Architecture and Application of Blockchain

Seminar Member (s)

Sl. No.	Reg. No.	Student Name
1.	18ETCS002121	Subhendu Maji
2.	18ETCS002131	Tanishq R Porwar

Supervisors: Mr. Nithin Rao R

Dec – 2021

B. Tech. in Computer Science and Engineering

FACULTY OF ENGINEERING AND TECHNOLOGY

M. S. RAMAIAH UNIVERSITY OF APPLIED SCIENCES

Bengaluru - 560 054

FACULTY OF ENGINEERING AND TECHNOLOGY

Certificate

This is to certify that the Seminar titled "Architecture and Application of Blockchain" is a bonafide work carried out in the Department of Computer Science and Engineering by Mr. Subhendu Maji bearing Reg. No.18ETCS002121 in partial fulfilment of requirements of the Course curriculum of 7th Sem Computer Science and Engineering of Ramaiah University of Applied Sciences.

Dec – 2021

(Name of Mentor): Mr. Nithin Rao R
Designation: **Asst. Professor**
Place:
Date:

FACULTY OF ENGINEERING AND TECHNOLOGY

Certificate

This is to certify that the Seminar titled "Architecture and Application of Blockchain" is a bonafide work carried out in the Department of Computer Science and Engineering by Mr. Tanishq R Porwar bearing Reg. No.18ETCS002131 in partial fulfilment of requirements of the Course curriculum of 7th Sem Computer Science and Engineering of Ramaiah University of Applied Sciences.

Dec – 2021

(Name of Mentor): Mr. Nithin Rao R
Designation: **Asst. Professor**
Place:
Date:

Acknowledgements

The success and final outcome of this project required a lot of guidance and assistance from many people and I am extremely privileged to have got this all along the completion of my seminar. First and foremost, I would like to offer my sincere gratitude to my seminar mentor, Mr. Nithin Rao R , Assistant Professor, Department of Computer Science Engineering, MSRUAS for his valuable suggestions, guidance, and encouragement which he has provided throughout the duration of this project. The experience, which I have gained by working under him, is an invaluable possession. I would like to express my sincere thanks to Dr. H.M. Rajashekara Swamy, Dean, Faculty of Engineering and Technology, MSRUAS for providing necessary support for this project. I am also very thankful to Dr. Pushphavathi T P, Head of Department, Computer Science Engineering, MSRUAS for providing all the help and facilities to carry out the research work.

Summary

Blockchain, the foundation of Bitcoin, has received extensive attention recently. Blockchain serves as an immutable ledger which allows transactions to take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation systems 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 report 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

Table of Contents

1. Introduction

During late 2008, and the global financial crisis was causing shock waves around the world. Anger at the worldwide banking industry, governments and other centralized authorities has reached fever pitch. Enter a mysterious figure named Satoshi Nakamoto, whose real identity continues to remain shrouded in mystery to this day. Satoshi authors and releases a white paper titled **Bitcoin: A Peer-to-Peer Electronic Cash System**.

The paper shared the workings for a new digital currency system that didn't rely on banks to facilitate transactions or governments to create and disseminate the currency. Shortly after its release it was studied by members of the Cypherpunk group and found to be extremely promising. In January 2009, the first transaction took place between Satoshi and Hal Finney, a developer and prominent member of the Cypherpunk movement. And the rest is history. Today, almost everyone has heard about Bitcoin and its value has skyrocketed. Even more profoundly, the Bitcoin currency along with its core blockchain operating technology has managed to propel a decentralized revolution around the world.

Historically, when it comes to transacting money or anything of value, people and businesses have relied heavily on intermediaries like banks and governments to ensure trust and certainty. Middlemen perform a range of critical tasks that help build trust into the transactional process. Things like payment authentication & record keeping. The need for intermediaries is especially acute when making a digital transaction. That's because the internet today is an internet of information, where information is copied and distributed around the world. Think video, email, any digital file.

