Submission Number: 2 **Submission Date: April 11, 2021**

Group Number: (C19-S4) 03

Group Members:

Full Legal Name	**Location (Country)**	**E-Mail Address**	**Non-Contributing Member (X)**
Divakaran Karunakaran	India	divakar94@gmail.com	
Moses E. Tommie	Liberia	tommiemoses1988@gmail.com	
Al Rey Villagracia	Philippines	arcvillagracia@gmail.com	

Statement of integrity: By typing the names of all group members in the text box below, you confirm that the assignment submitted is original work produced by the group (*excluding any non-contributing members identified with an "X" above*).

Divakaran Karunakaran
Moses E. Tommie
Al Rey Villagracia

Use the box below to explain any attempts to reach out to a non-contributing member. Type (N/A) if all members contributed.

X

** Note, you may be required to provide proof of your outreach to non-contributing members upon request.*

Introduction

Blockchain technologies have been prominent in developing or integrating software of networks to allow easy, cheap, scalable, and secured transactions for developers and businessmen. These blockchain technologies are widely accepted now and well supported by large technologies, banks, and corporates. In this work, we compared "scalability, consensus protocol, privacy, degree of decentralization and settlement finality" of Bitcoin, Ethereum, Hyperledger and Corda.

In this section, we looked at the project overviews of each blockchain technology.

Project Overviews

1. **Bitcoin**

Bitcoin blockchain was the first blockchain to be ever built. It was created by Satoshi Nakamoto. The token used in the blockchain is again Bitcoin which is now seeing ever-growing popularity as a worthy cryptocurrency of the future. The Bitcoin blockchain is complete, tamper-resistant and public. Below we shall see some of the features of this blockchain along with its advantages and disadvantages.

2. **Ethereum**

Ethereum is an open-source platform where developers can create decentralized applications (D'Apps). In comparison bitcoin is a blockchain technology meant to transact bitcoin tokens as a currency. The token generally used in Ethereum platform is referred to as 'Ether' which is the Ethereum currency. Ethereum follows several tech and protocols that bitcoin uses. Ethereum differs to bitcoin in the sense that it uses ERC20 token standard for the DApps built on its platform. Hence through this standard, DApps on Ethereum can be extended to include more than just currency ledgers.

3. **Hyperledger**

Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration including leaders in banking, finance, Internets, manufacturing industries, supply chains, and technology. Hyperledger does not promote a single blockchain codebase or a single blockchain project but enables a worldwide developer community to work together and share ideas, infrastructure, and code.

Hyperledger began in 2015 January with intention to create an enabling environment to make the vision of blockchain software a reality. Since then, it had drawn the interest of many companies working together to achieve more. It was immediately placed under the guardianship of Linux Foundation. The aim of Hyperledger is to create an enabling environment that will make the vision of blockchain. Hyperledger has more than 230 organizations as members and 3.6 million lines of code, 10 active working groups, and close to 28,000 participants who have come to 110+ meetups around the world. Hyperledger further assumed that the future of blockchain is modular, open-source platforms that would be easy to use.

Further, Hyperledger serves as a greenhouse –it brings together users, developers, and vendors from diverse sectors and market spaces to learn developing and using blockchain. It incubates new ideas, support each one with essential resources, and distribute the results widely. The green house structure as an open source development provides series of benefits:

- Help keeping up with developments
- Better productivity through specialization
- Collaboration to avoid duplicate efforts
- Better quality control of code
- Easier handling of intellectual property

4. Corda

Corda is a permissioned, private and enterprise blockchain platform developed by R3 launched in December 2018 for Distributed Ledger Technology (DLT) applications –based registration systems through a network of software platforms. It allows businesses to transact directly using smart contracts and in strict privacy with one another which follows a peer to peer transaction model. It aims to be the sole global ledger connecting institutions and people. It is backed by Amazon Web Services Intel, Microsoft, and a legion of the world's largest banks, technology and industries. Corda is open-source, open-design and open development. It does not have its own cryptocurrency to incentivize the nodes through mining operations. Corda uses "Notary Clusters," or bundles of data containing verified information relating to a transaction to validate the legitimacy of transactions. These "Notary Clusters". However, cryptocurrency (e.g. XDC) can still be added by businesses to supplement other blockchain technologies such as Ethereum.

