| | |
|---|---|
| Full Name | **Muhammad Hassam Khalid** |
| Student ID | **11669134** |
| Subject | ITC571 – Emerging Technology and Innovations |
| Assignment No | A2 - Project Proposal and Plan |
| Due Date | 05-April-2020 |
| Lecturer's Name | Malka N. Halgamuge |



## Title:

**Permissioned Blockchain and Permission-less Blockchain: Studying Consensus Algorithms and 2-tier architecture based on voting system**

## Project Blog:

http://thinkspace.csu.edu.au/11669134hassam/

# Contents

## Introduction:

When the blockchain technology was first introduced in 2008, the main purpose of this technology was to keep track of the digital assets with the help of distributed ledgers. Now after twelve years the research and development in the blockchain technology has resulted in the increase in the growth and usage of this technology. The main benefit of blockchain is decentralization, Blockchain, because of its protection of data due to decentralization is mainly used in the sector of finance, cloud computing, energy trading and in IT for securing the private and confidential data. Number of modules collectively make up blockchain, modules like distributed systems, data encryption, timestamping, distributed consensus algorithms and distributed ledger. These blockchain modules can be tweaked accordingly (Belotti, Božić, Pujolle, & Secci, 2019). Blockchain exists on multiple nodes of a network, and it grows every time new nodes are added. Every node has a timestamp and hash value of the previous node, in this was nodes make a link in this was no unauthorized node gets added in the link. Blockchain is now used to record transaction between two parties and the transaction data is stored in the nodes. The nodes hold the record ledger and relies on something while performing transaction, that something is the consensus algorithm. Consensus algorithm helps in validating the information without the help of any third-party. Consensus algorithm provides an environment free of interference to the nodes in which all the nodes come to an agreement of performing a task or transaction (Chaudhry & Yousaf, 2018).

With the advancement in the blockchain technology. Now blockchain can be implemented in two different methods, permission-less blockchain and permissioned blockchain. Permission-less blockchain is like an open environment in which any party can join the network or public can add nodes and each node is given equal consensus privilege (Kim, 2019). Bitcoin is an example of permission-less blockchain. While in permissioned blockchain is a closed environment with only known entities or nodes, Permissioned blockchain is used inside enterprises or between enterprises to share private and confidential data and transaction, no third party or public can be added in the permissioned blockchain. Example of permissioned blockchain is Hyperledger (Bach, Mihaljevic, & Zagar, 2018).

While Permissioned and permission-less blockchain has their own use cases but they cannot exist without the core concept of consensus algorithm. As both blockchains has different configurations each blockchain uses different algorithms. This report will study the algorithms in depth for each blockchain and will propose ways of making those algorithms more efficient and effective and make blockchain overall.

There is a need of research on the consensus algorithms for blockchain and the compatibility of the algorithm with the specific type of blockchain. For example, Proof-of-Work algorithm results in computation energy waste, this paper will cover that as well as come up with a solution. The research is needed because of the need to find the perfect compatibility of the consensus

algorithm for each type of blockchain to make it efficient and accurate. This paper will also propose algorithms which will make permissioned and permission-less algorithms more effective.

## Rationale:

1. **Problem domain:**

   The problem domain is the consensus algorithm for the blockchain. As the algorithms used are not effective in gaining the desired output. AS consensus algorithm is the main concept of the blockchain. Consensus algorithm is responsible in making the nodes of the network to come to an agreement in performing task or transaction.

2. **Purpose and justification:**

   The purpose of this paper is to study the consensus algorithms in depth for both permissioned and permission-less algorithms and propose solutions to make the algorithm more efficient as the current few algorithms result in computation energy waste like proof-of-work. The proposed solution will also help in finding best use cases for both permissioned and permission less algorithms.

## Supervisor Approval: Yes

## Research Questions:

1. **What is the aim and objective of the research?**

   To study the consensus algorithms of permissioned and permission-less blockchain and to propose solution to make consensus algorithm and blockchain overall more effective.

