VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Jnana Sangama, Belgavi-590018

A TECHNICAL SEMINAR REPORT

On

"An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends"

Submitted in partial fulfilment of the requirement for the degree of

BACHELOR OF ENGINEERING

In

COMPUTER SCIENCE & ENGINEERING

Submitted by

T N VARSHA **(1RG16CS103)**

Under The Guidance of

Mrs. Geetha Pawar

Asst Professor, Dept of CSE

RGIT, Bengaluru-32

Department of Computer Science & Engineering

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

Cholanagar, R.T.Nagar Post, Bengaluru-560032

2019-2020

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

(Affiliated to Visvesvaraya Technological University)

Cholanagar, R.T.Nagar Post, Bengaluru-560032

Department of Computer Science & Engineering

CERTIFICATE

This is to certify that the seminar report titled **"An overview of blockchain technology: Architecture, consensus and future trends"** is a bonafide work carried out by **Ms. T N Varsha (USN 1RG16CS103)** in partial fulfilment for the award of **Bachelor of Engineering** in **Computer Science and Engineering** under **Visvesvaraya Technological University, Belgavi**, during the year **2019-2020.** It is certified that all corrections/suggestions given for Internal Assessment have been incorporated in the report. This technical seminar report has been approved as it satisfies the academic requirements in respect of technical seminar work prescribed for the said degree.

Signature of Guide	Signature of HOD
Mrs.Geetha Pawar	**Mrs. Arudra A.**
Asst. Professor	Assoc. Professor & HOD
Dept. of CSE,	Dept. of CSE,
RGIT, Bengaluru	RGIT, Bengaluru

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Jnana Sangama, Belgavi-590018

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DECLARATION

I hereby declare that the technical seminar report entitled **"An overview of blockchain technology: Architecture, consensus and future trends"** submitted to the **Visvesvaraya Technological University, Belagavi** during the academic year **2019-2020**, is record of an original work done by me under the guidance of **Mrs Geetha pawar,** Asst Professor, Department of Computer Science and Engineering, RGIT, Bengaluru in the partial fulfillment of requirements for the award of the degree of **Bachelor of Engineering** in **Computer Science & Engineering.** The results embodied in this technical seminar report have not been submitted to any other University or Institute for award of any degree or diploma.

T N Varsha **(1RG16CS103)**

ACKNOWLEDGEMENT

I take this opportunity to thank my college **Rajiv Gandhi Institute of Technology, Bengaluru** for providing me with an opportunity to carry out this technical seminar report work.

I express my gratitude to **Dr. Nagaraj A M**, Principal, RGIT, Bengaluru and to **Dr. D G Anand**, Rector, RGIT, Bengaluru for providing the resources and support without which the completion of this seminar would have been a difficult task.

I extend my sincere thanks to **Mrs. Arudra A**, Associate Professor and Head, Department of Computer Science and Engineering, RGIT, Bengaluru, for being a pillar of support and encouraging me in the face of all adversities.

I would like to acknowledge the thorough guidance and support extended towards me by **Mrs. Geetha Pawar**, Assistant Professor Dept of CSE, RGIT, Bengaluru and **Mrs.Soniya Komal V**, Assistant Professor Dept of CSE, RGIT, Bengaluru. Their incessant encouragement and valuable technical support have been of immense help. Their guidance gave me the environment to enhance my knowledge and skills and to reach the pinnacle with sheer determination, dedication and hard work.

I also want to extend my thanks to the entire faculty and support staff of the Department of Computer Science and Engineering, RGIT, Bengaluru, who have encouraged me throughout the course of the Bachelor's Degree.

I want to thank my family for always being there with full support and for providing me with a safe haven to conduct and complete my technical seminar. I will ever grateful to them for helping me in these stressful times.

Lastly, we want to acknowledge all the helpful insights given to me by all my friends during the course of this technical seminar.

T N VARSHA **(1RG16CS103)**

ABSTRACT

Blockchain, the foundation of Bitcoin, has received extensive attentions recently. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However,there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome.This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architecture firstly and compare some typical consensus algorithms used in different blockchains. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possible future trends for blockchain.The technology that has had the most impact on our lifestyles in the last decade is Blockchain. A word that often arises when talking about Blockchain is Bitcoin. Many people still confuse Blockchain with Bitcoin; however, they are not the same. Bitcoin is just one of many applications that use Blockchain technology. In this paper, the authors conduct a survey of Blockchain applications using Blockchain technology and the challenges these face.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

CHAPTER 1

INTRODUCTION

Blockchain is a form of database storage that is non-centralized, reliable, and difficult to use for fraudulent purposes. Bitcoin, on the other hand, is a form of digital currency that uses a Blockchain public ledger to make transactions across peer to peer networks. Bitcoin is just one of the financial applications that use Blockchain technology, there are also others such as smart contract and hyperledger.Blockchain technology can therefore be used to create many applications.

Nowadays cryptocurrency has become a buzzword in both industry and academia. As one of the most successful cryptocurrency, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016 . With a specially designed data storage structure, transactions in Bitcoin network could happen without any third party and the core technology to build Bitcoin is blockchain, which was first proposed in 2008 and implemented in 2009 . Blockchain could be regarded as a public ledger and all committed transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency.Since it allows payment to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment. Additionally, it can also be applied into other fields including smart contracts , public services , Internet of things (IoT) , reputation systems and security services. Those fields favor blockchain in multiple ways. First of all, blockchain is immutable. Transaction cannot be tampered once it is packed into the blockchain. Businesses that require high reliability and honesty can use blockchain to attract customers.Besides, blockchain is distributed and can avoid the single point of failure situation. As for smart contracts, the contract could be executed by miners automatically once the contract has been deployed on the blockchain.

