August 2018

Performance Analysis of Blockchain Platforms

Pradip Singh Maharjan

PERFORMANCE ANALYSIS OF BLOCKCHAIN PLATFORMS

By

Pradip S. Maharjan

Bachelor of Computer Engineering
Tribhuvan University
Institute of Engineering, Pulchowk Campus, Nepal
2012

A thesis submitted in partial fulfillment of
the requirements for the

Master of Science in Computer Science

Department of Computer Science
Howard R. Hughes College of Engineering
The Graduate College

University of Nevada, Las Vegas
August 2018

UNLV | GRADUATE COLLEGE

Thesis Approval

The Graduate College
The University of Nevada, Las Vegas

May 4, 2018

This thesis prepared by

Pradip S. Maharjan

entitled

Performance Analysis of Blockchain Platforms

is approved in partial fulfillment of the requirements for the degree of

Master of Science in Computer Science
Department of Computer Science

Ajoy K. Datta, Ph.D.
Examination Committee Chair

Kathryn Hausbeck Korgan, Ph.D.
Graduate College Interim Dean

Laxmi Gewali, Ph.D.
Examination Committee Member

John T. Minor, Ph.D.
Examination Committee Member

Emma E. Regentova, Ph.D.
Graduate College Faculty Representative

Abstract

Blockchain technologies have drawn massive attention to the world these past few years mostly because of the burst of cryptocurrencies like Bitcoin, Etherium, Ripple and many others. A Blockchain, also known as distributed ledger technology, has demonstrated huge potential in saving time and costs. This open-source technology which generates a decentralized public ledger of transactions is widely appreciated for ensuring a high level of privacy through encryption and thus sharing the transaction details only amongst the participants involved in the transactions. The Blockchain is used not only for cryptocurrency but also by various companies to meet their business ends, such as efficient management of supply chains and logistics. The rise and fall of numerous crypto-currencies based on blockchain technology have generated debate among tech-giants and regulatory bodies. There are various groups which are working on standardizing the blockchain technology. At the same time, numerous groups are actively working, developing and fine-tuning their own blockchain platforms. Platforms such as etherium, hyperledger, parity, etc. have their own pros and cons. This research is focused on the performance analysis of blockchain platforms which gives a comparative understanding of these platforms.

Acknowledgements

"I would like to express my sincerest gratitude to my thesis advisor, Dr. Ajoy K. Datta for his immense encouragement, guidance, and support throughout my work. I would like to thank him for motivating me.

I would also like to thank Dr. John Minor, Dr. Laxmi Gewali and Dr. Emma E. Regentova for reviewing my work and providing valuable comments. I am grateful to have you in my thesis committee.

I would also like to offer my gratitude to my parents, my wife, my brother and sister for their love and support.

Finally, I would like to thank all my friends who directly or indirectly helped me during my thesis. "

Pradip S. Maharjan

University of Nevada, Las Vegas

August 2018

Table of Contents

List of Tables

List of Figures

Chapter 1

Cryptocurrency

Cryptocurrency is taking the world by storm. A cryptocurrency is a digital currency or virtual asset which uses cryptography to secure its transactions. Cryptography is the medium of secure communication in the presence of other elements or parties who can control the communication channel who can control the communication and eavesdrop[FT16]. These digital currencies work under a protocol named blockchain. The first cryptocurrency to emerge and catch the attention of the world was Bitcoin, launched by Satoshi Nakamoto [Nak08]. As of today, there are hundreds of various cryptocurrencies.

1.1 Digital Currencies

The rise of secure encryption while transferring a message in a network urged the developers to come up with digital money. There are various issues to address before digital money can be made trustworthy. They are listed below

1. Is the money authentic or not counterfeit?
2. How can digital money be controlled so that it can be spent only once? This is popularly known as the double-spend problem.
3. How can it be made secure so that others cannot claim my money?

Paper money must use sophisticated printing technology and more sophisticated papers to tackle the counterfeit problem. Every country comes up with new designs and schemes to battle against counterfeiters. There is no problem of double spending paper money as it will exist in only one place at a time. This conventional money is stored centrally and is transmitted digitally by

use of a centralized system. Unlike paper money, digital money uses cryptography to legitimize the ownership of the asset to the user. Encryption algorithms or cryptographic signatures are used in transactions to prove the validity of the transaction and ownership to the user [An117].

In the late 1980s, researchers came up with various cryptography techniques to build a digital currency backed by national currency and gold, but they were centralized, and transactions were settled at regular intervals, like the way a banking system handles transactions. However, they were prone to attacks by hacker and governments. This paved the way toward the decentralized digital currency Bitcoin, which is free from central authority and robust against attack from hackers [An117].

1.2 Bitcoin

Bitcoin can be said to be a concept or group of protocols for digital money. A unit of this money is called as bitcoin, which can be stored and transmitted among the users or participants in the network via the internet. This protocol is open source software and easily implemented and computed [An117]. Bitcoin currency can be used by transferring it over the network to be used just like traditional currencies, such as for the purchase of goods, transfer of money to other parties, etc. Bitcoin can be easily purchased, sold or exchanged for other currencies at specified currency exchanges. There are a number of Bitcoin ATMs operating to give a user easy access, like conventional currency. Bitcoin has no physical dimensions but is entirely virtual. Users of bitcoins have specific ownership values called keys which give them ownership of their money in the network. These keys can be used to sign transactions and allow a user to spend it by transferring it to a new owner. The Key is the ultimate prerequisite for a user to use their bitcoin, hence the control is in the hand of the user.

Unlike conventional banks, where every transaction is processed in a centralized server, bitcoin is a decentralized, distributed peer-to-peer system. The bitcoin creation is called mining. There are a number of nodes in the peer-to-peer system which process transactions by competing with other nodes to find a solution to a mathematical problem for achieving global consensus on the valid block of transactions. The new-found block is linked with previous blocks. To become a miner, anyone can participate in the bitcoin network and use their resources to verify and record transactions. However, one needs to run the full bitcoin protocol stack, which includes built-in algorithms to regulate the mining function, on their device. When a miner can solve the problem, and validate a block of transactions, he is rewarded with new bitcoins. This way, new bitcoins are

generated after each new block of transactions are validated. On average, a new block is mined after 10 minutes. The mathematical difficulty of the mining task is adjusted dynamically. After every four years, the rate of bitcoin generation is halved. In this protocol, the total number of coins is designed at 21 million coins which will be achieved in the year 2140. Due to its issuance rate, this currency is deflationary. The average size of a block is 1MB, and the bitcoin network can process a maximum(theoretical) of 7 transactions per second and average three transactions per second.

1.2.1 History of Bitcoin

Satoshi Nakamoto published a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008 where he combined several prior works such as b-money and HashCash to visualize a completely decentralized digital cash system with the motive to avoid central authority for issuance of currency and validation of transactions. He proposed one key algorithm, Proof-of-Work, which is used in distributed a peer-to-peer network to reach a consensus every 10 minutes, where all the nodes in the distributed network try to solve a mathematical problem to validate a new set of transactions in the network. This paper also addressed the double spending problem of digital currency [Nak08]. The bitcoin network, based on his paper, started in 2009 with open source code. The Bitcoin network has no individual control of by a single person and operates under consensus among participants in the network based on the mathematical Proof-of-Work algorithm.

Bitcoin presented a practical solution to a problem in distributed computing known as the "Byzantine Generals' Problem" [LL82]. This problem deals with coming up with a consensus on a course of action in the system, by exchanging messages over an unreliable or compromised network. Nakamoto's bitcoin is based on the Proof-of-Work to reach global consensus among the nodes in the distributed system. This solution is used not only for digital currency but for other purposes in distributed networks, such as lotteries, registrations, elections, logistics, etc.

1.3 Litecoin

Bitcoin popularity gave rise to other alternative currencies with a decentralized concept known as altcoins. One of them is Litecoin, derived from Bitcoin which runs on separate a blockchain. Litecoin is very much like Bitcoin and uses the same script to validate transactions. However, Litecoin is much faster than Bitcoin. Validating a block of transactions in the Litecoin network takes only around 2.5 minutes on average by Proof-of-Work, which is much faster compared to the

10 minutes needed in Bitcoin and settles around 28 transactions per second. Litecoin uses scrypt as Proof-of-Work whereas Bitcoin uses SHA-256 [Hin17].

1.4 Dogecoin

Dogecoin is another derived cryptocurrency of the Bitcoin Protocol. Like Bitcoin, it is also an open-source protocol, and it runs on its own blockchain. Compared to Bitcoin, it is easier to generate new coins in Dogecoin. The maximum cap in Bitcoin is 21 million bitcoins, whereas there is no bound on the number of Dogecoins. Using Proof-of-Work for a block on a Dogecoin blockchain take just 60 seconds. As in Litecoin, Dogecoin also uses scrypt for Proof-of-Work. Dogecoin is faster compared to Bitcoin and process as transactions faster than Bitcoin but is limited to the use of cryptocurrency only, as the data structure is not enough for non-cryptocurrency applications. Around 98 billion Dogecoins were initially circulated, and 5.2 billion Dogecoins are added each year. Dogecoins has become popular in the use of Internet tipping system and is used in many exchanges. Many online communities use Dogecoin to trade goods.

1.5 XRP

Arthur Britto, David Schwartz, and Noah Youngs introduced Ripple in 2012, a concept for currency exchange and remittance network built on top of principles of a distributed ledger[DS14]. The Ripple Network developed its own digital asset known as XRP. The Ripple protocol acts as the medium for banks and other financial institutions to use in their systems and allow their customers to use the service. In Ripple, a regulated financial institution holds the funds of customers and issues balances on behalf of its customers. It is based on a shared public ledger where transactions are validated by consensus. It is one of the first distributed exchanges allowing people to buy or sell currencies. Currently, Ripple does not have its own public blockchain, doesn't use Proof-of-Work and is controlled centrally. XRP is one of the fastest digital currency today with easy real-time payments globally. Compared to Bitcoin, Ripple transactions are settled in just 4 seconds, faster than a conventional central banking system. Ripple is rated to process around 50000 transactions per second. 100 billion XRP were created and, based on the Ripple protocol, no more XRP will be created. Unlike bitcoin, XRP is issued by Ripple Labs and not minted into blocks, hence no block mining[Rip, RB, MCR].

1.6 Comparison of cryptocurrencies

Properties	Bitcoin	Dogecoin	Litecoin	XRP
Release year	2008	2013	2011	2012
Block Generation Time	9.7 minute	1 minute	2.5 minute	3.5 second
Hash Rate	28.6*106 TH/s	167.6	213.6 TH/s	n/a
Cryptographic Algorithm	ECDSA	Scrypt	Scrypt	ECDSA
Reward per Block	12.5 BTC	10000	25 LTC	n/a
Power Consumption	Very High	Low	Moderate	low
Total money in circulation	16,959,448 BTC	113,920,730,597 DOGE	56,040,958 LTC	39,094,520,623 XRP
Price	1BTC = $ 6975.13USD	1 DOGE = $ 0.0034USD	1 LTC = $ 114.91USD	1 XRP = $ 0.534 USD

Table 1.1: Comparative analysis of various cryptocurrencies.