Discussion

In this section we compare each blockchain technology based on the following characteristics: “scalability, consensus protocol, , privacy, degree of decentralization, and settlement finality”.

Table 1 Comparison of Blockchain Technology

Characteristic	**Bitcoin**	**Ethereum**	**HyperLedger**	**Corda**
Scalability	Limited by Proof of Work (PoW)	Limited by Proof of Work (PoW). In development to move towards Proof of stake (PoS)	Considerable scalability and transactions per second (TPS)	Highly scalable
Consensus Protocol	Pseudo – Anonymity. But vulnerable to transaction graph analysis	Account based system reduces privacy as account balances become public	Confirms the correctness of all transactions in a proposed block, according to endorsement and consensus policies. It also agrees on order and correctness and results of	Requires validity consensus and uniqueness consensus
Privacy	Highly decentralized, but once Bitcoin supply is exhausted, lack of incentive might lead to centralization	Highly decentralized	two scenarios: strictly confidential to the outside members of the channel; confidential for the sorting service peer.	Identity protected by KYC. Only participants can determine the details of the transaction

Degree of Decentralization	Probabilistic (51% network approval needed)	Probabilistic (51% network approval needed)	While they are capable of preserving the confidentiality of data, decentralized architectures cannot easily protect them against the analysis of metadata.	Private decentralization tied to notary clusters/nodes. Within the corporate's firewall of decentralization.
Settlement Finality	Proof of Work (PoW)	Proof of Work (PoW). In development to move towards Proof of stake (PoS)	Committed ledger is final. Forward-only ledger.	Forward-only ledger.

1. Scalability

Bitcoin's major disadvantage lies in this area wherein the cryptocurrency's transaction speed is currently limited to 7 transactions per second. This disadvantage arises mostly due to Bitcoin's PoW consensus protocol which takes up to 10 minutes to validate a single block on to the blockchain. This is an important issue which hinders Bitcoin's acceptance as a currency. Compared to traditional methods the speed is extremely slow and hence acceptance of the public is still in question as this makes instantaneous sending and receiving of currency very slow.

Ethereum offers a slightly improved rate of transactions per second. In comparison to Bitcoin, it offers almost double the transactions speeds. Currently it stands at 15 transactions per second. This slow speed is once again attributed to the Proof of work consensus it follows just like bitcoin.

This had become the biggest challenge to Blockchain adoption due to the inability of the decentralized world to compete with the traditionally centralized entities which seem to be a norm proving largely hegemonic. Scalability is an important part of blockchain technology that helps firms to increase efficiency, reduce the cost of infrastructure and operations; increase profitability and increases consumer's confidence in an organization. Further, scalability the

central focus is how the system should process transactions. Therefore, it had become a key requirement for enterprises as a result of the large-scale of businesses in the industry.

Corda network can support billions of transactions daily across industries, and it can store and process data using a ledger. As Corda differs generally with a blockchain sharing encrypted data, Corda records its own deals as a distributed ledger technology to ensure confidentiality and increase its scalability.

2. Consensus Protocol

In traditional banks, there is always a centralized system or middleman through which transactions occur from one account to the other. In blockchains however, 'decentralized' system comes into play wherein there is no central party which must approve the transactions. In lieu of this, the creator of Bitcoin Satoshi Nakamoto came up with the idea of Proof-of-work (PoW) by which everyone can validate transactions. By this, computers around the world must compete to solve a complex mathematical equation. Whoever solves the equation first will be given the right to validate the next block on the chain. The 'miner' who was successful will receive a 'block reward' for his contribution to the blockchain after all other nodes have come into consensus with latest added block. This process in Bitcoin takes 10 minutes. It also creates an unfair playing field as people with more CPU resources will have an advantage over the others.

