Project Proposal

CSE 535: Asynchronous Systems

November 12th, 2018

Project Information

Project Topic	Implementation of Proof of Work Consensus in Dist Algo
Technology	DistAlgo and Python
Team Members	Arun Swaminathan (SBU ID:112044697)
	Hardik Singh Negi (SBU ID:111886786)
	Shubham Jindal (SBU ID:112129688)

Introduction

Since it's introduction in 2008 the blockchain technology has found its applications in several sectors ranging from cryptocurrencies to healthcare. At the very core, this technology is a distributed ledger that works asynchronously in a trustless environment to handle large amounts of data efficiently. Due to its decentralized nature, the blockchain requires the use of robust consensus algorithms to perform desired actions. Several efficient and robust consensus algorithms like proof of work (PoW), proof of stake (PoS), PBFT etc. have been leveraged by existing blockchain implementations.

In this project, we plan to explore, implement and analyze the proof of work (PoW) consensus algorithm. For the implementation purposes, we plan to leverage the DistAlgo[1] language framework as it will enable us to focus on the high-level implementation and analysis of the algorithm, as the framework will itself handle the nuances of distributed implementations.

Goal

- The primary goal is to implement the proof of work consensus algorithm in blockchain using the DistAlgo framework. According to the best of our knowledge, no such implementation exists in DistAlgo.
- We plan to implement this algorithm based on the design given in the paper and implementation given by Amitai Porat et. al [2][3]
- After this, we plan to analyze the performance of the system and perform correctness testing as a secondary goal.

Input

The input of the system will consist of transaction ledger, generated by recording different user transactions.

Output

The ideal output generated by the system is as follows:

- The miners present in the blockchain verify the transactions and the consensus is reached without violating any correctness property.

- Blocks of pending transactions are added to the blockchain.

Performance and Testing Metrics

We plan to perform the testing and benchmarking of the implemented system on the following metrics:

- The system must not violate correctness property and must also be live.
- Length of blockchain under varying parameters.
- Average time to mine a block.
- Length of blockchain according to varying parameters.
- Performance of the system under varying number of hosts.
- Performance of the system under the varying size of transaction ledger.

Please note that this list of metrics is not exhaustive and we will add more metrics to it for testing as the project materializes in the coming weeks.

State of the Art

The proof of work system was invented by Cynthia Dwork and Moni Naor and presented in a journal article[4] as a way to deter denial of service attacks and spams. However, in 2008 Satoshi Nakamoto leveraged this as a consensus algorithm for Bitcoin cryptocurrency blockchain[5][6]. Since then several other cryptocurrencies like Ethereum[7][8] have used PoW as a defacto consensus algorithm for their blockchains.

For the project, we are focusing on papers and implementations more centered on the PoW consensus and we found the implementation described in the paper by Amitai Porat et. al useful for our purpose.

Moreover, we will be developing our system based on the following PoW implementations:

1. Implementation of Proof-Of-Work consensus protocol using Python (Ver. 2.7) by Amitai Porat et. al.
   This is a proof of work consensus implementation based on Ethereum platform developed in Python.
2. Interactive blockchain built with Node.js by Matias Olivera[9]
   This is an interactive version of blockchain implementation developed on Node.js and javascript platform.
3. Justblockchain by Koshik Raj[10]
   This is a Python-based interactive implementation which allows users to interact with the blockchain via terminal.

Sub Tasks for Team Members

Member	Tasks
Arun Swaminathan	● Designing and development of PoW system. ● Benchmarking the system performance. ● Will work on Project presentation.
Hardik Singh Negi	● Designing and development of PoW system. ● Benchmarking the system performance. ● Project documentation and report generation
Shubham Jindal	● Designing and development of PoW system. ● Preparing test cases for the system. ● Testing the system for correctness and safety and report generation.

The subtasks mentioned above are not rigid and we will maintain flexibility in tasks carried out by the team members which will vary as per the requirement of the project and schedule of the members. All three of us will take an active part in designing the architecture of the system, developing it's modules and benchmarking but we have split other responsibilities like documentation, final testing, and presentation.

Weekly Plan

Week	Tasks
Week 1	● Read and understand the details of PoW consensus algorithm from the papers. ● Understand existing implementations' code base and finalize the design of our system. ● Start working on the DistAlgo implementation.
Week 2	● Complete the DistAlgo system with basic features. ● Document and report the development of system and progress in the project in parallel. ● Perform testing on the developed modules using predefined test cases.
Week 3	● Finalize the system implementation with all the required features. ● Perform testing and benchmarking of the final prototype. ● Finalize the documentation, reports, and slides for the final submission and presentation.

References

[1]Liu, Annie et. al. "DistAlgo Language", https://github.com/DistAlgo September 2018

[2]Porat, Amitai et. al. " Blockchain Consensus: An analysis of Proof-of-Work and its applications", http://www.scs.stanford.edu/17au-cs244b/labs/projects/porat_pratap_shah_adkar.pdf, December 2017

[3]Porat, Amitai et. al. " Blockchain Consensus: An analysis of Proof-of-Work and its applications", https://github.com/shahparth95/CS244Bproject, December 2017

[4]Dwork, Cynthia; Naor, Moni. "Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology". *CRYPTO'92: Lecture Notes in Computer Science No. 740*. Springer: 139–147. 1993

[5]Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[6]Mastering Bitcoin, https://github.com/bitcoinbook/bitcoinbook, November 2018

[7]Ethereum Homestead, http://ethdocs.org/en/latest/introduction/index.html, 2018

[8]Ethereum, https://github.com/ethereum, 2018

[9]Olivera,Matias "Interactive blockchain built with Node.js", https://github.com/olistic/simplechain, April 2018

[10]Raj, Koshik "Justblockchain", https://github.com/koshikraj/justblockchain, March 2018