Chapter 2

Blockchain Technology

The Blockchain is a shared public ledger distributed among various nodes in the network, where all the transactions or events are recorded. A majority of the participants in the network needs to come up to a consensus to validate the transactions before recording them in the ledger. Once the verified transactions are recorded, it cannot be erased. It contains a verified record of all the transactions from the very beginning[MCK15].

Bitcoin keeps its record on a shared distributed ledger based on Blockchain Technology. Bitcoin has been successful in creating hundreds of billion-dollar markets without governmental control on top of Blockchain Technology. Although Bitcoin has come under several regularity issues from a number of national governments and banks, blockchain technology has been solid and smooth and been accepted globally for various financial and non-financial applications. The Blockchain is believed to have the potential of disrupting conventional financial services.

Currently all our online transactions or activities are dependent on a central authority. Central authority does bank handling of all our financial transactions, such as purchase or sale of goods, transfer of money or an email service provider, while telling us that the online activities through them are secured and trustworthy. Our digital assets and information are tied with the trust of the central authority. Many issues have appeared with the trust of a central authority such as leakage of information, hacking of financial data, etc. This gives necessity to an alternative to a central authority, Blockchain technology. It has the potential to radically transform the digital world by use of a distributed ledger, where each activity is verified and recorded only after reaching consensus among all the parties. The distributed network gives additional privacy and security as it is very difficult to compromise information which has been verified by all the participants. The Blockchain is difficult in technical aspects and hard to regulate but is outweighed by its advantages.

Nowadays financial institutions and banks have begun to accept Blockchain technology and taken a step to change their model to fit into Blockchains. The world's biggest banks are exploring the application of blockchains. Considering how robust and secure blockchain is, it has been accepted not only in the banking and financial applications but also in areas like, private securities, health records, notary payments, royalty payments in the music industry, recording legal documents and many more.

2.1 Terminologies

Transactions: A transaction represents an event between two parties agreeing upon some term without meddling from a third intermediary. It is an important component in the blockchain, as a group of transactions validated is formed into a block which is recorded in a public ledger known as a blockchain [Nak08, CoB]. It can be represented in a data structure as in figure 2.1.

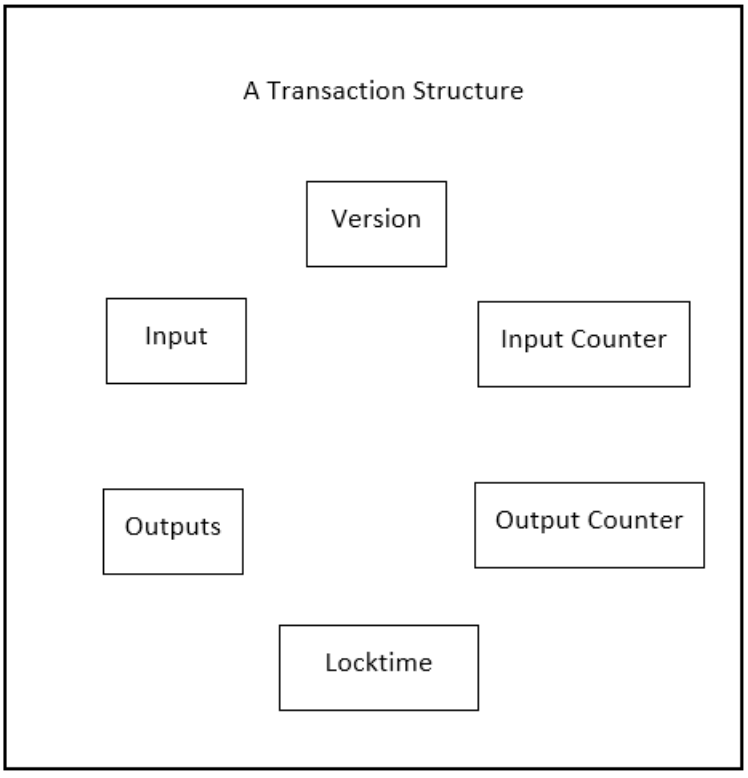

Figure 2.1: Transaction structure

Transaction Fee: A transaction, if not verified by a miner and included in a block, will not be confirmed by the network. The transaction fee is included in every transaction, as motivation for a miner to include that transaction in the next block. It is affected by network capacity, size of

the transaction and market forces [Bit15].

Block: A Block is a data structure that collects the verified transactions to be included in the blockchain. As seen in figure 2.2, a block consists of a header which contains various other metadata and collection of transactions. The block header is 80 bytes, and the average transaction is at least 250 bytes. Generally, a block contains more than 500 transactions, leading to the block size on average of 1 MB[An117]. The collected transactions are recorded in the block in the form of a Merkle tree.

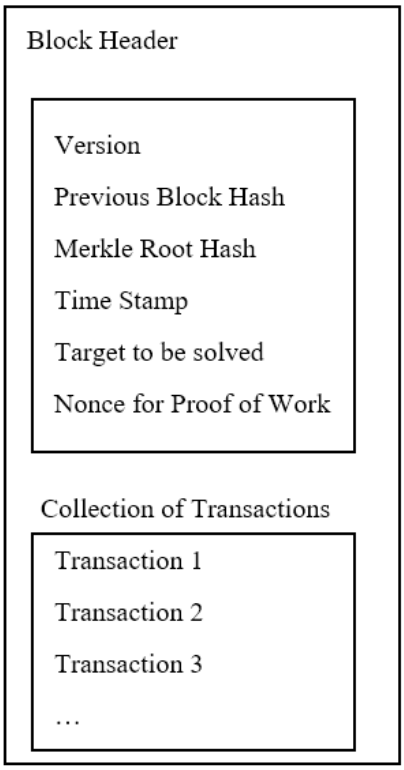

Figure 2.2: Structure of a block

Blockchain: A Blockchain is a distributed public ledger or database where all the transactions are recorded in the form of blocks. Basically, a blockchain can be defined as an ordered data structure, with a back-linked list of blocks of transactions. Each block within the blockchain is identified by a hash, computed by SHA256 encryption algorithm on the header of the block. Then each block references the previous block through the previous block hash field in the block header, as shown in figure 2.2. Then the chain of hashes linking each block goes back to the first ever block created, known as the genesis block [An117, KNS15, BAp, CoB].

Genesis block: It is the very first block in the distributed ledger.

Merkle Tree: The Merkle tree is very crucial in the blockchain technology. It is a binary hash tree which uses SHA256 algorithm to encrypt the transactions and create a summary of all transactions in the block[BAp, CoB]. It is possible to create a huge block of transactions using a Merkle tree, but it will eliminate participation of nodes with low computing resources.

Let us assume there are transaction T1 and T2:

Then, Hash(T1) = SHA256(SHA256(T1))

Hash (T1 T2) = SHA256(SHA256 Hash(T1) + Hash(T2))

The tree is constructed bottom-up. At first, the transactions in the leaves are hashed. As shown in figure 2.3, the adjacent leaf nodes are hashed into parent a node, and so on until only one hash known as the Merkle root is left [Nak08].

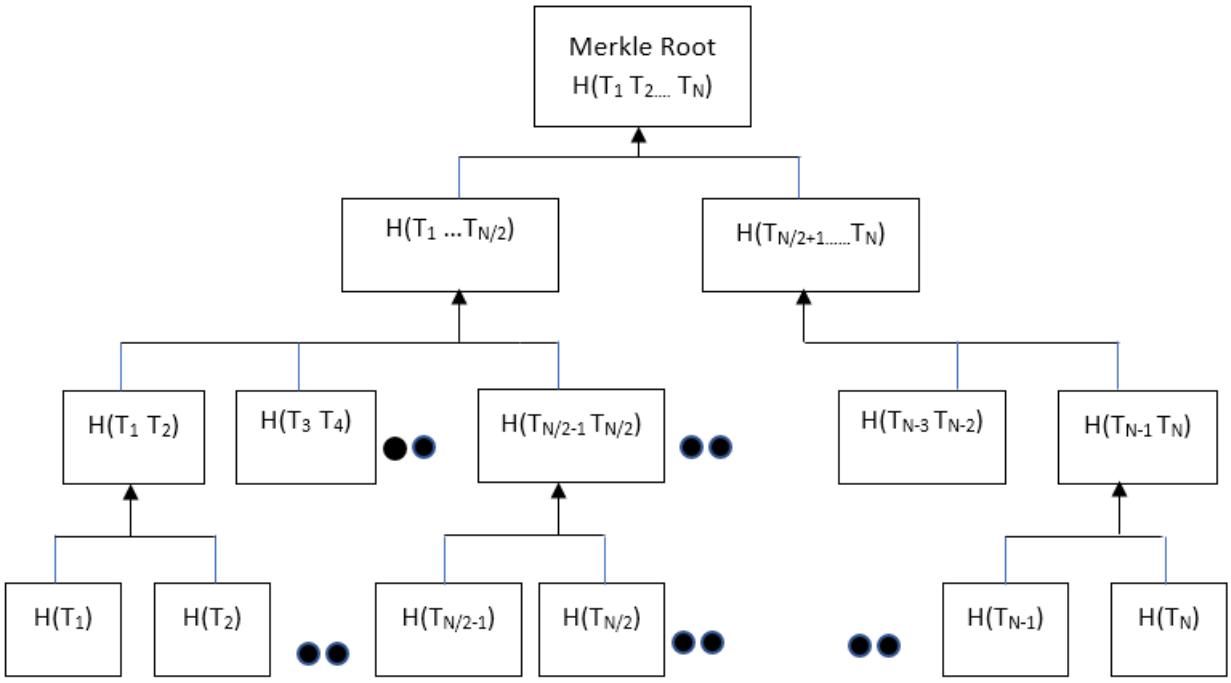

Figure 2.3: Merkle Tree depicting transactions

Miners: The Blockchain network is handled by the miners. They are responsible for hashing the transactions and creating blocks to be added in the blockchain. Miners play an important role in the security of the network and the ledger. A miner who is successful at generating a block and appending it to the blockchain is rewarded with a certain number of bitcoins. Miner nodes in the network compete to determine a new block in a certain time. The mining time depends on the complexity of the mathematical problem that the Proof-of-Work needs to solve [FT16, AKP15].

Block time: It takes a certain amount of time for the miners to find a solution to include transactions in a block, which is called as Block time. [Nak08].

Transaction pool: Miners consider a transaction pool which contains all the transactions for block generation and mining.

Block size: Block size determines the space reserved for each block which may depend on the number of transactions included in the block. For bitcoin, the block size is designed at 1MB.

Confirmation: A transaction is confirmed only after it is verified by the participants in the network and collected into the block. Then it is appended to the blockchain, after which reversing of the transaction is not possible [IER16].

Difficulty: Blockchain difficulty is defined as the complexity to generate a block or successfully validate a set of transactions to collect into a block.

Hashrate: Number of hashes a miner can generate per second to while mining a block is hashrate.

Proof-of-Work: It is a mathematical problem that miners need to solve when hashing transactions.