2. **What is the outcome of the research?**

   In depth understanding of the consensus algorithms and how they work and why the consensus algorithm is the integrity of the blockchain technology and gain knowledge to work further in blockchain technology and in consensus algorithm in focus.

3. **Can consensus algorithms for permission-less blockchain be used for permissioned blockchain and vice versa?**

   There are exceptions where the consensus algorithms for permission-less blockchain can be used for permissioned blockchain but at the expense of poor performance and network bottleneck/ Further will be discussed in the report (Lasisi & Hsu, 2019).

4. **What will be the representation of Algorithms in the report?**

The algorithms will be represented and explained in mathematical notations and in algorithm format if need be for further explanation of the algorithms.

5. **What will be the timeline of the research?**

This research is not limited to the ITC 571. As this research is the continuation of the research done in ITC 560 (internet-of-Things) which was analysing the challenges of blockchain in IOT and building an optimal network for IOT using blockchain, this research will be continued as personal project.

## Theoretical Framework:

The algorithms used to make nodes approve on a task or transaction to be performed, each consensus algorithm has their own requirements. For example, Proof-of-Work is the most common type of consensus algorithm used in permission-less blockchain (bitcoin) because Proof-of-Work works well in distributed network where each node has same priority on consensus algorithms, every node gets the same treatment from the consensus algorithm. Whereas, if somehow the Proof-of-Work is implemented in permissioned blockchain where the node entities are known and no unauthorized node can be added, proof-of-work will result in problems like high computational energy waste, nodes not been fully utilized and throttle neck in the network because in permissioned blockchain only selected nodes participate in consensus and proof-of-work algorithm is generally designed for large expanding distributed network with no limitation on computational power (Amiri, Agrawal, & Abbadi, 2019). Permissioned blockchain has its own algorithms which are more complex than algorithms used in permission-less blockchain because of the characteristics of the permissioned blockchain (Pahlajani, Kshirsagar, & Pachghare, 2019).

The research being done is interesting because of the outcome, which is in depth understanding of the permissioned and permission-less blockchain which will help in gaining motivation to continue the research further in the blockchain field. The outcome of this paper will also help in figuring out new scenarios where permissioned and permission-less blockchain can be used. The blockchain field in relatively new which makes room for much improvement, blockchain also being a field whose demand is rapidly increasing results in a topic worthy or research and development (Jalalzai, Busch, & Richard, 2019). This research being done is a part of understanding the current blockchain and understanding its gaps and limitations.

The research already being done in blockchain, particularly in consensus algorithm is about developing new algorithms for blockchain to satisfy the current demands whereas there is less study about improving the current consensus algorithms being used. Most of the studies are conceptual and few of them being done practically.

# Methodologies used and Material used:

1. **Sources of information:**

The source of information being used in this research is being gathered from the research papers and articles from IEEE portal online. The chosen research papers and articles are published by IEEE and are relatively new which are at least 1.5 years old.

2. **Research methodologies:**

The research method used in this research is a hybrid method which comprises of two methods, the chosen methods for the hybrid method are:

- **Problem-oriented method:** This method revolves around understanding the nature of the problem and to find out the solutions. This method includes in describing the problem domain in depth including the background which helps in developing a pathway towards finding the solution (Bhat, n.d.).
- **Quantitative method:** This method includes collecting and deriving data and analysing data to develop conclusions. Quantitative method will be used to derive data from the chosen research papers and from the problem-oriented method to make a benchmark for the proposition (Bhat, n.d.).

3. **Data Collection Methods:**

There are two research methods used in this research:

- **Observational method:** This method includes the observation of data in the available research papers. This allows researcher to develop a base or starting point of their research by observing already done research papers. Researcher also gets the knowledge of the topic he is working in. The researcher gets to understand the key points he needs to consider while conducting his own research and to develop to scope of his research.
- **Derived Method:** This method includes deriving data from the source and using it for own purpose for example: like comparing the derived data with your own result data (Dudovskiy, n.d.).