Therefore the tradeoff between block size and security has been a tough challenge. Secondly, it has been proved that miners could achieve larger revenue than their fair share through selfish mining strategy . Miners hide their mined blocks for more revenue in the future. In that way, branches could take place frequently, which hinders blockchain development. Hence some solutions need to be put forward to fix this problem. Moreover, it has been shown that privacy leakage could also happen in blockchain even users only make transactions with their public key and private key. Furthermore, current consensus algorithms like proof of work or proof of stake are facing some serious problems.

Contrast to , our paper focuses on state-of-art block chain researches including recent advances and future trends. The rest of this paper is organized as follows. Chapter 2 introduces blockchain architecture. Chapter 3 shows typical consensus algorithms used in blockchain. Chapter 4 summarizes the technical challenges and the recent advances in this area. Chapter 5 discusses some possible future directions and Chapter 6 concludes the paper. Blockchain is a database used for storage in a decentralized network. However Blockchain is not only used in financial applications. Moreover, we can design a transaction to match our application. In this section we will discuss Blockchain technology.

1.2 Technical Terms

First, it is important to clarify the meaning of several technical terms relating to Blockchain. Table 1.1 provides a list of these terms and their meaning.

Term	Description
Decentralized	The system that stores data across the network.
Transparent	Everyone in the node and can see the ledger that share amount decentralized network
Miner	Transaction verifier
Consensus	A v method used to verify the transaction.
Forks	The problem that arises when the node is used for different version of Block chain.
Hash	One-way hash function to check the integrity of a transaction or message.
Node	The ledger in the Block chain system.
Timestamp	A date and time in the computer system used as an electronic time stamp for the transaction.

Table 1.1 Technical terms

1.3 Bitcoin

The Bitcoin was invented by an unknown group or person under the pseudonym Satoshi Nakamoto as stated in "Bitcoin:A peer-to-peer electronic cash system.", a research study completed after the United States Subprime mortgage crisis in 2008. CNN Money define Bitcoin as "...a new currency that was created in 2009 by an unknown person using the alias Satoshi Nakamoto. Transactions are made with no middle men.There are no transaction fees and no need to give your real name. Wikipedia, on the other hand describe Bitcoin as a worldwide cryptocurrency and digital payment system called the first decentralized digital currency, as the system works without a central repository or single administrator .Thus, we can infer that Bitcoin is a cryptocurrency and digital payment system that is decentralized with no middle men and no transaction fees, however the miners will get their reward if they can prove the transaction, otherwise known as proof of work (PoW) or Proof of Stake (PoS).

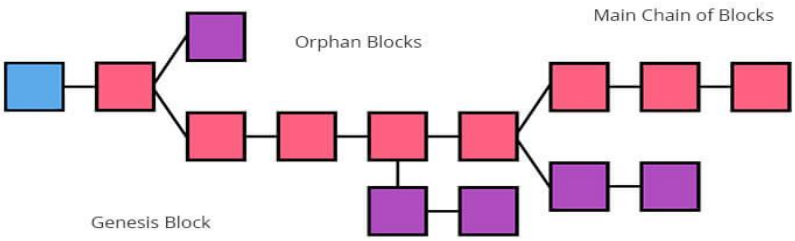

Figure 1.1 Bitcoin

1.4 Blockchain

A decentralized and distributed digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network." Figure 1 describes a formation of Blockchain where the longest chain,called the main chain (active chain), comes from the genesis block and the orphan block is the block that exists outside the main block. According to Christian Cachin et al.the Blockchain has 4 elements that are replicated: the ledger, cryptography, consensus and business logic.

BLOCKCHAIN ARCHITECTURE

CHAPTER 2

BLOCKCHAIN ARCHITECTURE

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. Figure 2.1 illustrates an example of a blockchain. With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks(children of the block's ancestors) hashes would also be stored in ethereum blockchain. The first block of a blockchain is called genesis block which has no parent block.

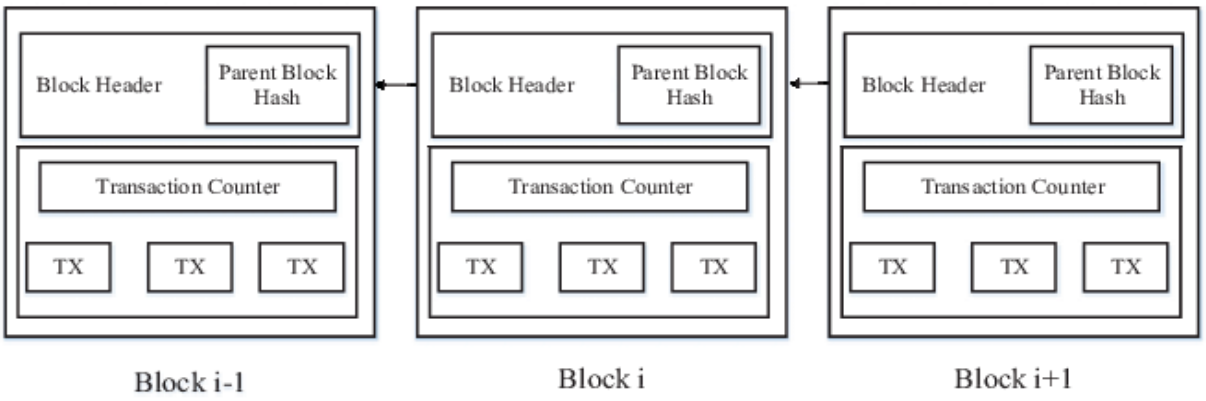

Figure 2.1 An example of blockchain which consists of a continuous sequence of blocks.