2.2 How does it work

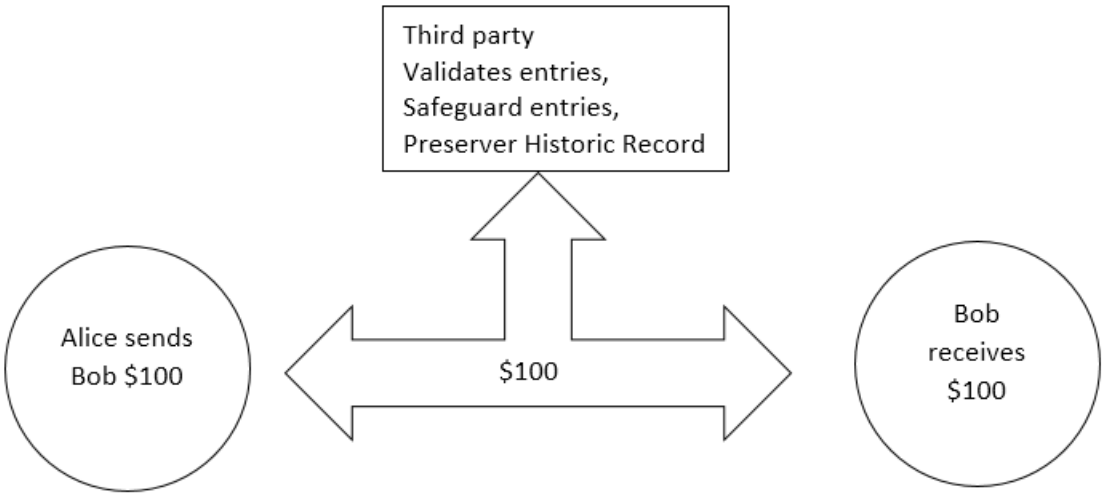

Figure 2.4: Sending money in presence of 3rd party

Blockchain working can be better explained by tying it with Bitcoin. E-commerce is tied with financial service providers which serve as trustworthy third parties. These service providers mediate any electronic transactions and process them. It is their responsibility to validate and secure the

transactions executed through them. Bitcoin uses cryptographic proof removing the third party from the equation to perform an online transaction over the network if two parties are interested. With encryption, each transaction is secured. Here, the public key of the receiver is sent and each transaction is digitally signed using the private key of the sender. To spend money, the owner of the bitcoin must prove the ownership of the private key. The receiver should verify the digital signature and thus ownership of the private key on the transaction using the public key of the sender [MCK15]. As in figure 2.5, every transaction is relayed over the distributed network where each node verifies the transaction and records in a ledger. Before recording, it must be validated for two things;

1. The cryptocurrency is owned by the sender, i.e. the digital signature on the transaction is verified.

2. The sender must have sufficient cryptocurrency in his/her account. It is done by validating every transaction against the sender's account using the public key in the ledger.

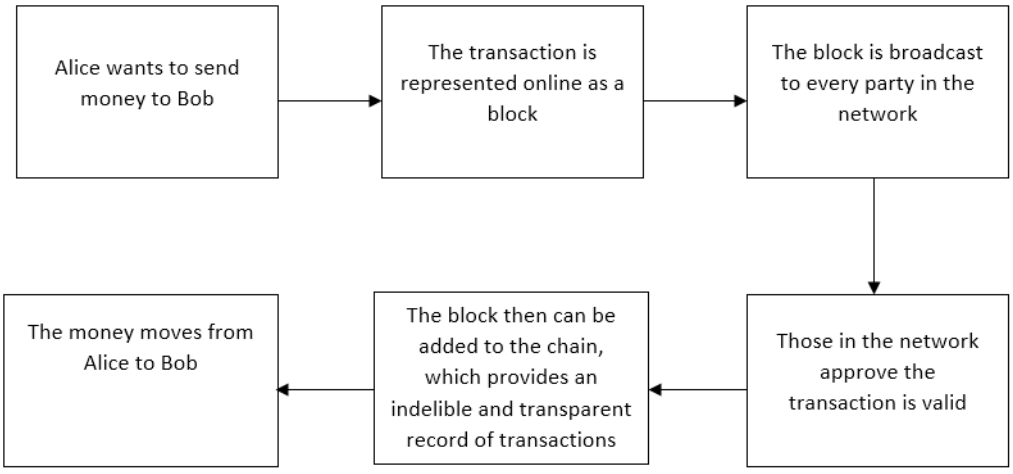

Figure 2.5: Blockchain Technology used to conduct financial transactions.

2.2.1 Double spending problem

The transactions may be broadcasted to all the nodes in the distributed network, but the transactions may arrive at a different time. One party may be involved in a number of consecutive transactions in a short amount of time. Each transaction may be propagated as they were created, but they may not be received by the nodes in the order in which they are generated. As shown in figure 2.6, the 2nd transaction may be validated before the 1st transaction, thus creating a problem

of double spending. So, the system should make sure that the double spending problem does not occur.

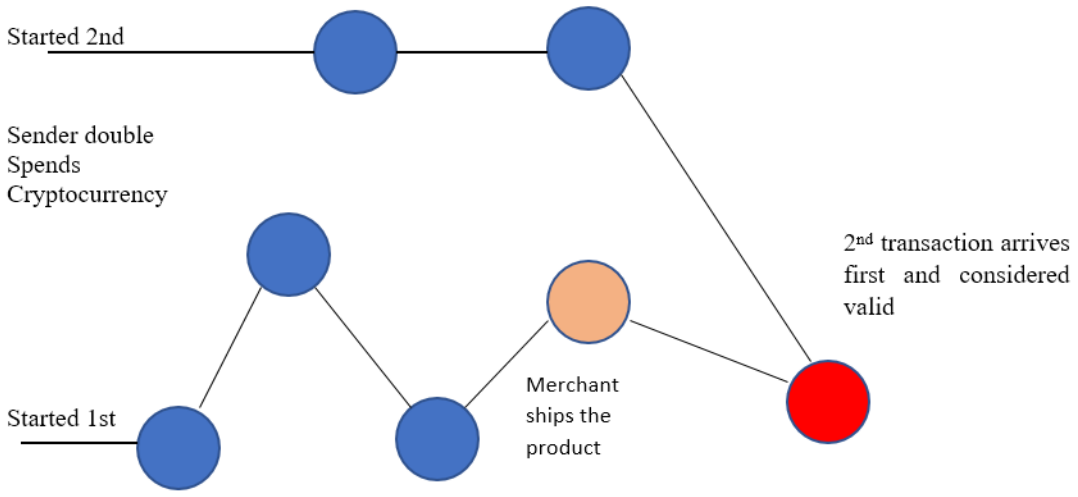

Figure 2.6: Propagation delay in Peer-to-Peer network causing double spending problem.

The transactions considered to happen at the same time in a blockchain are ordered in blocks, and those blocks are connected to each other in chronological order as shown in figure 2.7. All the nodes are busy competing with other nodes, collecting unconfirmed transactions in the network to form a new block and then relaying it to the rest of the network. There may be multiple blocks generated in the network. There must be some consensus among the nodes as to which block will append in the ledger. Also, at any given instant, a block may be different and collect a different number of transactions than other blocks. Also, these blocks which are distributed among the network for consensus can reach different nodes at different times, so the order in which a particular block arrives cannot be relied on.

Bitcoin solves this problem by using Proof-of-Work. The nodes in the network need to solve a mathematical puzzle where each block, collecting transactions after hashing them, must produce some answer that answers a specific condition by investing in computing resources. Each node is required to find a random number called a nonce value (number used once) which is between 0 and 4,294,967,926. This number, when hashed with transactions along with the hash of a previous block, should produce a hash with a certain number of leading zeros. To find this hash value, it will take approximately 10^{21} computations and approximately 10 minutes. If finding blocks becomes easier and quicker after improving the computer power, the number of leading zeros is increased to increase the difficulty and complexity so that a block is generated in an average of 10 minutes.

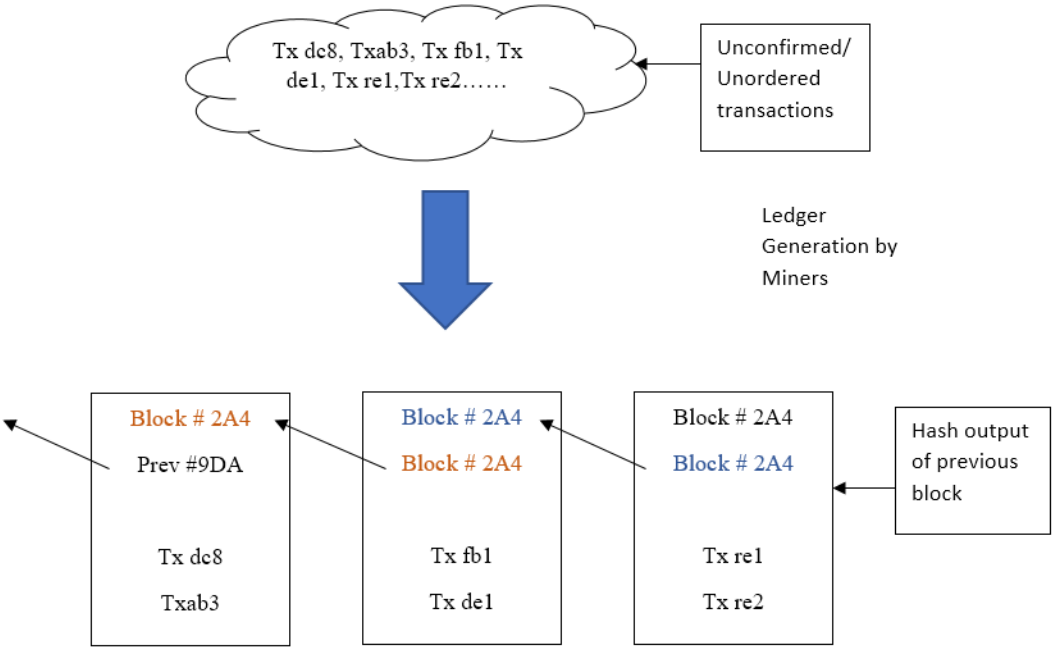

Figure 2.7: Generation of Blockchain from unordered transactions.

2.2.2 Protection of Transaction

As mentioned earlier, all the miners are involved in this race of solving mathematical problems to generate a valid block. Though it is very complicated, it is possible that more than one valid block can be created at any instant in the network. The first node, which solves the problem, appends the block to its ledger and relays it to the rest of the network. Even if there are more than one block solved at the same time and distributed in the network, the complicated computing process ensures that the blockchain stabilizes as every node comes to an agreement to accept the valid blocks.

