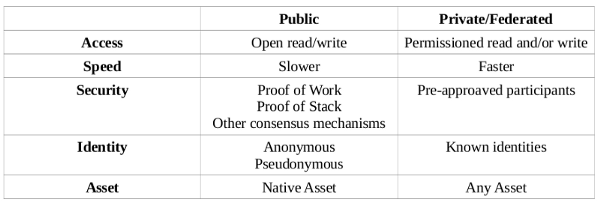
**Permissionless Blockchain:** Every node in the network participate in consensus procedure, e.g. Bitcoin Blockchain (Proof of Work)

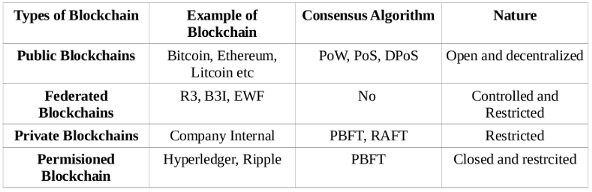
**Permissioned Blockchain:** Only Selected nodes(validators, e.g. Government or trusted nodes) participate in consensus procedure e.g. Hyperledger Blockchain.



**Public Blockchain:**Anyone in the world can download the data and read the data. Anyone can participate in the consensus process to write the data or block into the public Blockchain. There are numerous public blockchains. Bitcoin which is a peer to peer currency exchange was the first public Blockchain followed by Ethereum which allows anyone to build smart contracts and decentralized apps on it. Some other examples are Dash and Lisk. It is highly secured using cryptography and consensus protocol.

**Examples — Bitcoin, Ethereum, Dash, Lisk, Factom, and Blockstream.**

.