2.1 Block

A block consists of the block header and the block body as shown in Figure 2.2. In particular, the block header includes:

(i) Block version: indicates which set of block validation rules to follow.

(ii) Merkle tree root hash: the hash value of all the transactions in the block.

(iii) Timestamp: current time as seconds in universal time since January 1, 1970.

(iv) nBits: target threshold of a valid block hash.

(v) Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation (will be explained in details in Chapter 3).

(vi) Parent block hash: a 256-bit hash value that points to the previous block.

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions.

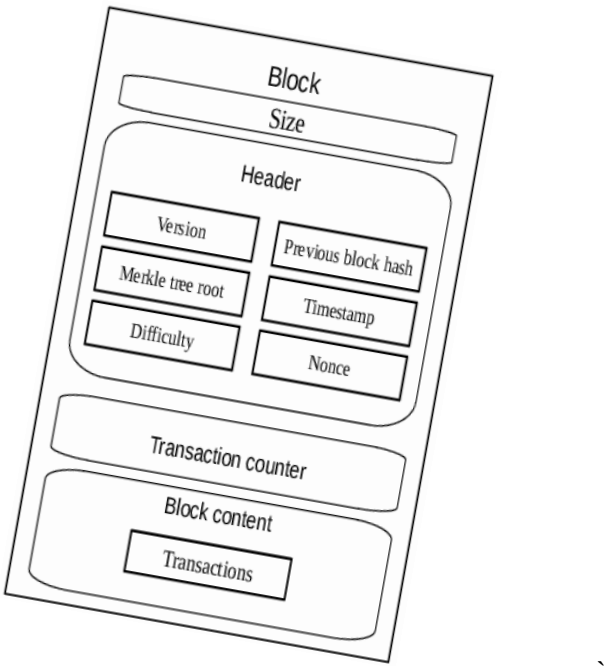

Figure 2.2 Block Structure

2.2 Digital Signature

Each user owns a pair of private key and public key.The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: signing phase and verification phase. For instance, an user Alice wants to send another user Bob a message.

(1) In the signing phase, Alice encrypts her data with her private key and sends Bob the encrypted result and original data.

(2) In the verification phase,Bob validates the value with Alice's public key. In that way,Bob could easily check if the data has been tampered or not.

The typical digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm (ECDSA).

2.3 Key Characteristics of Blockchain

In summary, blockchain has following key characteristics.

* Decentralization.

In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized

mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.

* Persistency.

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

* Anonymity.

Each user can interact with the blockchain with a generated address, which does not reveal thereal identity of the user. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint

*Auditability

Bitcoin blockchain stores data about user balances based on the Unspent Transaction Output (UTX-O) model [2]: Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switch from unspent to spent. So transactions could be easily verified and tracked.

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

Table 2.1 Comparison among public blockchain, consortium blockchain and private blockchain

2.4 Taxonomy of blockchain systems

Current blockchain systems are categorized roughly into three types: public blockchain, private blockchain and consortium blockchain . In public blockchain, all records are visible to the public and everyone could take part in the consensus process. Differently, only a group of pre-selected nodes would participate in the consensus process of a consortium blockchain. As for private blockchain, only those nodes that come from one specific organization would be allowed to join

the consensus process. A private blockchain is regarded as a centralized network since it is fully controlled by one organization. The consortium blockchain constructed by several organizations is partially decentralized since only a small portion of nodes would be selected to determine the consensus.

*Consensus determination.

In public blockchain, each node could take part in the consensus process. And only a selected set of nodes are responsible for validating the block in consortium blockchain. As for private chain, it is fully controlled by one organization and the organization could determine the final consensus.

*Read permission.

Transactions in a public blockchain are visible to the public while it depends when it comes to a

private blockchain or a consortium blockchain.

*Immutability.

Since records are stored on a large number of participants, it is nearly impossible to tamper transactions in a public blockchain. Differently, transactions in a private blockchain or a consortium blockchain could be tampered easily as there are only limited number of participants.

*Efficiency.

It takes plenty of time to propagate transactions and blocks as there are a large number of nodes

on public blockchain network. As a result, transaction throughput is limited and the latency is high. With fewer validators, consortium blockchain and private blockchain

could be more efficient.

* Centralized.

The main difference among the three types of blockchains is that public blockchain is decentralized,consortium blockchain is partially centralized and private blockchain is fully centralized as it is controlled by a single group.

* Consensus process

. Everyone in the world could join the consensus process of the public blockchain. Different

from public blockchain, both consortium blockchain and private blockchain are permissioned. Since public blockchain is open to the world, it can attract many users and communities are active. Many public blockchains emerge day by day. As for consortium blockchain,it could be applied into many business applications. Currently Hyperledger is developing business consortium blockchain frameworks. Ethereum also has provided tools for building consortium blockchains .