All the nodes in the network agree on accepting the longest blockchain as the valid one. Hence consensus in only one block and the other blocks are rejected. Due to this property, it is almost impossible to hack the blockchain. As the nodes in the network agree on the block with the longest blockchain as the valid one, an attacker in order to initiate a fraudulent transaction should produce a block by solving a mathematical problem. At the same time, his block must be accepted by the good nodes to generate subsequent blocks to make other nodes accept his transaction. As shown in figure 2.8, an attacker needs to gain consensus of the network to validate a fraudulent transaction in a long chain of blocks, which is possible only if the attacker has a significant amount of control

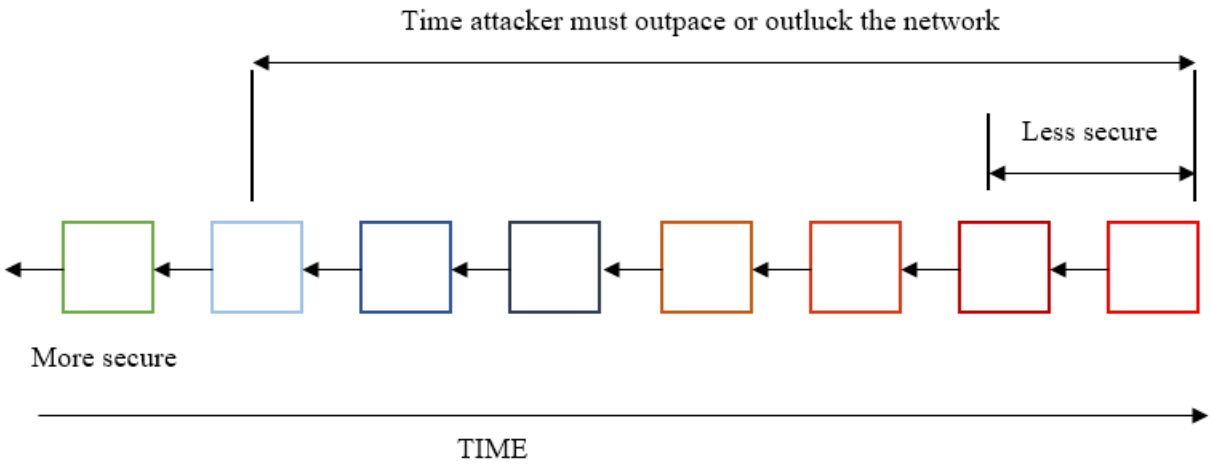

Figure 2.8: Mathematical race to protect transactions.

in the network. Since each block is linked together after encryption, it becomes even more difficult to attack the blockchain database [An117].

2.3 Different types of blockchain technologies

2.3.1 Bitcoin

Satoshi Nakamoto in 2008 released the concept for the first-ever blockchain in his paper "Bitcoin: A Peer-to-Peer Electronic Cash System" [Nak08]. He proposed the bitcoin network which groups together a number of cryptographic elements to create the first ever Peer-to-Peer(P2P) payment system, today known as bitcoin, allowing a user to create a peer to peer exchange of value without a trusted third party in between. Digital wallets, which are also known as bitcoin wallets, are used to execute transactions using private keys. In this system, transactions are recorded in the wallet and ledger. Bitcoin wallets store the private key which is important to access a bitcoin from a transaction and spend it. This model is called a UTXO or Unspent Transaction Output which means, after a transaction, a bitcoin which is not used is transferred back to the user. For a transaction to be valid, there must be one or more UTXOs available. A transaction can be invalid if someone is trying to double spend bitcoin or spend bitcoin which does not exist at all. In Bitcoin, the key gives ownership to bitcoins.

If a user wants to send a bitcoin to another person, he needs to create a bitcoin transaction, then selects a set of UTXOs as input and set the number of bitcoins to transfer. There may be

multiple outputs in the transaction if multiple parties are involved in the payment. As in figure 2.9 a user has 10 BTC in his wallet and wants to send 5 BTC to another user. Now the input to the transaction is 10 BTC, 5 BTC is sent to the other user and remaining 4.9 BTC is sent back to the sender. The remaining difference amount is considered as a transaction fee which is collected by miners. Any valid transaction must have the sum of input greater than the sum of output. The user must sign the transaction using a private key and then broadcast it to the Bitcoin network.

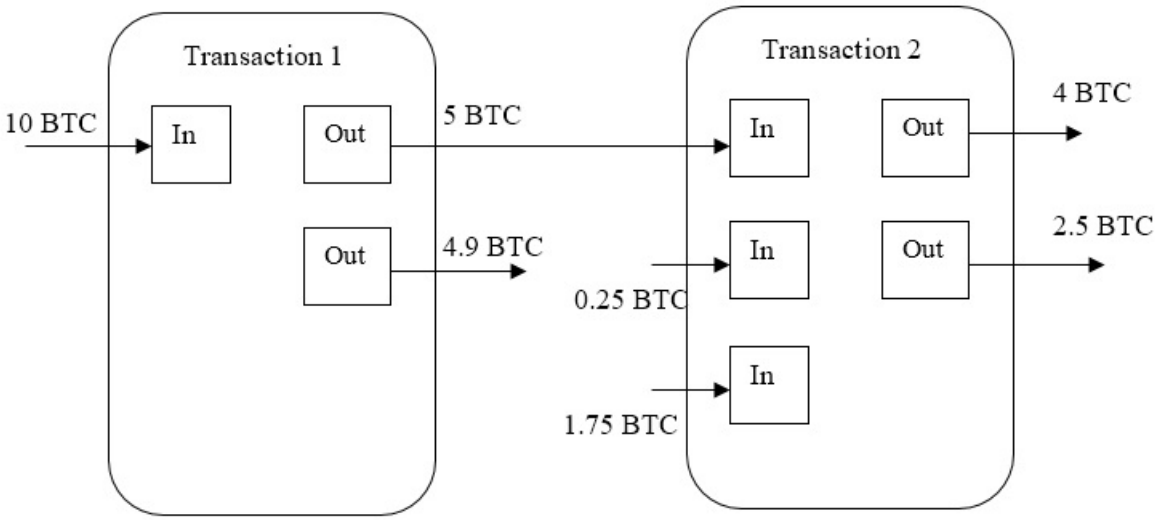

Figure 2.9: A Bitcoin transaction.

Consensus Model

All the transactions after signed by the user are propagated in the distributed network. The transactions are then processed by the nodes in the network, called miners, to validate the transactions executed and group the maximum possible number of transactions in a block. A miner is rewarded with a number of bitcoins for each block discovered in the network in addition to the sum of transaction fees from the transactions. These rewards are automatically credited to the miner's wallet. A block reward on every block generates new bitcoins in the network. To find a block, miners must compete against other miners in the network to solve a difficult mathematical problem, that is finding the nonce value, unique to each block. Without the correct value of nonce, the block cannot be submitted to the network; otherwise, it will be discarded by the network. All the nodes in the network must come to an agreement if the newly found block is valid or not. The Proof-of-

Work gives the correct answer to the nonce value. It helps in creating a trustless consensus in the distributed network, as well as deals with the double spend problem [Nak08]. The difficulty of the network is adjusted dynamically to limit the rate at which a new block can be generated, currently one block in every 10 minutes.

A new block found is appended to the blockchain by a miner in its ledger and is propagated in the network to inform other miners or nodes. Since it takes time for a new block to reach all miners in the network, if some miners were working on a solution but haven't found a new block, they will stop that process, append the new block in their blockchain and start mining for a new one. There may be a chance that another miner may have found the right block. Each miner will work on whichever block they received first, giving rise to a branch in the chain as in figure 2.10. In the network, miners work on consensus to build on the longest valid chain and reward is given only to the block of the longest blockchain. So, a point will be reached where a shorter chain will be dropped eventually, which motivates the miners to work together towards a single chain.

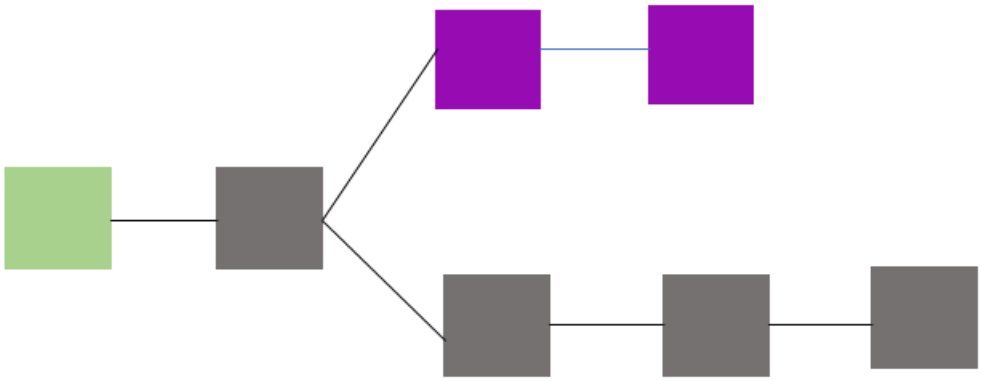

Figure 2.10: Orphan blocks, Stale blocks and Genesis block in the blockchain.

In figure 2.10, the green block is the genesis block. The purple ones are orphaned blocks which are not part of the blockchain. These blocks exist if they are successfully mined but not linked to the longest chain. The brown blocks shown in figure 2.10, except the most recent one, are called stale blocks. These blocks are the ones which already have a legitimate successor. Mining on stale blocks is a waste of energy and money because mining on old data will not be successful in creating a new block[StB, OrB].

The reward for each block started at 50 BTC per block when the bitcoin network began, and it decreases by 50% after every 210,000 blocks are created, which means 25 BTC per block reward is

given after 210,001 blocks in the blockchain. One block is mined every 10 minutes hence 144 blocks per day and 210,000 blocks per 4 years. Hence after every four years, the reward is halved. This reward will continue until all 21 million coins are produced. After that, miners will be rewarded with transaction fee only[Bloa].

The huge amount of computing power required for Proof-of-Work makes it very difficult for an attack on the public ledger, but it is possible if the attacker could manipulate the ledger by controlling 50% of the hash rate, also known as a 51% attack[CrA]. In reality, a 51% attack from a minority group cannot be imagined as the current hash rate hovers around 6354668 TH/s, i.e., Tera Hash per second which is a very huge amount of computing power. An attack can be possible only if the attacker has a huge amount of computing resource to control the network. Sometimes an attacker, not only steals the information from the ledger but also tries to validate their fraudulent transactions. The attacker can also prevent transactions from confirmation, hence giving rise to the double-spending problem.

2.3.2 Ethereum

Ethereum is one of the most popular open source platforms for blockchain technology. It provides a platform to build and distribute decentralized applications. Ethereum provides a platform with a programming language which is used to create smart contracts. It also helps users develop decentralized systems, such as financial systems, social systems, etc. with no requirement of a third party. Ethereum used the concept of blockchain technology and improved it in its own terms. An ethereum platform can also be used to trade money or execute transactions just like bitcoin in a more efficient manner compared to bitcoin [Etha].

Smart contracts

A smart contract can be interpreted as a piece of code which automatically executes terms defined in a contract. There are some conditions configured in the smart contract between the involved parties. If those conditions are met, then the parties involved in the contract can make payments automatically as per condition in the contract maintaining transparency. It is written in Solidity, a programming language, and compiles executable code which runs on EVM, i.e. Ethereum Virtual machine. Contracts are designed by creators, but the execution is managed by the Ethereum network. As long as the ethereum network exists, the smart contract exists and can be executed. Solidity helps in taking care of objects on the Ethereum blockchain, manages contracts, stores data,

makes decisions and sends a number of ether to other parties. Ether is one of the most important elements of Ethereum. It is a form of payment, can be called as cryptocurrency of ethereum, which is used by clients to machines after successful execution of smart contracts[Etha].