**Comparing the different Blockchain techniques:**

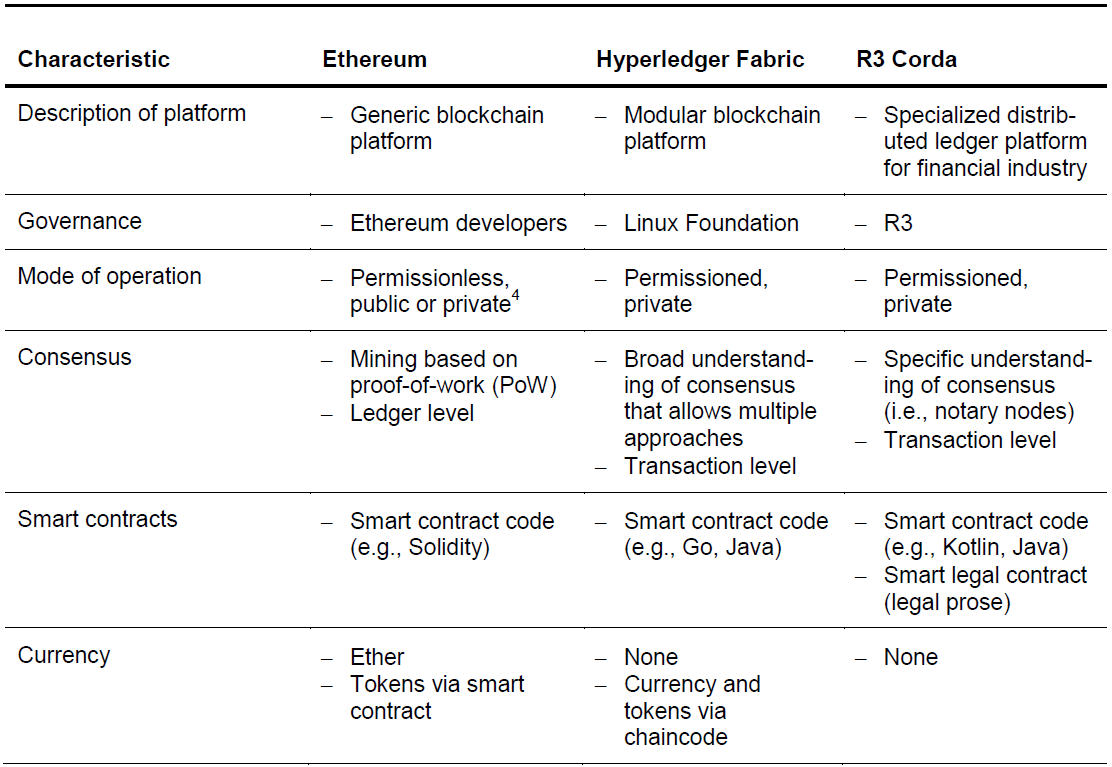


Table 1: Comparison of Ethereum, Hyperledger Fabric and Corda

**Hyperledger vs Ethereum**

|  |  |  |
| --- | --- | --- |
| **Features** | **Hyperledger** | **Ethereum** |
| **Purpose** | Preferred platform for B2B businesses | Platform for B2C businesses and generalized  applications |
| **Confidentiality** | Confidential transactions | Transparent |
| **Mode of Peer Participation** | Private and Permissioned Network | Public/Private and Permissionless Network |
| **Consensus Mechanism** | Pluggable Consensus Algorithm: No mining required | PoW Algorithm: Consensus is reached by mining |
| **Programming Language** | Chaincode written in Golang | Smart Contracts written in Solidity |
| **Cryptocurrency** | No built-in cryptocurrency | Built-in cryptocurrency called Ether |

**Annotated Biblography**

1. **Bitcoin: A Peer-to-Peer Electronic Cash System**

Nakamoto, S. (2018, January 14). Bitcoin: A Peer-to-Peer Electronic Cash System. *Economic Inquiry*, [online] 56(3).

https://bitcoin.org/bitcoin.pdf [Accessed 14 Oct. 2019].

Mr. Nakamoto discussed about the electronic cash system, where In its unstructured nature, the device is robust. Hubs work with little cooperation at the same time. They should be remembered as messages are not guided to a particular spot and should only be transmitted on the best basis of exertion. Hubs could easily exit and rejoin the network, tolerating the job chain verification as proof of what happened when they were no longer there.

1. **Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains**

Androulaki, Elli. (2018, August 24). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains.

Retrieved October 15, 2019 from

<https://arxiv.org/pdf/1801.10228.pdf>

Ms. Androulaki discussed about the hyperledger fabric, where fabric is a communicated job structure assessed and extensible to operate approved blockchains. It presents a novel layout that isolates exchange execution from agreement and empowers underwriting-based arrangement and suggests middleware-imitated databases.

1. **The Libra Blockchain**

Amsden, Zachary. (2017, October 12). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains.

Retrieved October 16, 2019 from

<https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf>

Mr. Zachary has stated brief description about the Libra Blockchain. This is a proposal for the Libra protocol, which permits a lot of validators to give a decentralized database to following programmable assets. We have examined an open-source model — Libra Core — of the Libra convention and indicated how the presentation of the Move programming language for shrewd agreements enables the protocol to execute the one of a kind plan of the Libra biological system.

1. **Hyperledger sawtooth: An Introduction**

Olson, Kelly. (2018, January 12). Hyperledger sawtooth: An Introduction.

Retrieved October 16, 2019 from

<https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf>

Ms. Olson discussed about the hyperledger sawtooth. Hyperledger Sawtooth is an enterprise blockchain platform for building distributed ledger applications and networks. The design philosophy targets keeping ledgers distributed and making smart contracts safe, particularly for enterprise use. Sawtooth intends to keep disseminated records circulated and to make savvy contracts alright for big business use.

1. **Hyperledger Architecture**

Bowman, Mic. (2018, February 19). Hyperledger Architecture.

Retrieved October 19, 2019 from

<https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf>

Mr. Bowman gave an overview on Hyperledger Architecture. In general, a consensus algorithm is a process in computer science used to achieve agreement on a single data value among distributed processes or systems.There are two main types of Consensus. Hyperledger makes use of the consensus from the pool of other consensus named the consensus. The operating assumption for Hyperledger developers is that business blockchain networks will operate in an environment of partial trust. Thus, the voting-based algorithms are advantageous in that they provide low-latency finality.

1. **Ethereum**

Wood, Gavin. (2019, January 12). ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.