CONSENSUS ALGORITHMS

CHAPTER 3

CONSENSUS ALGORITHMS

In blockchain, how to reach consensus among the untrustworthy nodes is a transformation of the Byzantine Generals (BG) Problem, which was raised in . In BG problem, a group of generals who command a portion of Byzantine army circle the city. Some generals prefer to attack while other generals prefer to retreat. However, the attack would fail if only part of the generals attack the city. Thus, they have to reach an agreement to attack or retreat. How to reach a consensus in distributed environment is a challenge. It is also a challenge for blockchain as the blockchain network is distributed. In blockchain, there is no central node that ensures ledgers on distributed nodes are all the same. Some protocols are needed to ensure ledgers in different nodes are consistent. We next present several common approaches to reach a consensus in blockchain.

3.1 Approaches to consensus

PoW (Proof of work) is a consensus strategy used in the Bitcoin network. In a decentralized network, someone has to be selected to record the transactions. The easiest way is random selection. However, random selection is vulnerable to attacks. So if a node wants to publish a block of transactions, a lot of work has to be done to prove that the node is not likely to attack the network. Generally the work means computer calculations. In PoW, each node of the network is calculating a hash value of the block header. The block header contains a nonce and miners would change the nonce frequently to get different hash values. The consensus requires that the calculated value must be equal to or smaller than a certain given value. When one node reaches the target value, it would broadcast the block to other nodes and all other nodes must mutually confirm the correctness of the hash value. If the block is validated, other miners would append this new block to their own blockchains. Nodes that calculate the hash values are called miners and the PoW procedure is called mining in Bitcoin.

Property	*PoW*	*PoS*	*PBFT*	*DPOS*	*Ripple*	*Tendermint*
Node identity management	Open	Open	Permissioned	Open	Open	Permissioned
Energy saving	No	Partial	Yes	Partial	Yes	Yes
Tolerated power of adversary	$< 25\%$ computing power	$< 51\%$ stake	$< 33.3\%$ faulty replicas	$< 51\%$ validators	$< 20\%$ faulty nodes in UNL	$< 33.3\%$ byzantine voting power
Example	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tendermint

Table 3.1 Typical consensus algorithm comparison

3.2 Comparison of consensus algorithm

Different consensus algorithms have different advantages and disadvantages. This gives a comparison between different consensus algorithms and we use the properties given by:

• Node identity management.

PBFT needs to know the identity of each miner in order to select a primary in every round while Tendermint needs to know the validators in order to select a proposer in each round. For PoW, PoS,DPOS and Ripple, nodes could join the network freely.

• Energy saving.

In PoW, miners hash the block header continuously to reach the target value. As a result, the amount of electricity required to process has reach an immense scale. As for PoS and DPOS, miners still have to hash the block header to search the target value but the work has been largely reduced as the search space is designed to be limited. As for PBFT, Ripple and Tendermint, there is no mining in consensus process. So it saves energy greatly.

• Tolerated power of adversary.

Generally 51% of hash power is regarded as the threshold for one to gain control of the network. But selfish mining strategy in PoW systems could help miners to gain more revenue by only 25% of the hashing power. PBFT and Tendermint is designed to handle up to 1/3 faulty nodes. Ripple is proved to maintain correctness if the faulty nodes in an UNL is less than 20%.

Eample.

Bitcoin is based on PoW while Peercoin is a new peer-to-peer PoS cryptocurrency. Further, Hyperledger Fabric utilizes PBFT to reach consensus. Bitshares, a smart contract platform, adopts DPOS as their consensus algorithm. Ripple implements the Ripple protocol while Tendermint devises the Tendermint protocol. PBFT and Tendermint are permissioned protocols. Node identities are expected to be known to the whole network,so they might be used in commercial mode rather than public.PoW and PoS are suitable for public blockchain.

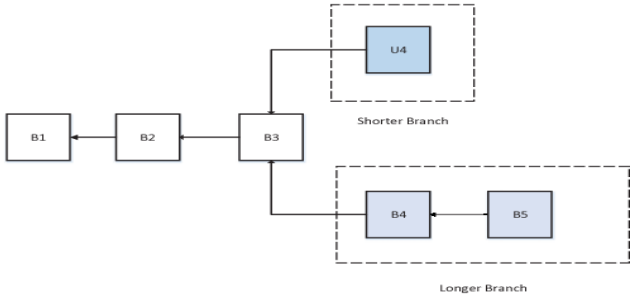

Figure 3.1 A typical consensus algorithm scenario

3.3 Advances on consensus algorithms

A good consensus algorithm means efficiency, safty and convenience. Recently, a number of endeavors have been madeto improve consensus algorithms in blockchain. New consensus algorithms are devised aiming to solve some specific problems of blockchain. The main idea of PeerCensus is to decouple block creation and transaction confirmation so that the consensus speed can be significantly increased. Besides,Kraft proposed a new consensus method to ensure that a block is generated in a relatively stable speed. It is known that high blocks generation rate compromise Bitcoin's security.So the Greedy Heaviest-Observed Sub-Tree (GHOST) chain selection rule is proposed to solve this problem. Instead of the longest branch scheme, GHOST weights the branches and miners could choose the better one to follow. Chepurnoy et al. presented a new consensus algorithm for peer-to-peer blockchain systems where anyone who provides non interactive proofs of retrievability for the past state snapshots is agreed to generate the block. In such a protocol, miners only have to store old block headers instead of full blocks.