Ethereum's current method of consensus is Proof of work. However, the developers of Ethereum are working towards a shift in this protocol towards Proof-of-stake (PoS) consensus. Proof of stake works differently in that it requires the miners to stake some of their cryptocurrency holdings to be voted for validating a block on the blockchain. Their chances of being selected as a node to validate the next block is proportional to the amount of cryptocurrency they stake. This way they are incentivized to be more cautious in validating the blocks as validating a block of fraudulent transaction would lead them to lose their stake.

The consensus in Hyperledger network is a process where the nodes in the network provide a guaranteed ordering of the transaction and validating those blocks of transactions that need to be committed to the ledger. It Interfaces and depends on smart-contract layer to verify correctness of an ordered set of transactions in a block. Consensus satisfies on average two properties in order to guarantee agreement among nodes: safety and liveness. Safety - each node is guaranteed the same sequence of inputs and results in the same output on each node. When the nodes receive an identical series of transactions, the same state changes will occur on each node. Liveness – each non-faulty node eventually receives every submitted transaction, assuming that communication does not fail.

Corda requires transactions to have validity and uniqueness consensus. Validity consensus is done by each required signer to check that the contract is valid and all its dependencies, while uniqueness consensus prevents double-spends and only performed by the notary cluster.

3. Privacy

Bitcoin is a public ledger. Although bitcoin transactions are anonymous and secure, they are not necessarily invisible and hence any transaction that occurs can be viewed by anyone. The public address although untraceable to the owner of the account, can be used in a transaction graph analysis where a graph is built, and patterns and links are drawn between various transactions. This was a critical method which was used by FBI to arrest the founder of 'Silk Road' platform which used only bitcoin for its transactions.

Privacy is one of the key areas where the difference between Bitcoin and Ethereum starts showing. Sharing Ethereum public keys for transactions immediately opens them up and lets others view the balance inside your account. Comparatively Bitcoin shields this information, and it is not possible to retrieve this information from a Bitcoin's public key. The Ethereum protocol keeps track of the user's ether balance. Ethereum's account-based model makes it more susceptible to such transparency. Moreover, it opens it up to Danaan-style attacks. Accounts can also be made human readable, and this further poses a huge risk to privacy.

In Hyperledger, private transactions offer a more fine-grained level than channels. the sensitive data is distributed peer-to-peer amongst parties relevant to the transaction, while only the hashes of that data are recorded on the shared/public ledger. The private data is stored in a database local to the authorized parties and maintained by the Fabric infrastructure. This database is updated alongside the public ledger as transactions containing references to private data are committed. The hashes on the public ledger serve as verifiable proof of the data. Private data is not allowed to reside off the premise of the parties involved in the transaction for regulatory and legal reasons. Privacy is achieved in that there is control as who can access such sensitive data.

In Corda, only the participants and those who need to validate the transaction can determine the details. They share only the necessary information between them without broadcasting it or its details across the entire network. Transactions are recorded by the ledger with assured identities of the parties involved without exposing it in the global ledger through the KYC requirements. Participants will only share the transaction history when necessary. The nodes

can be placed behind a corporate firewall so that their information is always secure. Lastly, Corda uses HSM integration to ensure that the process of signing keys remains protected.

4. Degree of Decentralization

With various technologies that power Bitcoin's blockchain and the other protocols governing it, Bitcoin has ensured that it is truly decentralized. However, one argument that opposes this is that the rise in 'mining pools'. Mining pools are places where resources such as CPU, GPU are pooled together to crack the complex math equations and the block rewards are shared among its investors. With major pools coming up, block validations are increasingly limited to a majority few and this has raised many concerns of pure decentralization as these block validators may approve fraudulent transactions to the blockchain by colluding

Unlike Satoshi, the founders of Ethereum did not stop after the white paper presentation and continue to work on Ethereum. This has raised many concerns about the 'centralization' of Ethereum. Apart from these concerns, Ethereum's decentralization degree is almost as same as Bitcoin's.