For example, When you read an email, you are actually looking at a copy of the original. The person who sent you the email has the original email while you have a copy. This

may seem obvious, but when you spend money online, you are not sending physical currency notes. Only data, which represents the transaction of currency (USD, YEN, POUNDS, etc.) is getting sent. So, money in the digital world is just another piece of data like an email or any digital file.

Until now, in this Internet of information, it has been impossible to store, move and transact money or anything of value without relying on an intermediary. That's because there's a big problem. Things don't work so well if you can send someone $100 online, yet still, have that original $100 under your name. That would mean you could just keep spending that $100 as many times as you wanted. The money would become meaningless

2.Background Theory

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 the 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, persistence, 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.

There is a lot of literature on blockchain from various sources, such as blogs, wikis, forum posts, codes, conference proceedings and journal articles. Tschorsch et al. made a

technical survey about decentralized digital currencies including Bitcoin. Compared to, our report focuses on blockchain technology instead of digital currencies. Nomura Research Institute made a technical report about blockchain . Contrast to , our report focuses on state-of-art blockchain research including recent advances and future trends.

3. Aim and Objectives

- **Title**
  - ❖ Architecture & Application of Blockchain
- **Aim**
  - ❖ To understand the architecture of blockchain and its applications
- **Objectives**
  - ❖ To highlight, inform, and discuss the architecture of blockchain
  - ❖ To identify the applications of blockchain
- **Methods and Methodology/Approach to attain each objective**

Objective No.	Statement of the Objective	Method/ Methodology	Resources Utilised
1	To highlight, inform, and discuss the architecture of blockchain	Literature review was carried out by referring to reputed journals, books, manuals and related documents .	Reputed journals and books
2	To identify the applications of blockchain	Literature review was carried out by referring to reputed journals, books, manuals and related documents .	Reputed journals and books

4 Discussion and Results

Physical money allows for money transfers without an external party. Doing that digitally requires a mediator (i.e. a bank) which has implications:

- Minimum transactions cost rise as banks can't avoid mediating disputes
- Merchants need information about customers to build trust as transactions are reversible

There is a need for a digital payments system where trust is ensured by incentives, probability and computation so that no bank interferes and also allows transaction costs to be cut, while making it impractical to reverse a transaction. Buyers can be protected by routine escrow mechanisms.

Transactions

The first thing is that owning some bitcoins isn't like having a dollar in the pocket / bank account. Balances are computed based on transactions which are chained to each other. If you send money to your brother and your neighbor sends it to his sister, both transactions will be part of the same chain. How much you own is defined by the transactions that are sending you coins and you didn't use. A digital wallet just aggregates those numbers to show a balance for you.

Cryptographic hash function: we can picture a hash function as a blackbox that takes a string as input (such as "Hello Bob") and returns a fixed size arbitrary string (such as "*98b0f4b363af4aceb81bc42fd81117e1*").

For a hash function to be usable cryptographically it must have certain properties:

- Same input always returns same output
- It's quick to compute

- You can't reverse engineer the "*98b0f4b363af4aceb81bc42fd81117e1*" that comes from "Hello Bob" without brute force (trial and error)
- A small change in the input will change the output a lot
- It's unfeasible that two inputs generate the same output

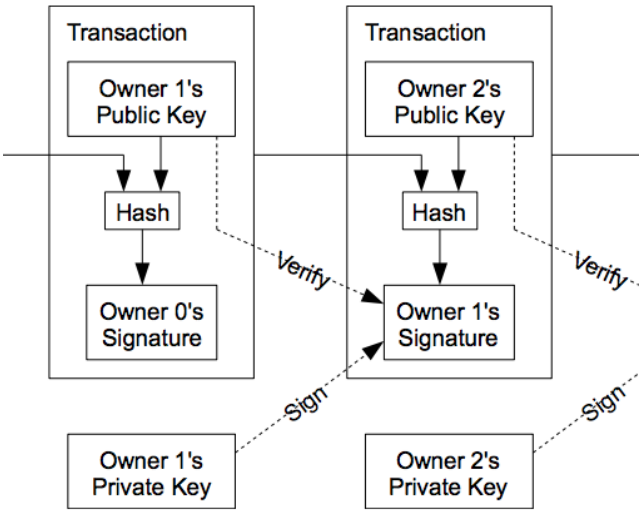
Asymmetric cryptography: it will allow us to communicate through an insecure channel. A typical use case is when Bob wants to send a message to Alice which only she can read. Another use case is to be able to verify who the sender of a certain message is.