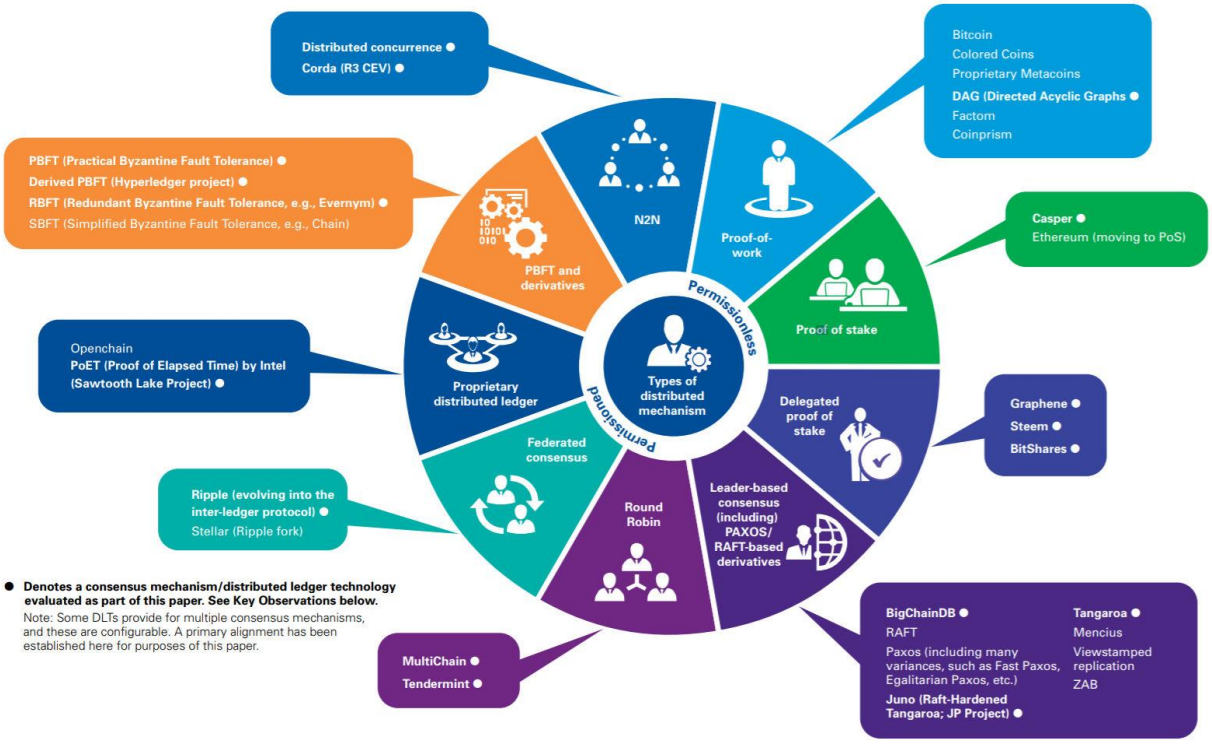

Figure 3.2 Blockchain consensus

CHALLENGES AND RECENT ADVANCES

CHAPTER 4

CHALLENGES AND RECENT ADVANCES

Despite the great potential of blockchain, it faces numerous challenges, which limit the wide usage of blockchain. We enumerate some major challenges and recent advances as follows.

4.1 Scalability

With the amount of transactions increasing day by day,the blockchain becomes bulky. Each node has to store all transactions to validate them on the blockchain because they have to check if the source of the current transaction is unspent or not. Besides, due to the original restriction of block size and the time interval used to generate a new block, the Bitcoin blockchain can only process nearly 7 transactions per second,which cannot fulfill the requirement of processing millions of transactions in real-time fashion. Meanwhile, as the capacity of blocks is very small, many small transactions might be delayed since miners prefer those transactions with high transaction fee.

There are a number of efforts proposed to address the scalability problem of blockchain, which could be categorized into two types:

(1) Storage optimization of blockchain:

Since it is harder for node to operate full copy of ledger, Bruce proposed a novel cryptocurrency scheme, in which the old transaction records are removed (or forgotten) by the network . A database named account tree is used to hold the balance of all non-empty addresses. Besides lightweight client could also help fix this problem. A novel scheme named VerSum was proposed to provide another way allowing lightweight clients to exist. VerSum allows lightweight clients to outsource expensive computations over large inputs. It ensures the computation result is correct through comparing results from multiple servers.

(2)Redesigning blockchain:

In, Bitcoin-NG (Next Generation) was proposed. The main idea of Bitcoin-NG is to decouple conventional block into two parts: key block for leader election and microblock to store transactions.The protocol divides time into epoches. In each epoch,miners have to hash to generate a key block. Once the key block is generated, the node becomes the leader who is responsible for generating microblocks. Bitcoin-NG also extended the heaviest (longest) chain strategy in which microblocks carry no weight. In this way, blockchain is redesigned and the tradeoff between block size and network security has been addressed.

4.2 Privacy Leakage

Blockchain can preserve a certain amount of privacy through the public key and private key. Users transact with their private key and public key without any real identity exposure.