EVM

EVM is defined as a distributed computer through which smart contracts are executed. Ethereum implements a technique to control the number of resources used when a smart contract is executed on every machine on the network. In this mechanism, two fields known as STARTGAS and GASPRICE are added in the transaction where STARTGAS represents the maximum number of computational steps the particular transaction can take, and GASPRICE is the value which represents the fee per computational step the sender agrees to pay. GASPRICE is the amount of ether per gas the sender pays. Let's say, X sends Y 1000 gas in 0.001 ether per gas price. Now 1000 * 0.001 =1 ether. So, one ether is decremented from X's account upon the use of the service. Sometimes, a particular computation may not require all the gas. Hence, after completion of the contract, the remaining amount of gas is computed back to a value of ether and returned to X's account. If the computation used up all the gas and exhausted the gas resource, all the state changes are reverted except for the fees. In most of the cases, one gas fee is required for each computation step. Cost depends on computational load as well as the amount of data processed. For every byte of transaction data, a fee of five gas is required. STARTGAS and GASPRICE fields play pivotal roles in avoiding accidental infinite loop in the execution and hence preventing computational wastage. This makes the system more secure and forces attackers to pay for the resource they use to manipulate the computation or data in the network[Etha].

Accounts

In Ethereum, the state of user's balances is stored in structures called accounts which has a 20 bytes address. There are two types of accounts: contract account which is controlled by their code and the externally owned account which is controlled by the user with their private key. Basically, an account in ethereum contains the following fields:

- The account's current ether balance
- The nonce value which is a value which determines that each transaction can only be used once.

- The account's contract code, if it is a contract account
- The account's storage

An externally owned account does not have the code field. It can communicate with other externally owned accounts or contract accounts by message passing through the creation and signing of a transaction. The only contract can produce a message, not an external actor. When a contract invokes code in another contract, a message is generated. A typical message contains the following fields:

- The information of the message sender
- The information of the message recipient
- Amount of ether to transfer
- STARTGAS value
- An optional data field

Generally, the transaction is signed by an external actor and contains a piece of data. Transactions contain the following fields.

- A signature identifying the sender
- The information about the recipient of the message
- A STARTGAS value
- A GASPRICE value
- The amount of ether transferred
- An optional data field

Basically, transactions can be categorized into three types: a normal transaction which contains regular ether transfer, contract creation transaction, and message call transaction to a smart contract.

Ethereum blockchain needs to keep track of states of every account, information between accounts and state transition function values. Every block keeps information of the transaction list and the most recent state where each state is taken care in the form of a tree called as Patricia

tree. In between two adjacent blocks, most of the tree does not change. Therefore, a Patricia tree is excellent to store data once and then referenced using pointers later when needed[Etha].

Consensus model

Mining blocks in the Ethereum is very much like the process in Bitcoin[Ethb]. Miners in the network produce valid block only if they successfully solve a Proof-of-Work difficulty. Compared to bitcoin, Ethereum uses a different hashing algorithm, known as Ethash, where difficulty is changed to achieve consensus among miners and generate one block every 15 seconds[Ethc]. Compared to 10 minutes in bitcoin, Ethereum's 15 second block time is very low. Because of this reason, there is a greater probability that a miner will work on a stale block as blocks take less time to propagate through the network. The Greedy Heaviest Observed Subtree, also called a GHOST protocol, was introduced to tackle the problem of blocks suffering from a high stale rate. Let's say, miner A mines a block slightly faster than B. Due to the delay in propagation, the block mined by A reaches B only after B mines its own block. B's block remains as stale and could be wasted if not taken care of. So, GHOST came up with the idea to include stale blocks, also known as uncle blocks in the blockchain as shown in figure 2.11. As block B2 is mined, the branch containing block B2 is considered as the best chain. If block C1 is the next best block mined to the block B2, it is also included in the chain of B branch as uncle block. Ethereum rewards miner of the uncle block too. This may drive miners towards mining more uncle blocks, which is avoided by limiting the uncle blocks up to seven generations only. Including uncle blocks make chain heavier and secure.

The reward for mining a new block in ethereum is as below:

- Five ether for each new block mined
- Sender compensates the amount of gas that a particular computation requires to execute all transactions within the block
- For each uncle block, 1/32 of the static block is rewarded

2.3.3 Hyperledger Fabric

Hyperledger Fabric is another implementation of the blockchain technology. It is one of the permissioned blockchain platforms where members involved in the network trade or exchange digital assets through execution of transactions controlled by the chaincode. Chaincode is a piece of code

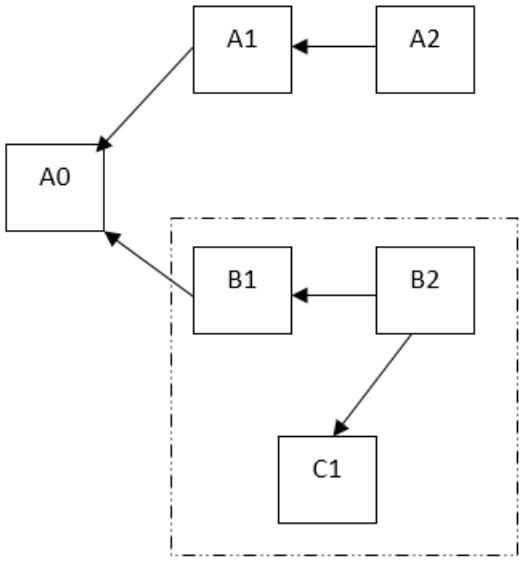

Figure 2.11: Greedy Heaviest Observed Subtree protocol.

installed and executed on the nodes of the Hyperledger Fabric network which enables interaction with the shared ledger. As a permission blockchain, each node in the network is required to maintain the identity of the members. Even the identity of client or end users should be maintained in the network. They need to be authenticated to be involved in any transaction in the network. The transaction and data of the participants in the network are restricted to a separate subset of the network participants also known as a channel. The members of the channel can establish a shared ledger to record transactions and digital assets keeping it within the channel, hence available to members of the channel only. So, there may be multiple subnetworks within a HyperLedger Fabric network and each subnetwork as channel maintains a separate ledger per channel. The ledger is made up of blockchains as well as a state database to maintain the current state which contains the latest values for all keys ever included in the blockchain. The nodes in the network execute transactions against the current state to make chaincode interactions efficient. The state database resides in memory for fast access whereas the blockchain is stored in the file system of the node [TTADO17, Ethd].

The Hyperledger Fabric architecture consists of peer nodes, ordering nodes and client applications. A peer node can deliver two roles: a committer when it maintains the ledger by committing transactions, and an endorser when it endorses the result after simulating the transactions executed by the chaincodes. A peer may be a committer for specific types of transactions while acting as an endorser for others. The ordering nodes take care of the order of the transactions in a block before

committing it to the ledger. This task can be centralized as well as decentralized. The job of peer and ordering nodes is similar to the work that miners do in bitcoin and ethereum.

Transaction flow

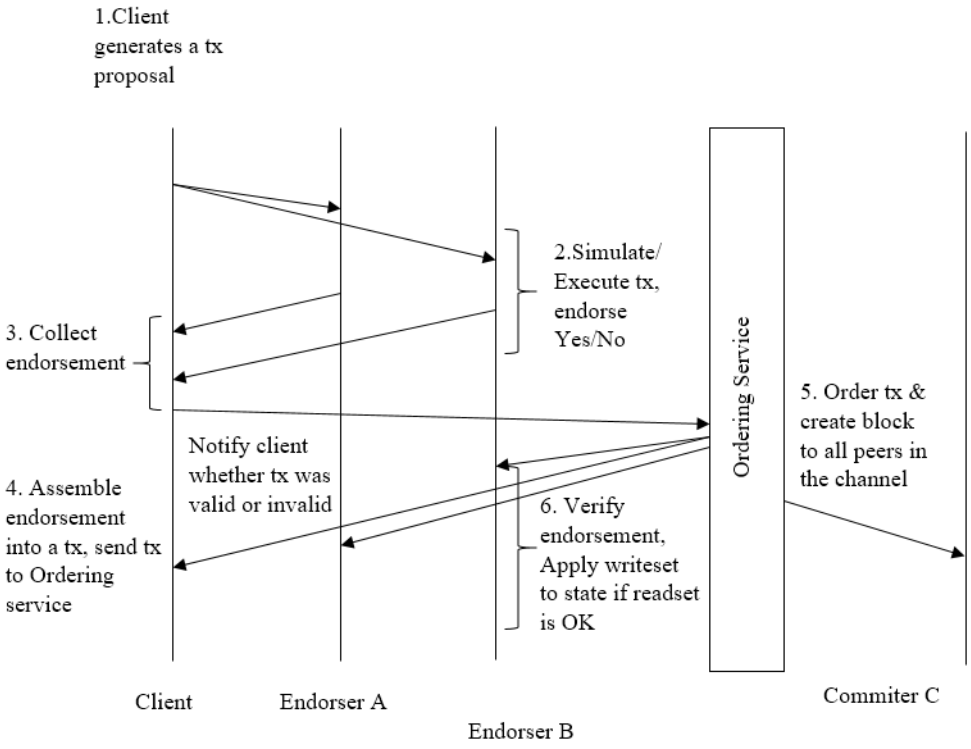

Figure 2.12: Illustration of one possible transaction flow

The figure 2.12 gives basic workflow of a transaction in a Hyperledger Fabric blockchain. It is started with the participation of two or more parties in the network. The participants may be companies or organizations which create and join a channel. First, all the members in the channel need to agree on conditions of the chaincode, because chaincode rules over the execution of transactions as well as the policies regarding channel membership. When an agreement is reached on the chaincode, it is then committed to the ledger. Now an end user or client who has privileges to join the channel can propose transactions to endorsers in the channel. The endorser needs to verify the signature before determining if the user has permission to perform the proposed operation. Endorsers use the transaction proposal as input and execute them against the current state database to produce results which include read set, write set and response value. The results along with endorser's signature and YES/NO endorsement are passed back to the user. The user

checks if the results from the endorsing peer are signed and consistent, then sends the transaction which contains result, endorsement and channel id to the ordering service. The ordering service simply puts one order on channels in a First Come First Served basis into a block. The blocks are then sent to the peers who commit the block into the ledger. Before committing the transactions, the committer needs to validate the transactions with the block to verify that the endorsement policy has been fulfilled, and to check if any changes have been made to read set variables in the ledger state. Every transaction in the block is tagged as being valid or invalid. Only write sets of valid transactions are committed to the current state database after the peer adds the block to the channel's blockchain[HTx].

Read and write set semantics

A read-write set is generated for the transaction as an endorser simulates the transaction. In the process of simulation, the endorser keeps the record of keys used from the state database to read their value as well as their committed versions of that value. A read set keeps a list of the keys and their committed version. The write set keeps a list of keys and their new values that the transaction writes. A delete marker can be set if the update performed by the transaction wants to delete the key. The following lines represented a read-write set prepared by the simulation of a transaction.

```
<TxReadWriteSet name "channelId" >
<read-set >
<read key ="Key1", version ="1" >
<read key ="Key2", version ="1" >
</read-set >
<write-set >
<write key="Key1", value="Value1" >
<write key="Key3", value="Value2" >
<write key="Key4", isDelete="true" >
</write-set >
</TxReadWriteSet >
```

The committer needs to iterate through the block to verify the validity of each transaction after the transactions are ordered in the block. A transaction is valid only if the version of each key in the read set matches the version for the same key in the current state database. For a valid

transaction, the committer then uses the write set to update the current state database, and the version of the key is changed to the latest version.

Endorsement policy

In this process, endorsers execute a transaction and return with a YES/NO response to the end user application or client. All the peers should execute the transactions attached to the specific chaincode. Then policy determines whether that transaction is properly endorsed or not. Depending upon the policy, endorsing from a minimum number of endorsers may be enough, or it may need endorsing from all the endorsers in the channel.

