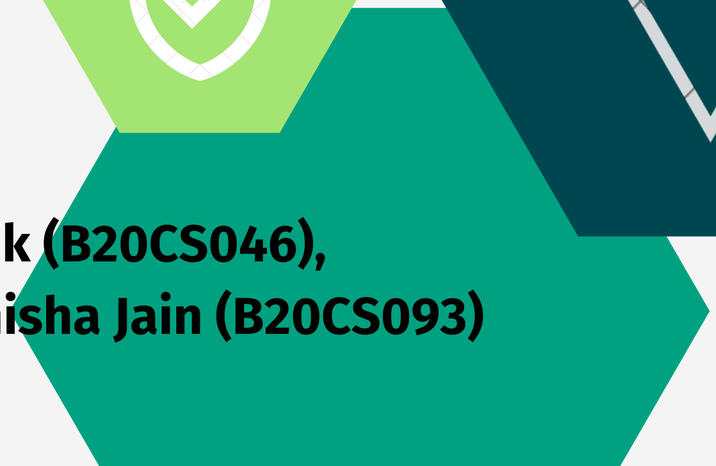
A Blockchain Communication Resource Optimization Consensus Method



Group no: 30

Anirudh Bajaj (B20CS005), Diksha Jena (B20CS013), R. Amshu Naik (B20CS046), Khobragade Atul Yashwant (B20CS027), Seema (B20CS064), Tanisha Jain (B20CS093)

Introduction

- Consensus is crucial for blockchain technology as it ensures that all network participants agree on the current state of the ledger, maintaining data integrity, decentralization, security, immutability, scalability, and effective governance in a decentralized system.
- Certain measures are taken to enable most nodes to agree on the same block. However, it also consumes huge computational, storage and communication resources, which makes the performance of the blockchain system low, and the more the number of nodes, the more prominent this drawback is.

Our Aim

CCRO implementation

- Reduced communication overhead
- Efficient resource utilization
- Speed and scalability
- The problems of low throughput and high transaction latency

Comparitive analysis of PBFT vs CCRO

- Throughput
- Consensus Time
- Message complexity

PBFT

Practical Byzantine Fault Tolerance

Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm designed for distributed systems to achieve consensus in the presence of Byzantine faults, which include arbitrary and potentially malicious behavior by nodes. Let's discuss PBFT in terms of complexity, fault tolerance, and node trust:

Fault Tolerance:

PBFT is designed to tolerate up to (n-1)/3 malicious or faulty nodes in a network of n nodes.

Node Trust:

PBFT assumes that a two-thirds majority of nodes are honest and correctly follow the protocol.

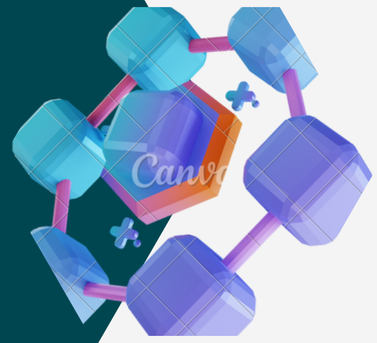
Complexity:

Message Complexity: PBFT has a message complexity of O(n^2), where n is the number of nodes in the network.

CCRO

(communication resource optimizational)

The CCRO consensus algorithm aims to reduce the communication overhead of consensus by dividing nodes into different domains and assigning different roles to nodes according to their trust levels. It introduces a new class of nodes called communication nodes, which are responsible for the delivery of messages in the consensus process.



Domain Partitioning

Communication Node Introduction

Message Complexity Reduction

Trust Based Role Assignment

Core concepts

Trust

Node trust in the consensus process is crucial for ensuring the alliance chain's state stability and is objectively evaluated .

Regionalization

Regionalization in blockchain involves organizing nodes into distinct domains, enhancing security by minimizing cross-platform interactions while maintaining scalability and data confidentiality within each domain

Communication resource optimization

Appoint trusted communication nodes to handle message transmission among consensus nodes, effectively reducing complexity and overhead in the consensus process

Message log

Message log records all consensus process messages, ensuring decentralization, with all nodes performing log backups and verifying voting information.