4. **Ethical issue and compliance:**

The data used from other research paper or article used in this research will be quoted to the original author and to give credit.

The blockchain technology has diverse scope. The scenarios described in this research will be legal and not in any way will promote the usage of blockchain technology against the law.

The blockchain must follow the compliances developed by regulatory bodies. The blockchain under compliance is the characteristic of immutability which makes data stores in blockchain safe from alteration and deletion**.** KYC and AML compliance allows blockchain to be used for identity checks in less time to prevent identity thefts.

5. **Proposition:**

The outcome of this research will include proposition of enhancing or improving the discussed consensus algorithms for permission-less and permissioned blockchain.

6. **Step-by-Step methodology:**

The hybrid research method will be used in this research which is comprised of problem-oriented method and quantitative method. The steps taken in this research will be as follows:

**Problem oriented method:**

1. Gather relevant papers and data.
2. Analyse the gathered paper and data to further understand the problem domain and background.
3. Develop a base or starting point for your research.

**Quantitative method:**

4. Derive the data from the gathered papers.
5. Take the research further and use the derived data to start developing proposition.
6. Develop the proposed solutions and explain.
7. Support the propositions with data.

# Project Plan:

1. **Deliverables:**

The deliverables of this research report will be

- Annotated Bibliography: (Complete date 02/April/2020)
- Research report: (Complete date 19/May/2020)
- Journal Report: (Complete date 20/May/2020)

2. **Work Breakdown Structure (WBS):**

WBS of the project is as follows:

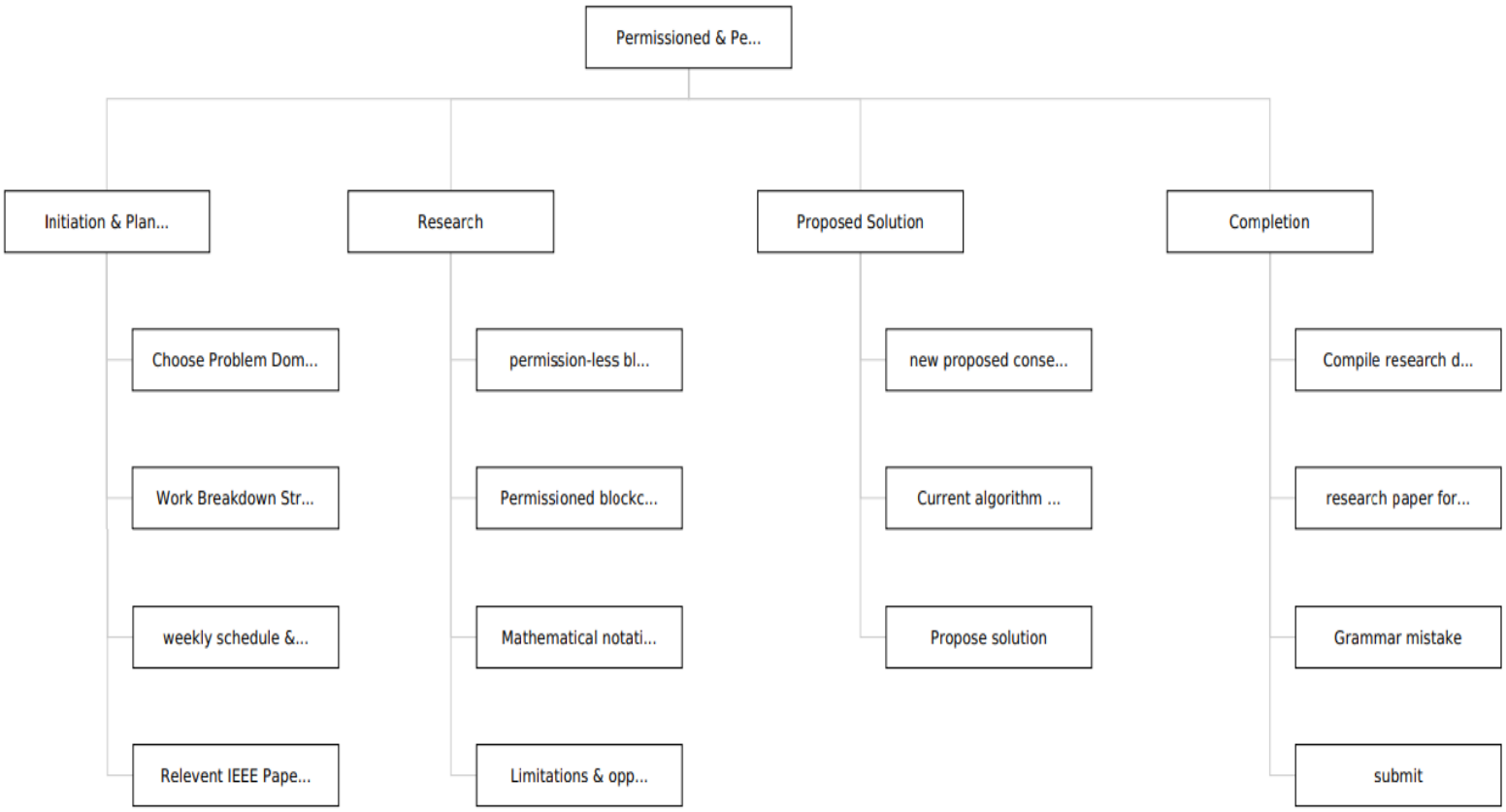



*Figure 1: Work Breakdown Structure.*



### 3. Risk Analysis:

The project faces 3 risks which are as follows along with mitigation, contingency and consequence.

| Risk | Probability | Impact | Mitigation | Contingency | Consequence |
|---|---|---|---|---|---|
| Insufficient Data on consensus algorithm | 40 | 80 | Use other online portals like Google Scholar to find research articles to find relevant data. | Focus on Permissioned vs Permission-less blockchain instead of their relevant consensus algorithms | If data relevant to permissioned blockchain consensus algorithm and permission-less algorithm is not found it will result in changing the scope of the research. |
| Insufficient time to complete the research | 15 | 50 | Leave the complex consensus algorithms to be done at end and focus on relatively easy algorithms first to keep the research going and on time. | Leave the complex algorithms and further explain the already done algorithms in depth along with mathematical notations. | Can result in low quality research report. |
| Grammar and reference mistakes | 10 | 30 | Check grammars mistakes and references before submitting report. | Check peer feedback before submitting the report | Can result in poor grade in report |