2.3.4 Private vs public blockchain

Blockchain systems can be classified into two categories: public and private. In a public blockchain, any node can participate in the peer-to-peer network, where the blockchain is fully decentralized. A node can leave the network if it wishes without any consent from the other nodes in the network. Bitcoin is one of the most popular examples that fall under public blockchain. In private blockchain, nodes need special access or permission without which they cannot get authentication from the network. Hyperledger is among the most popular private blockchains which allow only permissioned members to join the network after authentication [TTADO17]. Private blockchains due to their more secure nature, have sparked interest in major banking and financial institutions who claim that these platforms can disrupt current conventional centralized systems [MW16].

2.3.5 Applications of Blockchain Technology

Blockchain technology is being widely accepted in both financial and non-financial areas. The financial institutions such as banks and service providers are gradually moving into blockchain technology after it has proved how secure and robust it is. Another application called Smart Contracts brought up by Nick Szabo is 1994 to automatically execute contracts between participating parties found good use after the evolution of cryptocurrency. Now, blockchain and smart contract are coming together to automatically make payments when the pre-configured conditions of the contract are triggered.

Open source platform Ethereum has brought many enthusiasts to use this platform for their purpose. If any institution or group is interested, they can create their own cryptocurrency and use smart contracts to execute transactions. Ethereum is already being recognized and implemented in

wide areas such as banks, governments, financial derivatives trading, and settlement. Big companies such as Amazon, IBM, eBay, UBS, Samsung, etc. are exploring blockchain technology to model into their applications. Goldman Sachs, JPMorgan, UBS, Royal Bank of Scotland, State Street and many other banks have collaborated with New York based financial firm R3 to develop framework using blockchain which can be used in financial applications[ReU].

Financial Applications

Private Securities: To take a company public, banks must work to underwrite deals and attract investors. Then the stock exchanges will list the shares of the company in the market. Trading of stocks is difficult and sometimes slow due to a third party. With the use of blockchain, companies can directly issue shares. Shares can be traded in the market that is implemented based on the blockchain. NASDAQ Private Equity cooperated with a San Francisco based company called chain.com to work on private equity exchange implemented on top of blockchain where blockchain based smart contracts are implemented to exchange functionality[NAS].

Insurance: Any property such as laptops, diamonds, gold, physical assets, and real estate can be registered in the blockchain. Some nodes in the network can work as insurers and validate the ownership and transaction history. This way assets are uniquely identified and difficult to destroy or forge. Everledger, a company based on this concept, uses blockchain to keep records of diamond certification in distributed ledger[ELe]. It records the transaction history of the diamonds along with the characteristics such as height, width, depth, color, etc. The Insurance companies, law enforcement agencies, and owners can verify the diamonds. It provides a web API service to look at a diamond, where insurance companies can create or read or update claims or police reports can be created or updated.

Non-Financial Applications

Notary Public: Blockchain technology can be used to verify the authenticity of a document eliminating the need for a third party as a trusted authority. Various document certification services may be required to determine who authored it, i.e., Proof of Ownership at certain times, Proof of Existence and Proof of Integrity of the documents. Blockchain provides a counterfeit-proof verification of the document and secures the privacy of the document, which eliminates the need for expensive notarization and insecure ways of transferring documents.

Stampery is a company that uses blockchain to stamp any files or emails[StP]. It simplifies

certification of documents by sending it to the email specifically created for each customer. As it is very cost efficient, many law firms have started using Stampery to certify documents. Block Notary, an iOS app, uses blockchain technology to create proof of existence of any content ranging from photo, audio, video to any documents[BN].

Music Industry: Due to the growth of the Internet and various applications boosting the availability of a wide range of streaming services over the Internet, the music industry has grown into the whole new dimension. It is impacting everyone in the music world from artists, publishers, writers to users. The rise of internet service has made music royalties even more complicated to maintain transparency in the payment to the artists and writers. Blockchain can play a vital role to maintain an accurate and comprehensive distributed database of music rights ownership information. Even royalty split for each work can be added to the database where the smart contract can define relationships between various stakeholders and automate their interactions[PT].

Proof of existence of documents: In any legal works, validating documents is very crucial. In the traditional world, the documents are validated by central authorities. As the documents become older, validating documents become more complicated. The blockchain technology can be used as a platform where the user can sign the document with the timestamp to verify proof of existence and possession of legal documents[PE].

Proof of Existence: It is a simple service that uses blockchain technology as a platform allowing users to secure the ownership of the document. This service stores the cryptographic signature of the file, linked to the time in which a user submits his document. Here only a signature is stored, not the document. Later, the user can certify the existence of the document using that signature. This service provides security and privacy, giving the user decentralized proof of the document that can't be modified by a third party. Proof of Existence web service is available at https://proofofexistence.com/.

Decentralized Storage: Various cloud storage solutions such as One Drive, Dropbox, Google Drive are growing popular these days where users can store documents, media files, etc. The major issue related to these services is that a user must trust these third parties with their valuable files and information. There have been various instances where the security of these services has been compromised, and private information of the user has been leaked online which gave the motive to look for a distributed peer-to-peer storage platform.

Storj is a company that provides a blockchain based cloud storage platform on a peer-to-peer network. Using this platform, users can transfer and share data without putting their trust on

a third-party data provider. Here, people in the network share spare disk space on the personal computer and unused bandwidth to store files for which they are remunerated with bitcoins. Storj platform uses a cryptographic solution to check the integrity and availability of the file. Also, a separate blockchain is used for storing metadata about the files stored[Str].

Decentralized Internet of Things: The Internet of Things is becoming a popular technology for both users and service providers. A large number of IoT platforms provides services based on the centralized model. When devices need to exchange data between themselves autonomously, the centralized model becomes less effective. The blockchain technology provides an implementation of decentralized IoT platforms with secure and trusted communication as well as keeping records of all the communication between smart devices within the IoT topology in a distributed ledger. IBM partnered with Samsung to develop a platform ADEPT (Autonomous Decentralized Peer to Peer Telemetry) that uses blockchain technology to build a distributed network of devices, i.e. decentralized Internet of Things (IoT). ADEPT uses three protocols-BitTorrent for Peer-to-Peer file sharing, Ethereum for executing the smart contracts and TeleHash for Peer-to-Peer Messaging in the platform[IBM].

Blockchain based Anti-Counterfeit Solutions: The blockchain technology in the distributed network provides an alternative to conventional anti-counterfeiting mechanisms providing more secured service to merchants and consumers. The blockchain network where brands, merchants, marketplaces are the main players, can be used to validate the authenticity of the products. With the blockchain platform, stakeholders in the supply chain can verify the authenticity of the products by using distributed ledger without depending on the centralized entity.

BlockVerify is one of the blockchain platforms which gives anti-counterfeit solutions and maintain transparency in supply chains[Blob]. Nowadays, it has gained popularity in various fields such as diamonds, pharmaceutical, luxury items and electronics industries.

2.3.6 Summary of blockchains

Types	Bitcoin	Ethereum	HyperLedger Fabric
Purpose	Cryptocurrency	Run smart contracts	Creation of blockchains for industry use cases.
What kind of data can be stored?	Cryptocurrency transactions	Cryptocurrency, digital assets, smart contracts	Chaincode, smart contracts
Scripting Languages	Script	Solidity, Serpent	Go
Is the ecosystem open?	Yes	Yes	No
How can one participate?	Use source code from GitHub, and follow their instructions.	Use source code from GitHub and follow their instruction.	User source code. Register for identity to the network membership services.
Native Currency	Bitcoin(BTC)	Ether (ETH or ETC)	N/A
Who are the registration authorities?	N/A	N/A	Defined before blockchain is initialized
Is decision making transparent?	Yes	Yes	Unknown
Does it use a managed Public Key Infrastructure?	No	No	No
Who manages Public Key Infrastructure?	N/A	N/A	N/A
Block-release Timing	10 minutes	12 secs	Configurable
Transaction Size	250 bytes average	Theoretically no max (actual max: 89KB)	Maximum size configurable
Transaction Rate	3 txns/sec avg.7 txns/sec theoretical maximum	Theoretically no maximum	More than 10,000 transactions/sec
Mining	Proof of Work	Proof of Work using Ethash algorithm	N/A

Table 2.1: Comparison of blockchain technnologies.

Chapter 3

Performance Analysis

Two public blockchain platforms, Bitcoin and Ethereum, were compared based on their performance over the period of two years from May 2016 to April 2018. Parameters such as Block time, Block size, No of Transactions and difficulty were used to compare between these two platforms. Also, two private blockchain platforms, Hyperledger Fabric and Ethereum, were compared based on throughput performance.

Throughput: In blockchain technology, throughput can be defined in terms of a number of transactions confirmed per second. Most of the modern payment processing systems like Visa has an average throughput of 2000 transactions per second. Performance of ethereum and Hyperledger fabric were compared in term of average throughput.

We compared Ethereum and Hyperledger Fabric by creating a network of 5 nodes using 5 Amazon ec2 instances (t2. small instances). For each platform, blockchain nodes were deployed by downloading and installing appropriate software, which were Ethereum's Geth and Hyperledger Fabric.

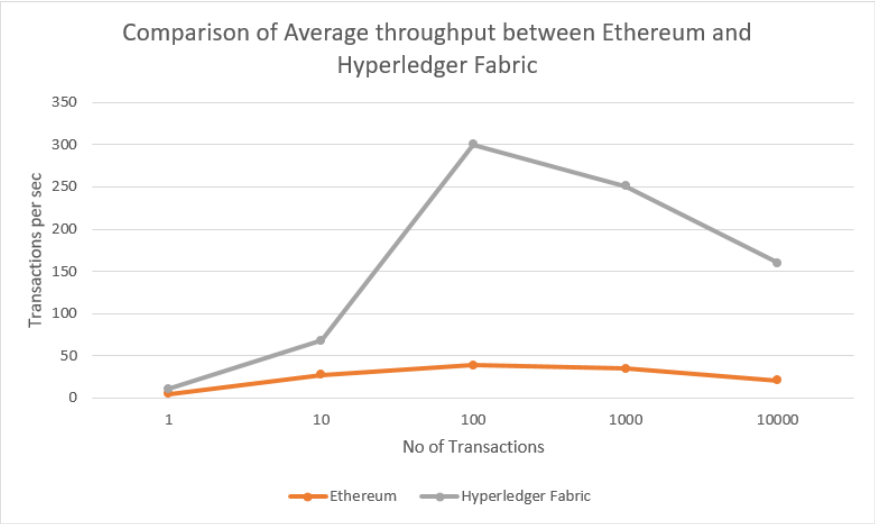

Figure 3.1: Average throughput Comparison between Ethereum and Hyperledger Fabric

Figure 3.1 shows the comparison of average throughput in five sets of different experiments for each platform. Average throughput of Hyperledger Fabric is clearly higher than Ethereum. We can see that Hyperledger Fabric can process up to 300 transactions per second in a given network compared to around 40 transactions per second by Ethereum in the same network.