However, it is shown in that blockchain cannot guarantee the transactional privacy since the values of all transactions and balances for each public key are publicly visible. Besides, the recent study has shown that a user's Bitcoin transactions can be linked to reveal user's information.Moreover, Biryukov et al. presented an method to link user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls. In, each client can be uniquely identified by a set of nodes it connects to. However, this set can be learned and used to find the origin of a transaction. Multiple methods have been proposed to improve anonymity of blockchain, which could be roughly categorized into two types:

* Mixing: In blockchain, users addresses are pseudonymous. But it is still possible to link addresses to user real identity as many users make transactions with the same address frequently. Mixing service is a kind of service which provides anonymity by transferring funds from multiple input addresses to multiple output addresses. For example, user Alice with address A wants to send some funds to Bob with address B. If Alice directly makes a transaction with input address A and output address B, relationship between Alice and Bob might be revealed. So Alice could send funds to a trusted intermediary Carol. Then Carol transfer funds to Bob with multiple inputs c1, c2, c3, etc., and multiple output d1, d2, B, d3, etc. Bob's address B is also contained in the output addresses. So it becomes harder to reveal relationship between Alice and Bob. However, the intermediary could be dishonest and reveal Alice and Bob's private information on purpose.It is also possible that Carol transfers Alice's funds to her own address instead of Bob's address. Mixcoin provides a simple method to avoid dishonest behaviours. The intermediary encrypts users' requirements including funds amount and transfer date with its private key. Then if the intermediary did not transfer the money, anybody could verify that the intermediary cheated. However, theft is detected but still not prevented. Coinjoin depends on a central mixing server to shuffle output addresses to prevent theft. And inspired by Coinjoin, CoinShuffle uses decryption mixnets for address shuffling.

*Anonymous: In Zerocoin, zero-knowledge proof is used. Miners do not have to validate a transaction with digital signature but to validate coins belong to a list of valid coins. Payment's origin are unlinked from transactions to prevent transaction graph analyses.But it still reveals payments' destination and amounts.Zerocash was proposed to address this problem.In Zerocash, zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs) is leveraged.Transaction amounts and the values of coins held by users are hidden.

4.3 Selfish Mining

Blockchain is susceptible to attacks of colluding selfish miners. In particular, Eyal and Sirer showed that the network is vulnerable even if only a small portion of the hashing power is used to cheat. In selfish mining strategy, selfish miners keep their mined blocks without broadcasting and the private branch would be revealed to the public only if some requirements are satisfied. As the private branch is longer than the current public chain, it would be admitted by all miners. Before the private blockchain publishment, honest miners are wasting their resources on an useless branch while selfish miners are mining their private chain without competitors. So selfish miners tend to get more revenue. Based on selfish mining, many other attacks have been proposed to show that blockchain is not so secure.

Blockchain technology can also be used in various fields of business. One interesting implementation of Blockchain technology is in the healthcare system. This satisfies all stakeholders such as Hospitals, Healthcare, Health Authorities by meeting information consumer's needs and protecting patient privacy by using Blockchain to pay fees with Bitcoin.

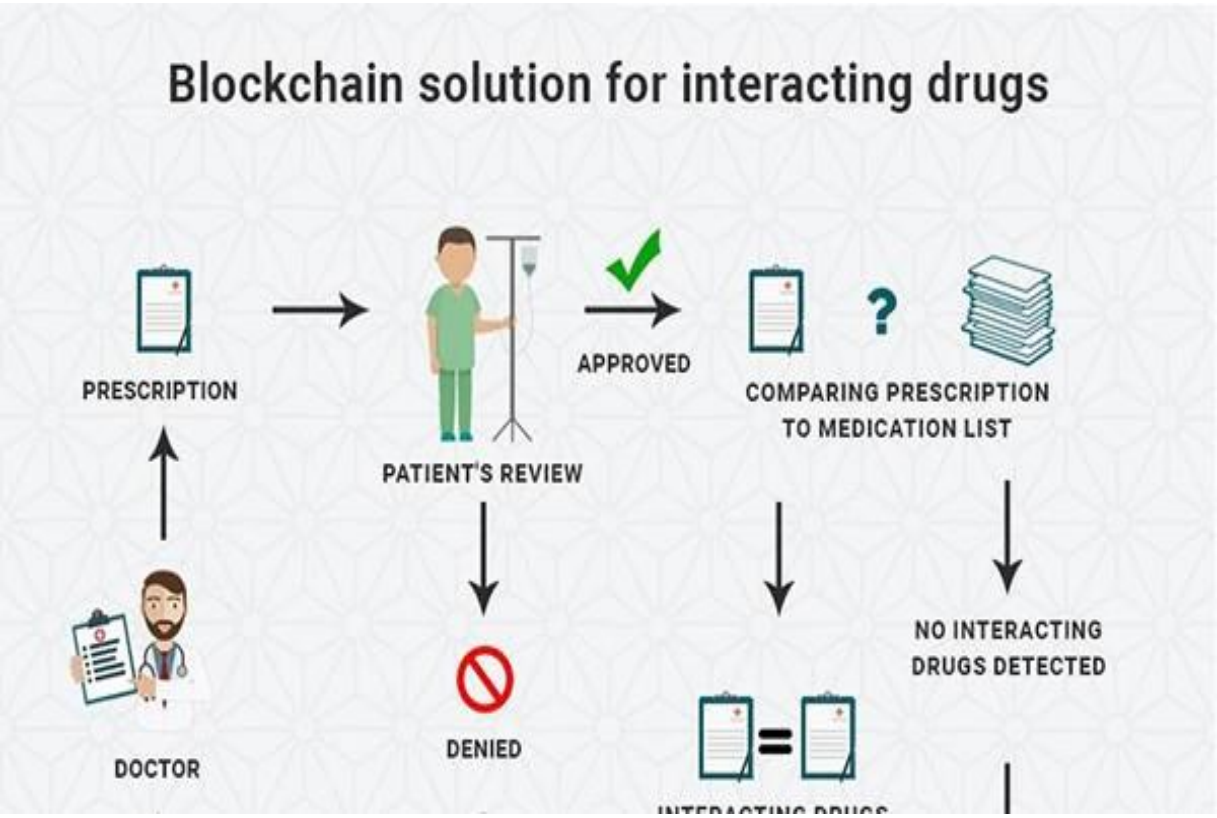

Figure 4.1 E-health system using blockchain

ANALYSIS

CHAPTER 5

ANALYSIS

There are many use cases, that can be realized using blockchain technology. But from the economic and technical perspective, the realization doesn't make sense every time. Therefore, you will find a proposal for the analysis of potential blockchain use cases on suitability in the following. This analysis aims less on technical specifications and the blockchain protocol which is to be used. Rather the parameters and circumstances of the use cases which determine the realization are to be examined.Therefore, four criteria were identified and presented in Table 5.1. The higher the criteria are developed in the use case, the higher is the added value when implementing blockchain technology.