**4. Duration:**

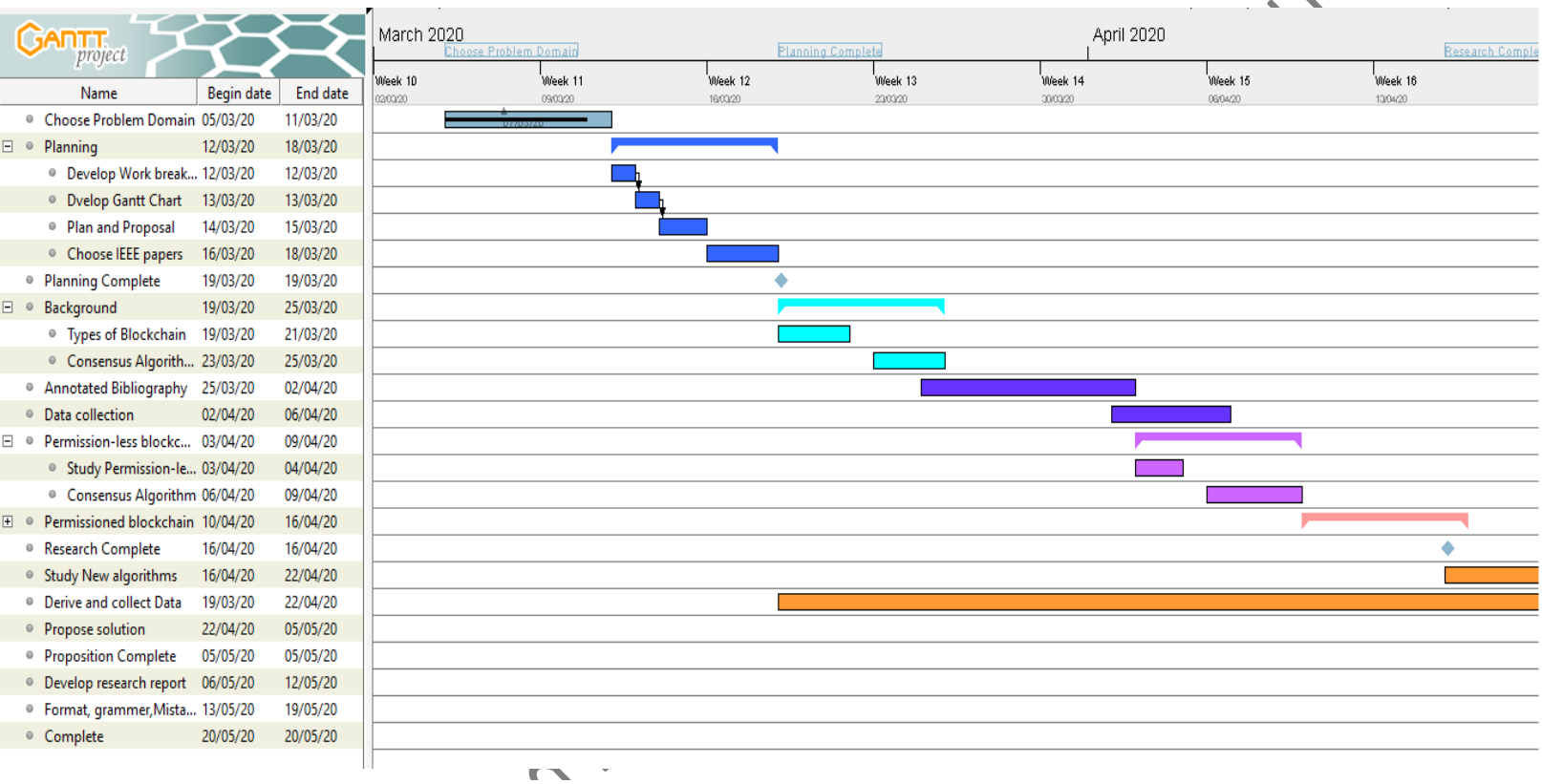
The duration of this research project is 12 weeks. Starting from 05-March-2020.

**5. Gantt Chart:**

the Gantt chart of the project is as follows: The first Gantt chart shows represents schedule of March and April while second Gantt chart shows schedule of April and May. The tasks are on the left side. The Whole Schedule in Gantt chart has 3 milestones.

- **Milestone 1 Planning Complete:** The initial phase and planning will be completed, and all the required IEEE papers will be chosen.

- **Milestone 2 Research Complete:** The research phase will be completed, and all the required data will be derived which will be needed in developing the proposition solutions which is the final phase.
- **Milestone 3 Research report Complete:** The proposed solutions will be developed. All the research data will be compiled and converted into research report with required format.