Retrieved October 21, 2019 from

<https://gavwood.com/paper.pdf>

Mr. Wood discussed about ethereum cryptocurrency. The Ethereum was planned from the beginning to be a proof of Stake blockchain, but the software wasn't prepared, to facilitate migration to Proof of Stake, an internal mechanism called a difficulty bomb was introduced to increase the mining difficulty. Just like Bitcoin, with the premise that mining would be a simple swap from electricity to Ether, Ethereum was designed to be as accessible as possible to as many people as possible. Bitcoin has a scourge known as ASICs that mine with advanced hardware to stop ASICs Ethereum implements another proof-of-stake algorithm called Ethash comparison.

1. **Hyperledger Blockchain Performance Metrics**

(2018, March 24). Hyperledger Blockchain Performance Metrics.

Retrieved October 23, 2019 from

<https://www.hyperledger.org/wp-content/uploads/2018/10/HL_Whitepaper_Metrics_PDF_V1.01.pdf>

This paper serves as to characterize the fundamental terms and key measurements that ought to be utilized to assess the exhibition of a blockchain technology and afterward impart the outcomes.This paper likewise fills in as a stage freethinker asset for specialized blockchain designers and supervisors keen on utilizing industry standard classification.This paper is focused on blockchain performance evaluation and the associated metrics, rather than on benchmarking.

1. **Hyperledger Burrow (formerly eris-db)**

Middleton, Dan. (2017, January 28). Hyperledger Burrow (formerly eris-db).

Retrieved October 22, 2019 from

<https://www.hyperledger.org/wp-content/uploads/2017/06/HIP_Burrowv2.pdf>

Mr. Middleton gave descriptive overview of Hyperledger Burrow. Burrow acknowledges customer side detailed and marked exchanges for which we have an interface for remote marking accessible. Further work is in progress to coordinate character the executives to permit existing RSA X.509 confirmation answers for attest substantial elliptic bend open keys on the blockchain. We anticipate contribution from and arrangement with the Hyperledger Identity workgroup on this issue.

1. **Hyperledger Indy Public Blockchain**

Olson, Kelly. (2017, November 21). Hyperledger Indy Public Blockchain.

Retrieved October 23, 2019 from

<https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf>

Ms. Olson discussed briefly about Hyperledger Indy Public Blockchain. The Hyperledger Indy is purpose-built for identity. I has its own Ledger and consensus protocol implementation, it is in production (Sovrin network) for more than 2 years, Authentication, Authorization and dynamic validation is based on the information from the Ledger ○ Audit Ledger synchronizes the ledgers and introduces blocks. Hyperledger Indy is a distributed ledger, purpose-built for decentralized identity. Developers can use the tools and libraries from Hyperledger Indy to create identity solutions that are interoperable across jurisdictions and agencies.

1. **Block chain Technologies: Logical Government Application and Challenges**

Hamill, Julie. Attorney. B. Harris (2018, November). Block chain Technologies: Logical Government Application and Challenges.

Retrieved November 4, 2019 from

<https://icma.org/sites/default/files/2018-Nov%20Blockchain%20White%20Paper.pdf>

This paper clarifies the potential utilizations of square chain innovation for neighborhood government use just as the dangers and difficulties related with its usage, as demonstrated for certain situation thinks about performed to date. Block chain may improve nearby government proficiency and information integrity, and limit cost in the long haul.

1. **Wrapped Tokens: A multi-institutional framework for tokenizing any asset**

2018, January 24. Wrapped Tokens: A multi-institutional framework for tokenizing any asset.

Retrieved November 4, 2019 from

<https://www.wbtc.network/assets/wrapped-tokens-whitepaper.pdf>

In this paper it has been clarifies that wrapped tokens is a multi-institutional resource tokenization system that sticks to the brought together approach. Be that as it may, rather than depending completely on a solitary foundation, it depends on a consortium of organizations performing various jobs in the system. Ethereum based tokens have risen as a significant resource class, on account of the gigantic selection of the ERC20 standard and the inclination of Ethereum as the go to block chain innovation for DeFi (decentralized finance) ventures.