This is the case that we are interested in (Did Bob really send that message?).
Bitcoin currently uses the ECDSA standard for that (you would have to understand DSA as well) but we can abstract the technical details into the following:
A pair of private and a public keys are generated for every entity (Bob, a computer, a bitcoin address, …) with which they can sign documents the same way you can sign a car rental contract physically. Bob can use his private key to sign (generate a signature for) a document containing "Best car contract ever" and anyone can use the public key of Bob to verify that he (owner of the private key) actually signed that document. There is no way someone else could have generated that signature without having the private key of Bob which leads to him being the author. Check here if you want to get a feeling on how the ECDSA keys/signature look.

The chain

A transaction is a transfer of Bitcoin value from one or more inputs to one or more outputs.
Let's suppose we are Owner 1 (generating the transaction on the right). We use the public key of the person we are sending bitcoin to ("Owner 2's Public Key") and the

previous Tx (line coming from the left Tx) to produce a hash which we are signing (through "Owner 1's Private Key").

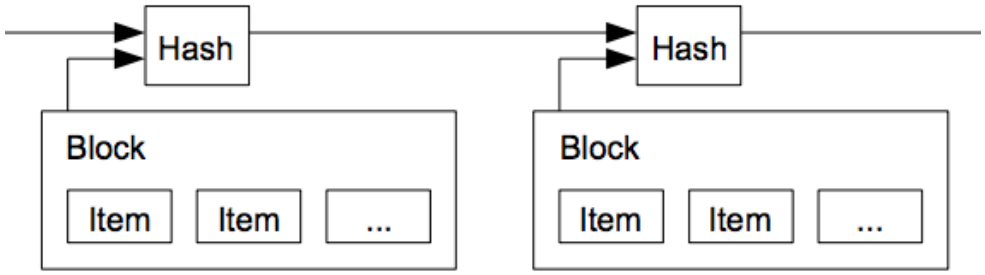


Double spending

Someone could add two transactions that consume from the same output unless we have a single chain which someone checks. If this chain is centralized we would have to trust that entity that no double spending would be produced and the chain won't be altered which is no different to the current situation with normal banks.

We consider the first transaction as the valid one, but without a centralized entity every transaction must be publicly announced and we need the participants to agree on when each transaction arrives at the time they have to generate a new one.

Timestamp server



A timestamp determines when an event occurred by using a sequence of characters. In UNIX it's common to use the seconds since January 1st 1970 UTC time as a timestamp, which makes 04/15/2018 @ 11:56am (UTC) look like 1523793381.

Proof of work

We saw that a SHA-256 function produces a fixed-length (256 bits) string (in Hexadecimal) from a certain data input. Let's have a look at how such a hash looks for some inputs ("Alice", "alice" and "ALICE"). Output is represented in Hexadecimal and Binary (only the beginning for brevity):

Input	Hexadecimal(64)	Binary(256)
Alice	3BC51062973C458D5...	001110111100...
alice	2BD806C97F0E00AF1...	001010111101...
ALICE	E7DCEE3CC63D170BA...	111001111101...

As you can see, the output drastically changes for small changes on the input but will remain the same when it isn't changing.

Hashcash PoW

This asymmetry of I/O has been exploited in Hashcash to ensure a certain operation has a cost associated with it.

An example could be reducing email SPAM: I give you a challenge to be resolved before sending the email which will cost you some computing power (i.e. electricity hence money). It will be small enough so that sending one email is cheap but costly enough to avoid a spammer sending many. What could the challenge be?