| Name | Begin date | End date |
|---|---|---|
| Choose Problem Domain | 05/03/20 | 11/03/20 |
| Planning | 12/03/20 | 18/03/20 |
| Develop Work break... | 12/03/20 | 12/03/20 |
| Dvelop Gantt Chart | 13/03/20 | 13/03/20 |
| Plan and Proposal | 14/03/20 | 15/03/20 |
| Choose IEEE papers | 16/03/20 | 18/03/20 |
| Planning Complete | 19/03/20 | 19/03/20 |
| Background | 19/03/20 | 25/03/20 |
| Types of Blockchain | 19/03/20 | 21/03/20 |
| Consensus Algorith... | 23/03/20 | 25/03/20 |
| Annotated Bibliography | 25/03/20 | 02/04/20 |
| Data collection | 02/04/20 | 06/04/20 |
| Permission-less blockc... | 03/04/20 | 09/04/20 |
| Study Permission-le... | 03/04/20 | 04/04/20 |
| Consensus Algorithm | 06/04/20 | 09/04/20 |
| Permissioned blockchain | 10/04/20 | 16/04/20 |
| Research Complete | 16/04/20 | 16/04/20 |
| Study New algorithms | 16/04/20 | 22/04/20 |
| Derive and collect Data | 19/03/20 | 22/04/20 |
| Propose solution | 22/04/20 | 05/05/20 |
| Proposition Complete | 05/05/20 | 05/05/20 |
| Develop research report | 06/05/20 | 12/05/20 |
| Format, grammer,Mista... | 13/05/20 | 19/05/20 |
| Complete | 20/05/20 | 20/05/20 |