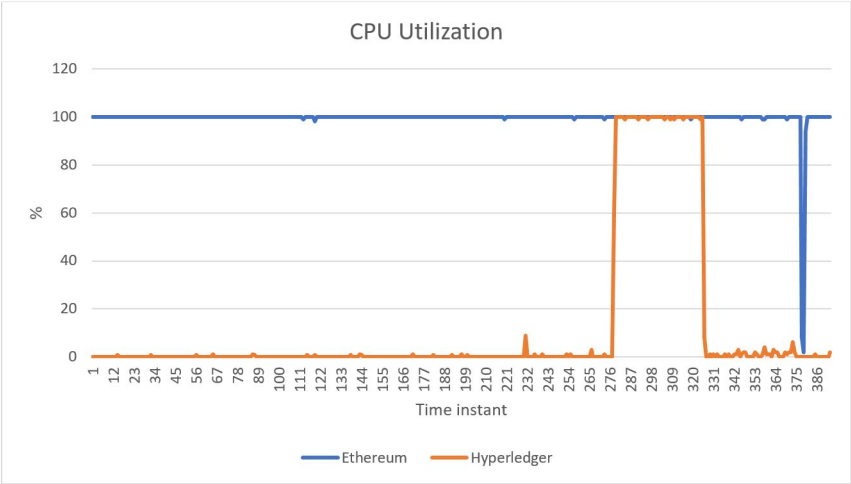

Figure 3.2: CPU Utilization Comparison between Ethereum and Hyperledger Fabric

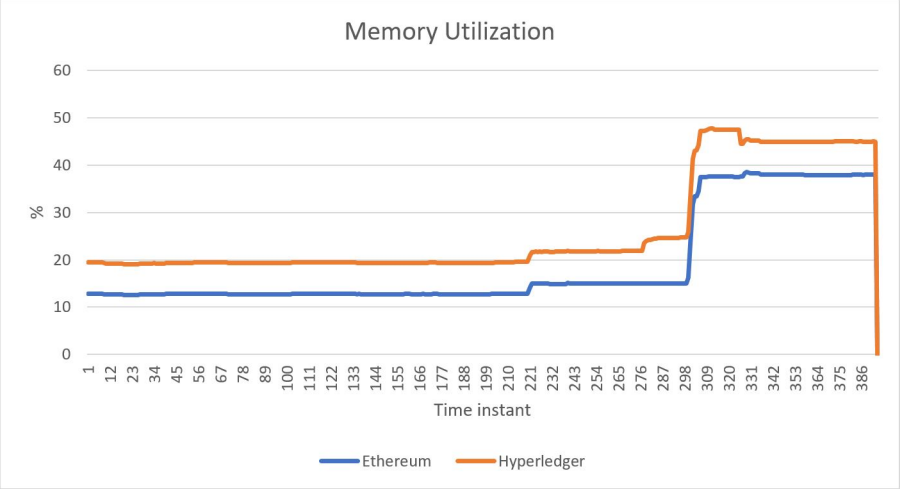

Figure 3.3: Memory Utilization Comparison between Ethereum and Hyperledger Fabric

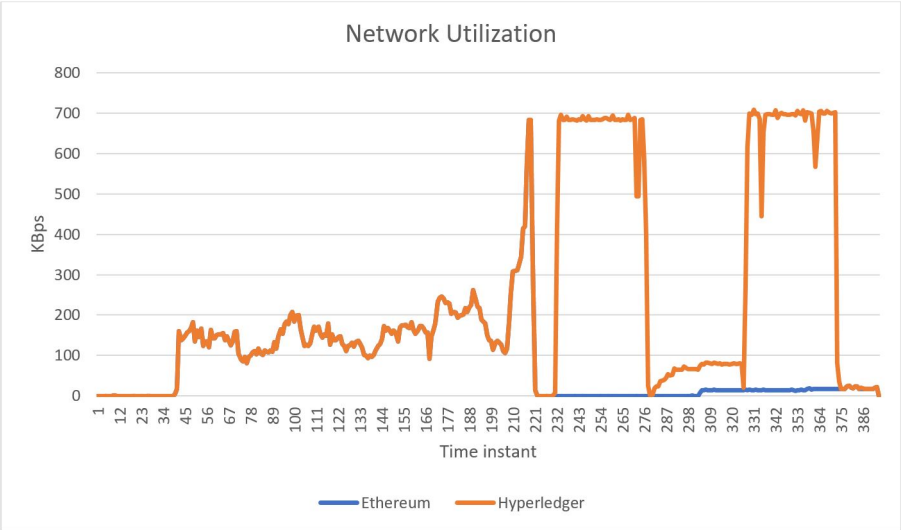

Figure 3.4: Network Utilization Comparison between Ethereum and Hyperledger Fabric

Figure 3.2, 3.3 and 3.4 compare Ethereum and Hyperledger Fabric on the basis of CPU usage, Memory Usage, and Network Usage. From the results, we can say that the Ethereum is CPU heavier platform than Hyperledger. Hyperledger requires more Memory and Network resources compared to Ethereum.

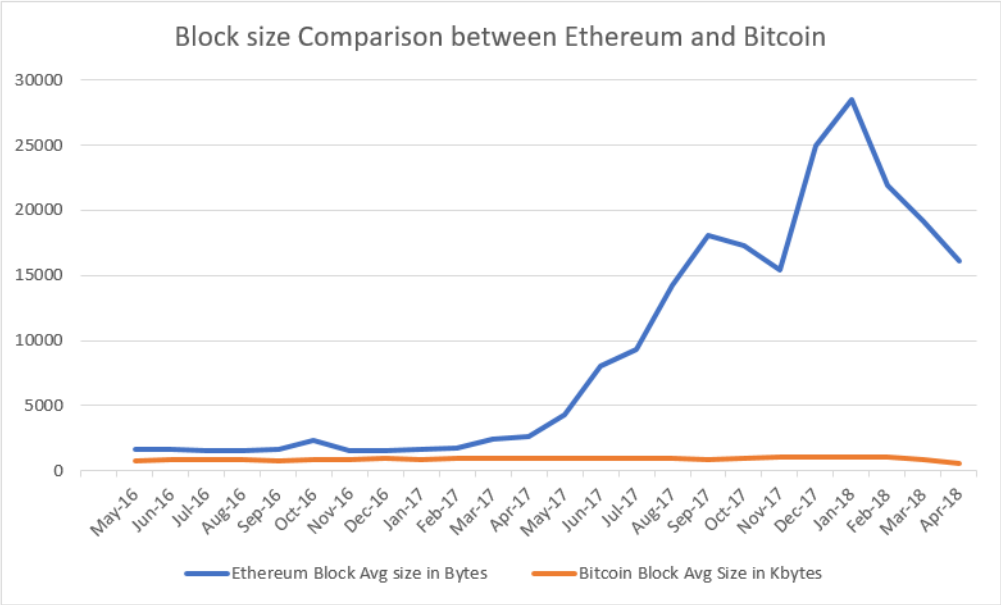

Figure 3.5: Block Size Comparison between Ethereum and Bitcoin

The block size of Bitcoin is designed to be less than 1MB, while the size of an Ethereum block can vary depending upon the number of transactions it includes. From figure 3.5, we can tell that the size of Bitcoin remained on average 1MB while the size of an Ethereum block varied from 2000 Bytes to around 28000 Bytes in the span of two years.

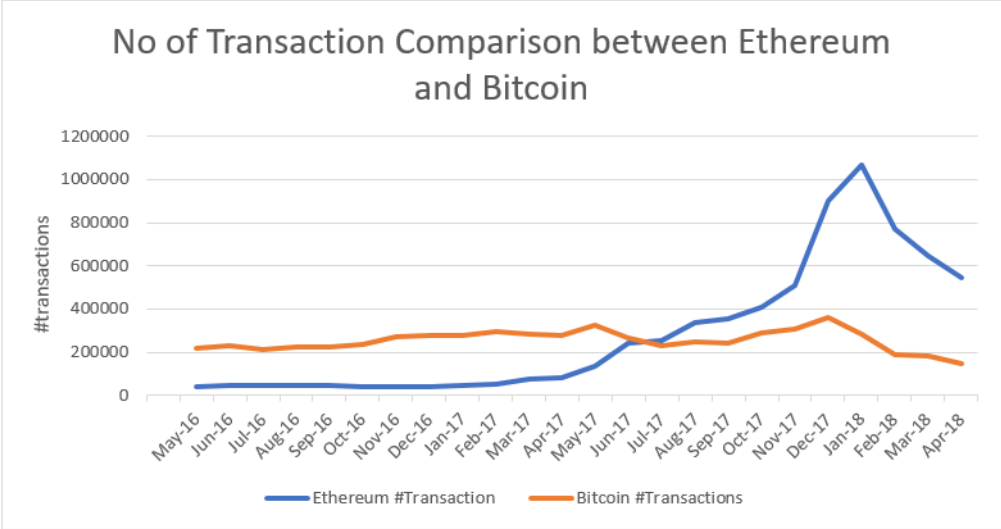

Figure 3.6: No of Transactions Comparison between Ethereum and Bitcoin

Figure 3.6 shows that Ethereum has become popular compared to Bitcoin over the period of two years as more and more users are using the Ethereum platform.

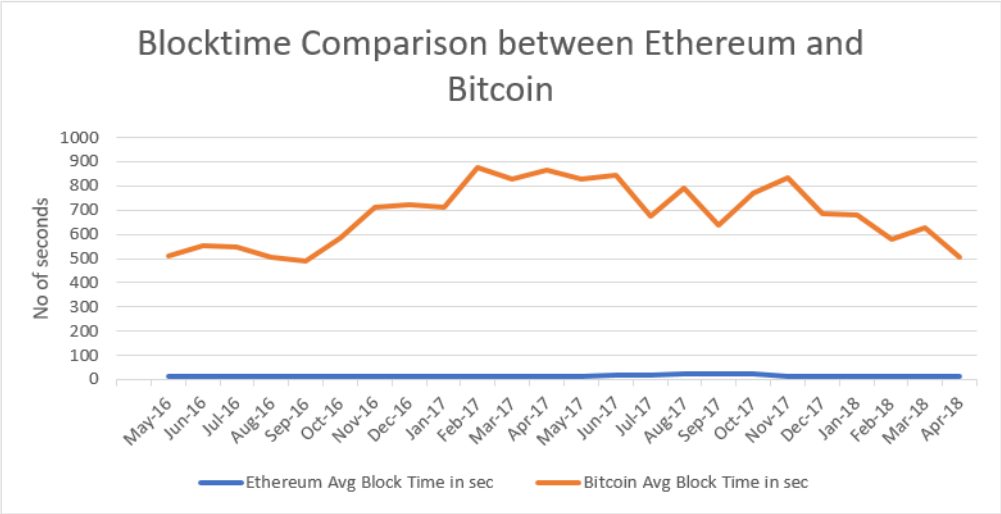

Figure 3.7: Block time comparison between Ethereum and Bitcoin

From Figure 3.7 we can tell that Ethereum takes very much less time, around 15 seconds, to generate a block while Bitcoin needs 600 seconds or 10 minutes on average to generate a block.