Input	Hexadecimal(64)	Binary(256)	K	Solved?
Alice0	E2E90D225B4A14C14...	111000101110...	0	NO
Alice1	9D328D8B7AC56E1F7...	100111010011...	0	NO
Alice2	**3574A3A090231B3A7...**	**001101010111...**	**2**	**YES**

Let's say the content of the email you are sending is "Alice". We know the output of a SHA-256 applied to the content starts with 3 (0011 in binary) from the table above. A challenge I could give you is to find a number which when appended to the content (i.e. "Alice24") will produce a binary output with a certain amount of 0's in the beginning. Why would I do that? Well, it's just math. You can picture the binary output as a sequence of flipping coins (we don't know what output we get from a certain input so the sequence of 0's and 1's is random, just like the chance of flipping a coin). What is the chance to get one 0 from a certain number appended to Alice? Well, 50% (it's flipping

one coin). To have two consecutive 0's? 25%. And so on… The more 0's I ask you for, the more difficult the challenge gets.

So let's say k is the number of 0's we are asking for. Given the input "Alice" and a challenge k=2:

We have found a solution by calculating the hash 3 times. Everyone can calculate the hash just once and verify that we solved the challenge correctly. We could make the challenge much more difficult by requiring more 0's to appear on the output (k=20 requires on average 1 million tries).

Incentive

Every mined block has a first transaction called coinbase transaction. It's the one that gives the reward to the miner for doing it's PoW. That's how bitcoins are initially put into circulation and the amount of reward gets capped every 210000 blocks (~4 years) by half.

Reclaiming disk space

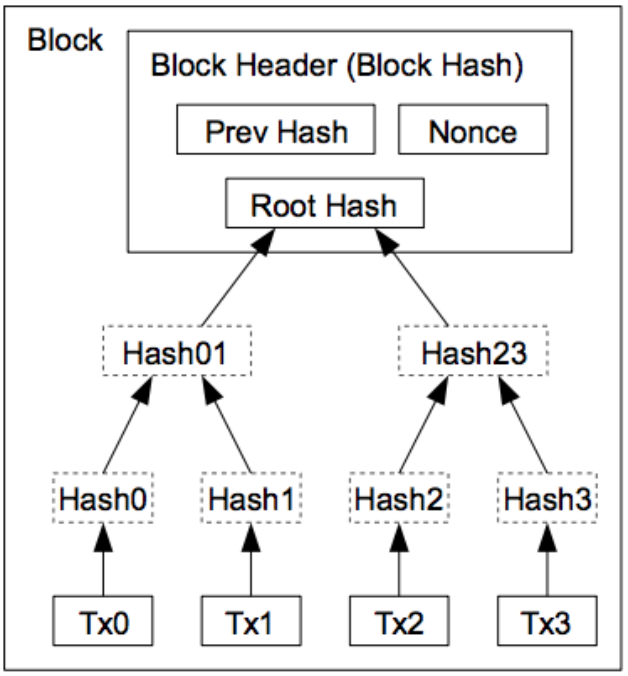
Each transaction size varies depending on the number of Inputs/Outputs. The average transaction size since 2014 is around 520 Bytes. There are around 277 Million transactions for that period. Excluding the size of the blocks it would mean that storing all these transactions would occupy ~144 GB. In reality they occupy ~150GB. Quite a lot if you want to interact within your smartphone!

The block header with no transactions occupies ~80 Bytes. The number of blocks for the same period is ~240,000 which occupies a total of 19MB. Such size sounds much more competitive.

Merkle tree

The leaf nodes (Hash0, Hash1, …) are a hash function applied to some data (in this case Tx0, Tx1, etc…). Upper nodes (Hash01, Hash23) are just a hash function applied to the concatenation of their respective children hashes. The Root Hash is the upper-most hash which is included in the block header and ensures what transactions are present.