Criteria	low	medium	high
Multi-party process	– 1 to 3 stakeholders	– 4-10 stakeholders	– More than 10 stakeholders
Single-source of truth	– No matching of data between parties necessary	– Matching of data with blockchain, but no central function	– Added value is based on matched data from the blockchain
Missing trust	– Existing trust between stakeholders	– Stakeholders know each other, but don't trust each other	– No existing trust
Open ecosystem	– No open ecosystem, closed process	– Mostly closed process with connections to other areas	– Open ecosystem, unlimited access

Table 5.1 Criteria for evaluation of blockchain suitability

Blockchain technology has a lot of different characteristics, that are suitable for many different purposes. With the following categorization, a clear assignment of the use cases according to their characteristics is supposed to be enabled. This might help to develop a general understanding of blockchain technology in the mobility sector.

5.1 Disadvantages of blockchain technology

- Blockchain data is often stored in thousands of devices on a distributed network of nodes . The data are highly resistant to technical failure and malicious attacks.
- Each network node is able to replicate and store the copy of the database , due to this there is no single point of failure.
- Once the data is registered in the blockchain network it is not easy to be removed, hence this is extremely useful to store financial data.
- Audit trail is required to change or modify data to be recorded on a public ledger..

5.2 Disadvantages of Blockchain technology

- Block chain uses public key and provides users with their private key which they need to keep secret to access their data, incase lost money is effectively lost and nothing can be done about it.
- Block chain specially those using proof of work are highly inefficient since mining is highly competitive .
- The proof of work consensus algorithm that protects the blockchain is very efficient out of the few attacks 51% are more discussed.

APPLICATIONS

CHAPTER 6

APPLICATIONS OF BLOCKCHAIN

Blockchain has shown its potential in industry and academia. We discuss possible future directions with respect to four areas:

blockchain testing, stop the tendency to centralization,big data analytics ,blockchain application.

6.1 Blockchain testing

Recently different kinds of blockchains appear and over 700 cryptocurrencies are listed in up to now. However, some developers might falsify their blockchain performance to attract investors driven by the huge profit. Besides that,when users want to combine blockchain into business, they have to know which blockchain fits their requirements. So blockchain testing mechanism needs to be in place to test different blockchains. Blockchain testing could be separated into two phases: standardization phase and testing phase.

In standardization phase, all criteria have to be made and agreed. When a blockchain is born, it could be tested with the agreed criteria to valid if the blockchain works fine as developers claim. As for testing phase, blockchain testing needs to be performed with different criteria. For example, an user who is in charge of online retail business cares about the throughput of the blockchain, so the examination needs to test the average time from a user send a transaction to the transaction is packed into the blockchain, capacity for a blockchain block and etc.

6.2 Stop the tendency to centralization

Blockchain is designed as a decentralized system. However, there is a trend that miners are centralized in the mining pool. Up to now, the top 5 mining pools together owns larger than 51% of the total hash power in the Bitcoin network . Apart from that, selfish mining strategy showed that pools with over 25% of total computing power could get more revenue than fair share. Rational miners would be attracted into the selfish pool and finally the pool could easily exceed 51% of the total power. As the block chain is not intended to serve a few organizations, some methods should be proposed to solve this problem.

6.3 Big data analytics

Blockchain could be well combined with big data. Here we roughly categorized the combination into two types: data management and data analytics. As for data management,blockchain could be used to store important data as it is distributed and secure.

Blockchain could also ensure the data is original. For example, if blockchain is used to store patients health information, the information could not be tampered and it is hard to stole those private information. When it comes to data analytics, transactions on blockchain could be used for big data analytics. For example, user trading patterns might be extracted. Users can predict their potential partners' trading behaviours with the analysis.

6.4 Blockchain general purpose applications

Currently most blockchains are used in the financial domain, more and more applications for different fields are appearing. Traditional industries could take blockchain into consideration and apply blockchain into their fields to enhance their systems. For example, user reputations could be stored on blockchain. At the same time, the up-and-coming industry could make use of blockchain to improve performance. For example, Arcade City , a ride sharing startup offers an

open marketplace where riders connect directly with drivers by leveraging blockchain technology.A smart contract is a computerized transaction protocol that executes the terms of a contract . It has been proposed for long time and now this concept can be implemented with

blockchain. In blockchain, smart contract is a code fragment that could be executed by miners automatically. Smart contract has transformative potential in various fields like financial services and IoT.

As noted previously, the Blockchain is not a Bitcoin but a form of database stored in a decentralized system. The Blockchain can therefore be adapted for use in a variety of areas. The following are just some of the Blockchain applications active today. □

6.5 Financial Applications

(i)Bitcoin: The Bitcoin or digital currency was first introduced by an anonymous person or group under the alias Satoshi Nakamoto in 2008 . Bitcoin uses a Blockchain public ledger to make transactions across a peer to peer network. Examples of active Bitcoins are Bitbond, BitnPlay, BTC Jam, Codius and DeBuNe.