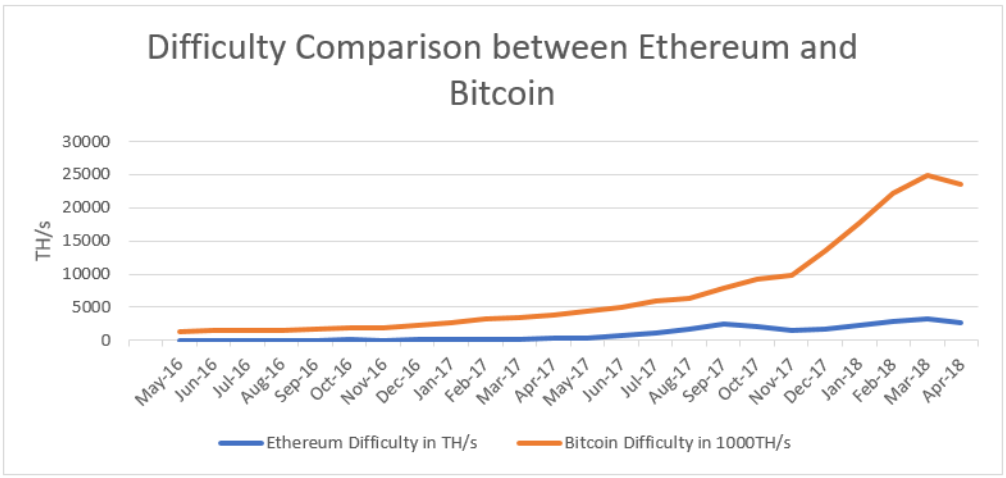

Figure 3.8: Difficulty Comparison between Ethereum and Bitcoin

As more and more miners are attracted to mine lucrative bitcoin, the complexity to generate a new block has grown exponentially. Figure 3.8 shows the comparison between the difficulty of generating a new block between Ethereum and Bitcoin. Bitcoin difficulty rose as high as 25 million TeraHash per second. The difficulty of mining a block in Ethereum blockchain is also growing, but not much as compared to Bitcoin.

Chapter 4

Discussion

After the comparative study, it is obvious that the blockchain platforms have their own issues with performance and scalability. A platform which may be better at one application may not perform better on other applications. Permissioned or private blockchains such as Hyperledger have better performance compared to public blockchains. Bitcoin is the most complicated blockchain with the scalability issue. Ethereum can be implemented as a public as well as a private blockchain. Both types of Ethereum have benefits as well as drawbacks. There are various constraints involved in comparing these various platforms.

The following sections describe techniques to improve performance and scalability in Bitcoin, Ethereum, and Hyperledger Fabric.

Bitcoin: The rise and popularity of Bitcoin after being widely accepted as a cryptocurrency around the world had raised some concerns over its performance. The main problem of bitcoin is its ability to scale as it is restricted to a maximum number of transactions because of its block size. Each block, generated in around 10 minutes, can accommodate around 500 transactions with size reaching up to 1MB. In recent years, the block size has reached the maximum of 1MB which limits the transaction throughput to 2-4 transaction/sec. Currently, there are more than 24 million wallet-users, which gives ten transactions per year each user on average can send in the network[WU]. Only ten transactions each year makes it difficult for financial services to adopt it. The situation could get worse if the number of users is increased. This may lead to increase in the transaction fees as an incentive to miners to verify transactions with higher transaction fees. Unless we find a solution to this congestion problem, delay of transactions being verified on the blockchain will continue.

One of the solution could be by increasing the size of the block, but it must be agreed upon

by all the miners in the network. It has been discussed among the community to change the size of the block which can be done by a hard fork. Any change made in Bitcoin protocol that makes it less restrictive is a hard fork. Growing the size of the block may increase the computing resources to solve the Proof-of-Work problem. The other solution could be micropayments. In the real world, some parties involve in a number of transactions every day. Instead of propagating all the transactions in the distributed network, a micropayment channel can be created between two parties, and they can send as many transactions as they like through this channel. So, in the end, only one net transaction between two parties needs to be recorded in the blockchain, which allows Bitcoin to scale up to millions of transactions per day.

Ethereum: In Ethereum, every node must participate in processing the transactions and record the entire state of every account balance, contract code, etc. This provides security but limits the scalability where the number of nodes processing transactions together can't perform better compared to a single node. One possible solution is to form a new rule, where only certain predefined group of nodes take part in verification of transactions. There must be a sufficient number of nodes to verify each transaction to make system secure and allow parallel processing of the transactions. This method is known as Sharding. In this method, the global state of accounts is divided into smaller groups known as shards. Each shard maintains its own history of transactions and the effect of a transaction is limited to the state of a particular shard. However, the transactions across shards can be achieved with debit and credit kind of transactions to achieve overall consensus[Ethd].

Hyperledger Fabric: Hyperledger Fabric is completely different from Bitcoin as it is used as a permissioned blockchain. In this system, different types of nodes with their respective responsibilities can be configured in a network of nodes to scale independently. There is no parallel relationship between the number of peers and orderers in the network. Endorsers and committers can be added without adding corresponding orderers. Chaincodes can be installed on disjointed endorsers thus giving partitioning of chaincodes between endorsers and allowing parallel execution of chaincode. Also, endorsers involved in heavy computation will not be affected after being apart from the ordering service. The ordering service takes care of the ordering of transactions and double spending. So, endorsers can push through as many transactions as possible. Developers can write their own complex applications without disrupting the ordering, endorsing and committing activity in the network.

Chapter 5

Conclusion and Future works

There are numerous Blockchain platforms available, but not all of them have reached stable design, established user base and implementation. Ethereum and Hyperledger Fabric are most developed and mature blockchain platforms. So, we chose these platforms for our comparison analysis study. These platforms can be analyzed on the basis of various metrics, but we used throughput and resource utilization only.

From our analysis, we found Ethereum CPU intensive compared to Hyperledger Fabric, while Hyperledger Fabric was found more Memory intensive and network intensive. Compared to Ethereum, Hyperledger Fabric fared better in terms of throughput. We got rather a low throughput for both Ethereum and Hyperledger Fabric. However, these results do not reflect actual performances. If powerful machines with huge computing power could be deployed, both platforms could handle thousands of transactions per second. It is hard to test the performance of a distributed system with limited resources. If we could run the experiment with several powerful computers connected in a network, then we may be able to evaluate the maximum throughput of each platform.

From the result, it can be said that Hyperledger Fabric is much faster and scalable than both Bitcoin and Ethereum. For many enterprise and financial institutions, Hyperledger Fabric can meet the business requirements that are impossible to meet with a public blockchain. Hyperledger Fabric can certainly outperform other blockchain platforms, but it would be interesting to see how it would fare compared to the centralized systems used today.

In future, as more platforms become stable and mature, a number of metrics such as throughput, latency, scalability, fault tolerance and security could be defined to benchmark the platforms. It will give a better picture of the performance of the blockchain platforms and help to decide which platform performs better for any particular application.

Bibliography

[AKP15] E. Shi Z. Wen A. Kosba, A. Miller and C. Papamanthou. The blockchain model of cryptography and privacy-preserving smart contracts. *Cryptology ePrint Archive*, 2015.

[An117] *Mastering Bitcoin-Programming the open Blockchain.* OReilly Media, 2017.

[BAp] www.blockchain.info/api [Online, Accessed April 2, 2018].

[Bit15] Understanding Bitcoin. Time, clocks and the orderings of events in a distributed system. *Wiley Finance Series*, 2015.

[Bloa] https://en.bitcoin.it/wiki/Block [Online, Accessed March 15, 2018].

[Blob] http://www.blockverify.io/ [Online, Accessed March 3,2018].

[BN] https://www.blocknotary.com/ [Online, Accessed March 3,2018].

[CoB] https://developers.coinbase.com/docs/wallet/coinbase-connect/two-factor-authentication [Online, Accessed March 15, 2018].

[CrA] https://learncryptography.com/cryptocurrency/51-attack [Online, Accessed March 15, 2018].

[DS14] A. Britto D. Schwartz, N. Youngs. The ripple protocol consensus algorithm. 2014.

[ELe] https://www.everledger.io/ [Online, Accessed March 3,2018].

[Etha] https://github.com/ethereum/wiki/wiki/White-Paper [Online, Accessed March 15, 2018].

[Ethb] https://github.com/ethereum/wiki/wiki/Mining [Online, Accessed March 15, 2018].

[Ethc] https://github.com/ethereum/wiki/wiki/Ethash [Online, Accessed March 15, 2018].

[Ethd] https://github.com/ethereum/wiki/wiki/Sharding-FAQ [Online, Accessed March 15, 2018].

[FT16] B. Scheuermann F. Tschorsch. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communication Surveys & Tutorials*, 18, 2016.

[Hin17] Zane Hintzman. Comparing blockchain implementations. *SCTE/ISBE EXPO*, 2017.

[HTx] http://hyperledger-fabric.readthedocs.io/en/latest/txflow.html [Online, Accessed March 15, 2018].

[IBM] Empowering the edge practical insights on a decentralized internet of things. *IBM*.

[IER16] E. Sirer I. Eyal, A. Gencer and R. Renesse. Bitcoin-ng: A scalable blockchain protocol. *USENIX The Advanced Computing Systems Association*, 2016.

[KNS15] A. Miller K. Nayak, S. Kumar and E. Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. *IACR Cryptology ePrint Archive*, 2015.

[LL82] M. Pease L. Lamport, R. Shostak. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 1982.

[MCK15] P. Pattanayak S. Verma M. Crosby, Nachiappan and V. Kalyanaraman. Blockchain technology beyond bitcoin. *Sutardja Center for Entrepreneurship and Technology*, 2015.

[MCR] https://bitinfocharts.com/comparison/marketcap-btc-xrp.html [Online, Accessed April 2, 2018].

[MW16] J. Morgan and O. Wyman. Unlocking economic advantage with blockchain. a guide for asset managers. 2016.

[Nak08] S. Nakamoto. A peer-to-peer electronic cash system. 2008.

[NAS] https://www.nasdaqprivatemarket.com/ [Online, Accessed March 3,2018].

[OrB] https://bitcoin.org/en/glossary/orphan-block [Online, Accessed March 3,2018].

[PE] https://proofofexistence.com/ [Online, Accessed March 3,2018].

[PT] http://peertracks.com/ [Online, Accessed March 3,2018].

[RB] https://coincentral.com/ripple-vs-bitcoin/ [Online, Accessed April 2, 2018].

[ReU] http://www.reuters.com/article/2015/09/15/us-banks-blockchain-idUSKCN0RF24M20150915 [Online, Accessed March 3, 2018].

[Rip] https://ripple.com/xrp/ [Online; accessed April 2, 2018].

[StB] https://bitcoin.org/en/glossary/stale-block [Online, Accessed March 3,2018].

[StP] https://stampery.com/ [Online, Accessed March 3,2018].

[Str] https://storj.io/ [Online, Accessed March 3,2018].

[TTADO17] G. Chen L. Rui K.-L. Tan T. T. A. Dinh, J. Wang and B. C. Ooi. Blockbench: a benchmarking framework for analyzing private blockchains. *SIGMOD*, 2017.

[WU] https://blockchain.info/charts/my-wallet-n-users [Online, Accessed March 15, 2018].

Curriculum Vitae

Graduate College

University of Nevada, Las Vegas

Pradip S. Maharjan

Degrees:

Bachelor of Computer Engineering 2012

Tribhuvan University, Nepal

Thesis Title: Performance Analysis of Blockchain Platforms

Thesis Examination Committee:

Chairperson, Dr. Ajoy K. Datta, Ph.D.

Committee Member, Dr. John Minor, Ph.D.

Committee Member, Dr. Laxmi Gewali, Ph.D.

Graduate Faculty Representative, Dr. Emma E. Regentova, Ph.D.