*Figure 2: Gantt Chart March - April*

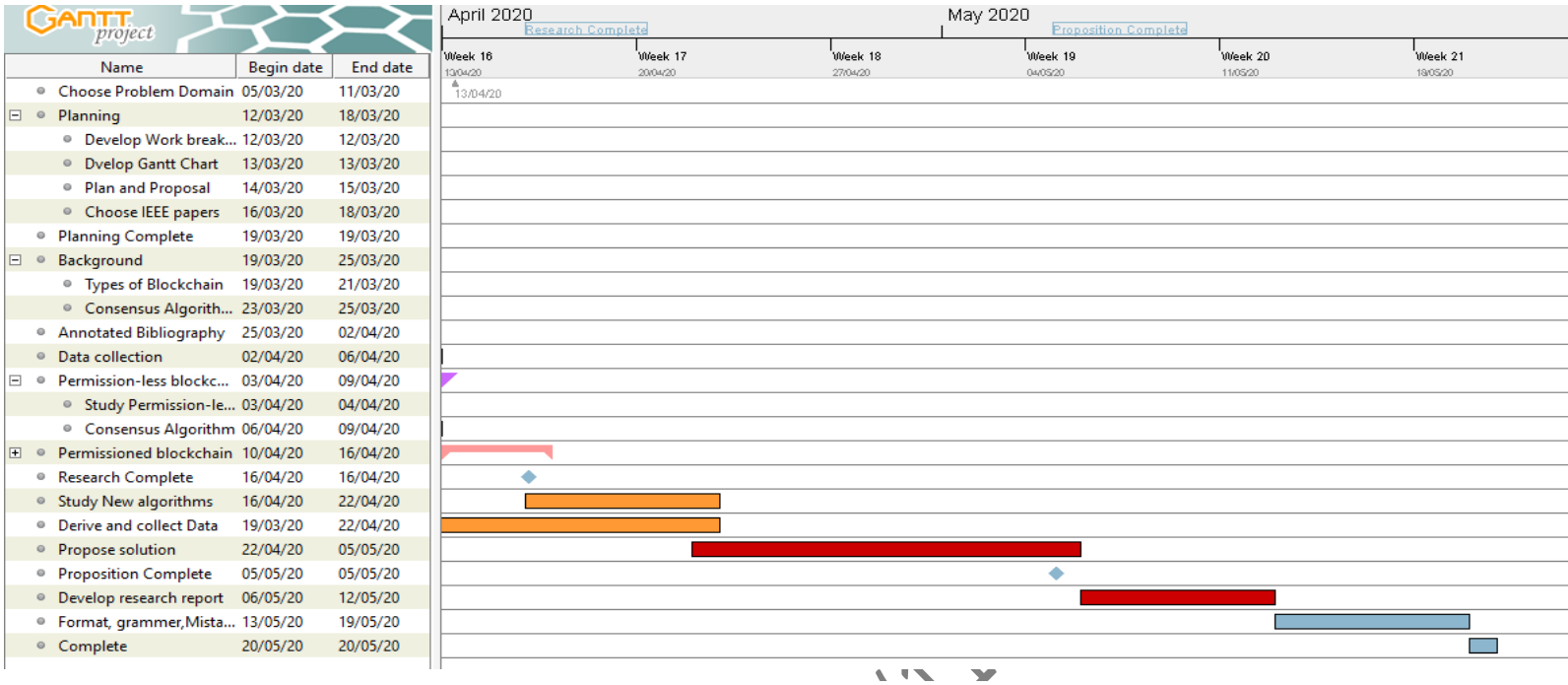



*Figure 3: Gantt Chart April - May*



## 6. 12-Week Schedule:

| Week | Task |
|---|---|
| 1 | Attend workshops on how to do research and write research papers & choose problem domain |
| 2 | Select research papers from IEEE relevant to the research |
| 3 | Develop project proposal and plan |
| 4 | Understand types of blockchain and consensus algorithm in depth. |
| 5 | Annotated bibliography of chosen papers and collect data |
| 6 | Work on permission-less blockchain and relevant consensus algorithm |
| 7 | Work on permissioned blockchain and relevant consensus algorithm |
| 8 | Study research papers on new proposed consensus algorithms |
| 9 | Derive data from the chosen research papers and implement in research |
| 10 | Start compiling the research report |
| 11 | Implement the proposed solutions for the consensus algorithms in the research report. |
| 12 | Transform research report into appropriate format and check for grammar mistake. Go through the proposition method. Check references |

*Table 1: Weekly Project Schedule*

The work breakdown structure and Gantt chart of the project are developed by keeping the above weekly project schedule in mind.

# Bibliography


Amiri, M. J., Agrawal, D., & Abbadi, A. E. (2019). On Sharding Permissioned Blockchains. *2019 IEEE International Conference on Blockchain (Blockchain).* Atlanta, GA, USA, USA: IEEE.

Bach, L. M., Mihaljevic, B., & Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).* Opatija, Croatia: IEEE.

Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials ( Volume: 21 , Issue: 4 , Fourthquarter 2019 )*, 3796 - 3838.

Bhat, A. (n.d.). *WHAT IS RESEARCH – DEFINITION, METHODS, TYPES & EXAMPLES.* Retrieved from QUESTION PRO: https://www.questionpro.com/blog/what-is-research/

Chaudhry, N., & Yousaf, M. M. (2018). Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities. *2018 12th International Conference on Open Source Systems and Technologies (ICOSST).* Lahore, Pakistan, Pakistan: IEEE.

Dudovskiy, J. (n.d.). *Research Methods*. Retrieved from RESEARCH METHODOLOGY: https://research-methodology.net/research-methods/

Jalalzai, M. M., Busch, C., & Richard, G. G. (2019). Proteus: A Scalable BFT Consensus Protocol for Blockchains. *2019 IEEE International Conference on Blockchain (Blockchain).* Atlanta, GA, USA, USA: IEEE.

Kim, D.-H. (2019). RSP Consensus Algorithm for Blockchain. *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS).* Matsue, Japan, Japan: IEEE.

Lasisi, A., & Hsu, S. (2019). Consensus Mechanism in Enterprise Blockchain. *2019 IEEE International Conference on Intelligence and Security Informatics (ISI).* Shenzhen, China, China: IEEE.

Pahlajani, S., Kshirsagar, A., & Pachghare, V. (2019). Survey on Private Blockchain Consensus Algorithms. *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT).* CHENNAI, India, India: IEEE.