(ii)Ripple: The Ripple is a currency exchange, remittance and realtime gross settlement system (RTGS) that uses ripple protocol across a peer-to-peer network, a decentralized exchange that focuses on the banking market. Other well-known currency exchange and remittance systems are Coinbase, BitPesa, Billion, Stellar, Kraken and CryptoSigma.

6.6 Non finanancial Applications

(1) Ethereum

A Next-Generation Smart Contract and Decentralized Application Platform was created by a cryptocurrency researcher and programmer named Vitalik Buterin . It uses a Blockchain-based distributed computing platform with a Turing complete scripting language that enables the processing of smart-contracts on the Blockchain.

(2)Hyperledger

The Hyperledger is a Linux foundation project that develops Blockchain technologies for business, supporting only registered members. Hyperledger is an open source collaborative effort created to advance cross-industry Blockchain technologies. This is a global collaboration, hosted by The Linux Foundation, which includes leaders in finance,banking, the Internet of Things, supply chains, manufacturing and technology.There are also many other non-financial applications using Blockchain technologies such as Election Voting (Follow MyVote), Smart Contracts (Otonomos, Mirror, Symbiont), and Blockchain in IoT (e-Plug, Filament).

CONCLUSION

CONCLUSION

Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization,persistency, anonymity and auditability. In this paper, we present a comprehensive overview on blockchain. We first give an overview of blockchain technologies including blockchain architecture and key characteristics of blockchain. We then discuss the typical consensus algorithms used in blockchain. We analyzed and compared these protocols in different respects.Furthermore, we listed some challenges and problems that would hinder blockchain development and summarized some existing approaches for solving these problems. Some possible future directions are also proposed. Nowadays blockchain based applications are springing up and we plan to conduct in-depth investigations on blockchain-based applications in the future. Information technology has become a critical innovation in almost every industry. Those institutions or teams that can use technology correctly and effectively play a major role in disrupting the status quo in a leadership position. Those that don't keep up with technology generally do not survive. The authors of this paper have identified the Blockchain technology as a catalyst for emerging use cases in the financial and non-financial industries such as industrial manufacturing, supply chain, and healthcare. The research indicates Blockchain can play a pivotal role in transforming the digitization of industries and applications by enabling secure trust frameworks, creating agile value chain production, and tighter integration with technologies such as cloud computing, and IoT. In producing a cloud-based application called HealthChain, the researchers have demonstrated the capability to apply professional engineering principles, combined with a DevOps approach to iterative development and management, and integration of cyber security, distributed computing, and Block-chain technologies. We feel HealthChain is one of many examples that demonstrate the transformative capability of Blockchain.Industry is looking to produce efficiencies, create new innovative products, and strengthen customer relationships globally by the effective use of mobile, IoT (Internet of Things), social media, analytics and cloud technology to generate models for better decisions. Blockchain offers a secure way to exchange any kind of good, service, or transaction. Establishing the initial technology in the financial sector as given us insight and recommendations to be applied to other industries including health care where security, transformation and regulation plays a major role in advancing. Blockchain will enable more agile value chains, faster product innovations, closer customer relationships, and faster integration with the Internet of Things (IoT) and cloud technology.

BIBLOGRAPHY

BIBLOGRAPHY

[1] “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,” 2016. [Online]. Available: http://www.coindesk.com/state-of-blockchain-q1-2016/

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] G. W. Peters, E. Panayi, and A. Chapelle, “Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective,” 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn 2646618

[4] G. Foroglou and A.-L. Tsilidou, “Further applications of the blockchain,”2015.

[5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.

[6] B. W. Akins, J. L. Chapman, and J. M. Gordon, “A whole new world: Income tax considerations of the bitcoin economy,” 2013. [Online]. Available: https://ssrn.com/abstract=2394738

[7] Y. Zhang and J. Wen, “An iot electric business model based on the protocol of bitcoin,” in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.

[8] M. Sharples and J. Domingue, “The blockchain and kudos: A distributed system for educational record, reputation and reward,” in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.

[9] C. Noyes, “Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning,” arXiv preprint arXiv:1601.01405, 2016.

[10] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.

[11] A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in bitcoin p2p network,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.

[12] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[13] NRI, “Survey on blockchain technologies and related services,” Tech. Rep., 2015. [Online].Available: http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf

[14] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc: eee:monogr:9780128021170

[15] V. Buterin, “A next-generation smart contract and decentralized application platform,” white paper, 2014.

[16] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ecdsa),” International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[17] V.Buterin,“On public And private blockchains,” 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[18] “Hyperledger project,” 2015. [Online]. Available: https://www.hyperledger.org/

[19] “Consortium chain development.” [Online]. Available: https://github. com/ethereum/wiki/wiki/Consortium-Chain-Development

[20] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[21] S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” Self-Published Paper, August, vol. 19, 2012.

[22] “Bitshares - your share in the decentralized exchange.” [Online].Available: https://bitshares.org/

[23] D. Schwartz, N. Youngs, and A. Britto, “The ripple protocol consensus algorithm,” Ripple Labs Inc White Paper, vol. 5, 2014.

[24] J. Kwon, “Tendermint: Consensus without mining,” URL http://tendermint. com/docs/tendermint { } v04. pdf, 2014.

[25] S. King, “Primecoin: Cryptocurrency with prime number proof-of- work,” July 7th, 2013.