Decentralization deals with a system where there is no authority that governs and handles the network. Consequently, such network can be full of control, immutable data and a high level of security. However, there is high level of cost attached and it misuse of authority and volatility. Further, in decentralization of Hyperledger, there is no third-party involvement

Since Corda is distributed ledger technology, it records its own deals and can be placed behind the corporate firewall. It is a private decentralization within the corporate and to other companies it deals with sharing only the details of each transaction with each other.

5. Settlement Finality

In a centralized system, it is possible to reverse transactions. In bitcoin, the transactions cannot be reversed once they are added to the Blockchain and a consensus has been reached. In theory, if most of the network (51%) decides to go back, it can re-mine and go back to a blockchain's previous state. Hence there is a probability that settlements can be reversed. This probability reduces with increase in chain length over time. This is essentially why people wait for over 6 more blocks to be added before they confirm their transactions as complete.

Like Bitcoin, finality of settlements is probabilistic and 51% of nodes need to agree to go back to reverse the transactions.

This is a statutory, regulatory, and contractual construct that refers to the moment in time when one party is deemed to have discharged an obligation or to have transferred an asset or financial instrument to another party, and such discharge or transfer becomes unconditional and irrevocable despite the insolvency or entrance into bankruptcy of either party. The specific criteria differ by jurisdiction, asset class (*e.g.*, currency or securities), modes of payment or transfer (*e.g.*, checks or wire), and type of participant (*e.g.*, banks or non-banks). It is important for large-value payment systems to demonstrate that their operational processes are recognized by applicable jurisdictions as resulting in settlement finality.

Unlike Bitcoin or Ethereum, proof of work consensus is unfit for enterprise usage. Only the participants and the notary cluster can finalize the transactions. Corda follows the forward-only ledger in which it is unlikely to change the previous transactions.

Summary

In this work we discussed the project overviews of Bitcoin, Ethereum, Hyperledger and Corda as blockchain technology platforms which is well-supported by world's largest technologies and banks. We compared their characteristics with respect to their scalability, consensus protocol, privacy, degree of decentralization, and settlement finality. Each blockchain provides their own advantages and disadvantages, and sometimes they can supplement each other.

References

1. https://www.ledgerinsights.com/corda-enterprise-accenture-blockchain-winner/ retrieved on April 10,2021
2. https://www.corda.net/blog/corda-v-hyperledger-v-quorum-v-ethereum-v-bitcoin/ retrieved on April 10,2021
3. https://www.ledgerinsights.com/corda-network-first-digital-currency-symbol-xkd/ retrieved on April 10,2021
4. https://medium.com/swlh/choosing-an-enterprise-blockchain-an-exhaustive-guide-749ba7db382c retrieved on April 10,2021
5. https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0022-2 retrieved on January 30, 2019
6. Gledhill, R (August 16, 20190: Choosing an Enterprise Blockchain: An exhaustive guide. Available at https://medium.com/swlh/choosing-an-enterprise-blockchain-an-exhaustive-guide-749ba7db382c
7. https://www.hyperledger.org/wpcontent/uploads/2018/10/HL_Whitepaper_Metrics_PDF_V1.01.pdf retrieved on February 10, 2018
8. https://hal.archives-ouvertes.fr/hal-01382006/document Retrieved on October 15, 2016
9. https://101blockchains.com/hyperledger-blockchain/ retrieved on March 15, 2019
10. https://www.hyperledger.org/wpcontent/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf retrieved on August 21, 2018
11. https://medium.com/akachain-blog/why-scalability-is-important-to-enterprise-adoption-of-blockchain-technology-the-akachain-6d235175813c retrieved on January 14,2019
12. https://www.skcript.com/svr/consensus-hyperledger-fabric/# retrieved on May 21, 2018
13. https://dzone.com/articles/privacy-and-confidentiality-with-hyperledger-fabri retrieved on January 6, 2018
14. https://www.yalejreg.com/nc/on-settlement-finality-and-distributed-ledger-technology-by-nancy-liao/ retrieved on June 9, 2017