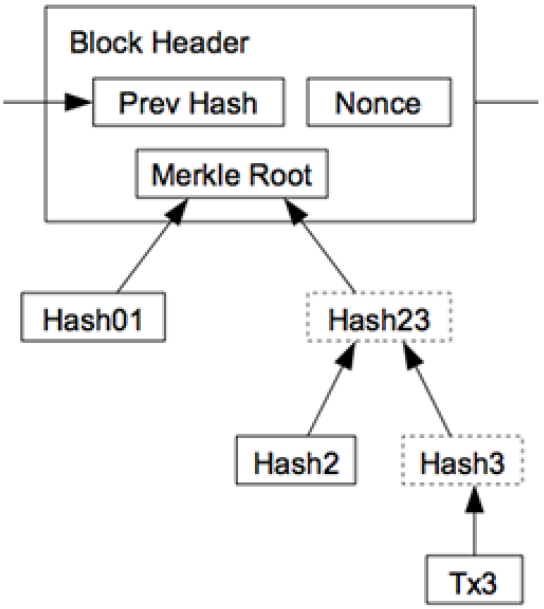
If we wanted to validate if a transaction is part of a block which has many transactions, a Merkle Tree would allow us to do it at logarithmic cost compared to getting all hashes.



Simplified Payment Verification

Supposing we have a thin client which doesn't have access to the transactions but only block headers, we must find a way to validate that a specific transaction is valid.

Such a node can get the longest proof-of-work chain at the moment (from several thick nodes) and request the Merkle Tree branch where the transaction is supposed to be. Once the node knows the transaction is part of the chain and that there are blocks after it he can conclude it was a valid transaction as it was accepted by other thick nodes.
As long as we are asking honest nodes this scheme will work. If that's not the case Satoshi proposes an alerting system whenever an invalid block is detected by some node.



Hacking the blockchain

If we suppose an attacker could get more power than the honest nodes he can alter the chain. He can't alter it in any way he wants, as honest nodes wouldn't accept an invalid transaction/block (such as sending other people money to himself or creating money out of thin air).
The only option is to alter the outputs of his latest transactions or revert them (the bigger the chain after the transaction the more proof of work is required to generate the longest valid chain).

The math behind the results shows that the probability of the attacker catching up decreases exponentially the more blocks are confirmed:

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

P = probability of the attacker to catch up (0.1%)

q = probability of the attacker finding the next block (10%, 15%, …)

z = number of block confirmations

These numbers tell us that the more CPU power an attacker has (q) the more confirmations we have to wait (5, 8, …) to know that the probability of the attacker catching up with the chain will be < 0.1%.

This sounds like the chance for an attack is pretty low given the constantly growing size of nodes within the network but remains a risk for newly created PoW based chains.

5. Conclusions and Suggestions for Future Work

Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability. In this report, 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.

The original bitcoin paper proposes an electronic transactions system that relies on distrust. Ownership is proven by digital signatures while double-spending is mitigated through the PoW-based P2P network. All rules and incentives are enforced within the network consensus. Bad actors are penalized while honest ones are rewarded. This laid the foundation to the blockchain technology and most of the applications in use the method proposed in some way. Although new consensus protocols have been suggested.

Future works

We discuss possible future directions with respect to four areas:

- blockchain testing
- stopping the tendency to centralization
- big data analytics
- blockchain application.

Blockchain testing

Recently different kinds of blockchains appear and over 700 cryptocurrencies are listed 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 a blockchain testing mechanism needs to be in place to test different blockchains. Blockchain testing could be separated into two phases:

- standardization phase
- testing phase.

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 own more 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 blockchain is not intended to serve a few organizations, some methods should be proposed to solve this problem.

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 with and it is hard to steal that private information. When it comes to data analytics, transactions on blockchain could be used for big data analytics. For example, user trading patterns might

Blockchain 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.

References

- http://caliberhr.com/assets/upload/12dbfce36c9f7e0474e1ebadbb0dd647.pdf
- https://static1.squarespace.com/static/567bb4f069a91a95348fa0b2/t/5cd27c8bb208fcb3a45d2196/1557298317565/Intrepid+Ventures+Bitcoin+White+Paper+Made+Simple.pdf
- https://medium.com/coinmonks/bitcoin-white-paper-explained-part-1-4-16cba783146a