1. **Multichain Private Blockchain**

Greenpan G, Multichain Priveate Blockchain

Retrieved November 1, 2019 from

<https://www.multichain.com/download/MultiChain-White-Paper.pdf>

In this white paper author Greenpan explain about the multichain private blockchain. According to him, at the heart of bitcoin lies the blockchain, a global decentralized ledger which stores the full history of all bitcoin transactions. The blockchain is verified and stored by every node in the bitcoin network. Bitcoin protocol ensure ever node in the bitcoin network has the same version of the blockchain without requiring the authorization which would be decided by the central authority.

1. **ChainDB: A Peer-to-Peer Database System**

ChainDB: A Peer-to-Peer Database System

Retrieved October 29, 2019 from

<https://bitpay.com/chaindb.pdf>

In this paper the concept of chainDB has been explained in a very effective manner. According to author Chain DB is new approach to securely store data related to bitcoin in the cloud. The Bitcoin has identified itself to be safe and host large number of database administration of clients around the planet. ChainDB seeks to apply that same approach to securing arbitrary sets of data in the cloud. ChainDB uses the existing Bitcoin mining network rather than creating another Bitcoin clone which requires its own mining network.

1. **Blockchain**

Blockchain white paper

Retrieved November 2, 2019 from

<https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf>

In this white paper it has been explained that the blockchain technology is a database that is consensually shared , replicated and synchronized.The replication and storage of transactional data by each part or node on a blockchain network is called as distributed ledger. Blockchain while similar to database are not used to store general storage but rather than hold information about transactions.

1. **Reinforcing the Links of the Blockchain**

Peck Morgen. November 2017. Reinforcing the Links of the Blockchain

Retrieved October 17, 2019 from

<https://blockchain.ieee.org/images/files/pdf/ieee-future-directions-blockchain-white-paper.pdf>

In this technical paper the author Peck Morgen has been delivered the understating about theBlockchain innovation and according to him blockchain is ready to change about each aspect of our advanced lives, from the manner in which we send cash to the manner in which we heat our homes. By hindering outsiders, blockchains guarantee to make our frameworks progressively effective. By bypassing restriction, they guarantee to make our frameworks progressively fair.

1. **YAC: BFT Consensus Algorithm for Blockchain**

Muratov Fedor. L. Andrei. I. Nikolai. September 3, 2018. YAC: BFT Consensus Algorithm for Blockchain

Retrieved October 24, 2019 from

<https://arxiv.org/pdf/1809.00554.pdf>

Author Fedor has described abut the BFT Consensus Algorithm for blockchain according to him Consensus in decentralized systems that asynchronously receive events and which are subject to Byzantine faults is a common problem with many real-life applications. YAC is a practical decentralized consensus algorithm, that solves the problems of inefficient message passing and strong leaders that occur in classical Byzantine fault tolerant consensus algorithms

1. **An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends**

Zheng Z. Xie S. June 2017. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

Retrieved October 17, 2019 from

<https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends/link/59d71faa458515db19c915a1/download>

In this paper a complete outline on blockchain innovation has been provided. We give a review of blockchain architechture right off the bat and think about some run of the mill accord calculations utilized in various blockchains. Besides, specialized difficulties and late progresses are quickly recorded. We likewise spread out conceivable future patterns for blockchain.

1. **Introduction to Libra blockchain**

An Introduction to Libra

Retrieved October 17, 2019 from

<https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf>

The Libra Blockchain, on which the currency runs, is pseudonymous, which will be allowing users to contain one or more addresses that are not linked with their real-world identity. It is also open source, so it can be used by any user, developer or company, create products on top of it, and add value through its services. It will start as a "permission blockchain," meaning that Facebook must determine what entities will serve as validator nodes for processing transactions.

1. **Hyperledger Architecture volume II**

Hyperledger Architecture volume II.

Retrieved November 10 from

<https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf>

In this paper author has explained about the Hyperledger Architecture, according to him this smart contract paper offers a simplified smart contract reference architecture. The paper also discusses how various blockchain implementations of Hyperledger which are Burrow, Fabric, Indy and Sawtooth, which apply the reference architecture. The blockchain's new state (or, literally, system) is modeled as a versioned key-value store (KVS), where names and values are arbitrary blobs.

Blockchain technology implementation is not only limited to the finance industry alone. In various sectors such as supply chain management, digital advertising, forecasting, cyber security, Internet of things, networking, etc., it has a fantastic future.