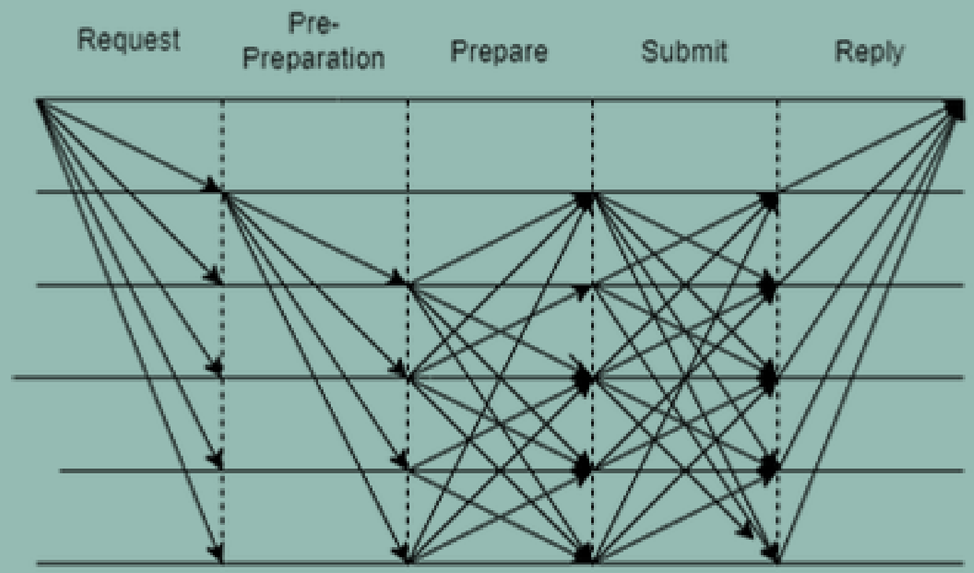
Back to Agenda Page

Methodology

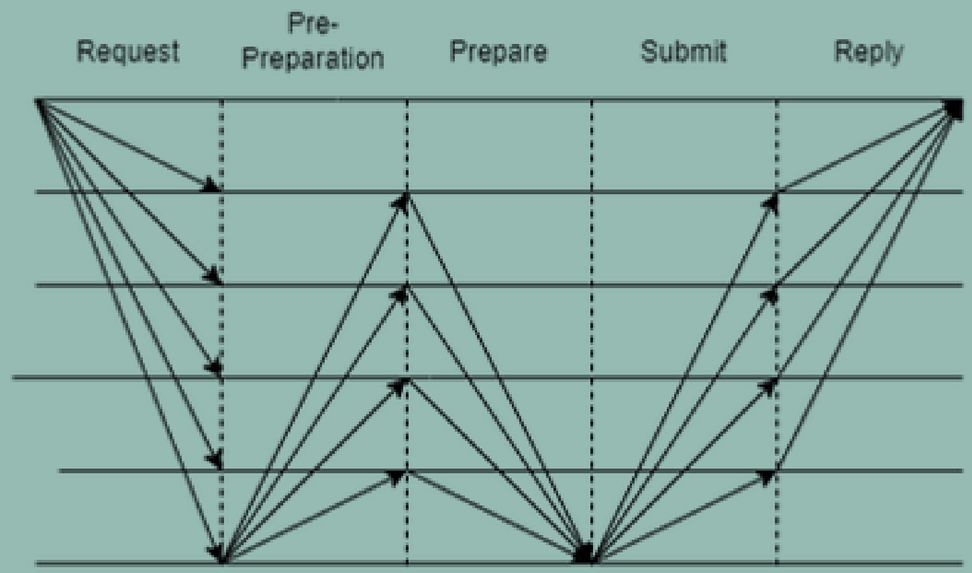
In the CCRO consensus algorithm, the methodology involves a systematic process for achieving agreement in distributed systems. The setup initializes nodes with specific roles and cryptographic keys.

- Node setup
- Role Assignment
- Data synchronization phase
- Request phase
- Monitor node status
- Verify data synchronization
- Pre-preparation phase
- Preparation phase
- Submission phase
- Reply phase
- Storage phase
- Analysis

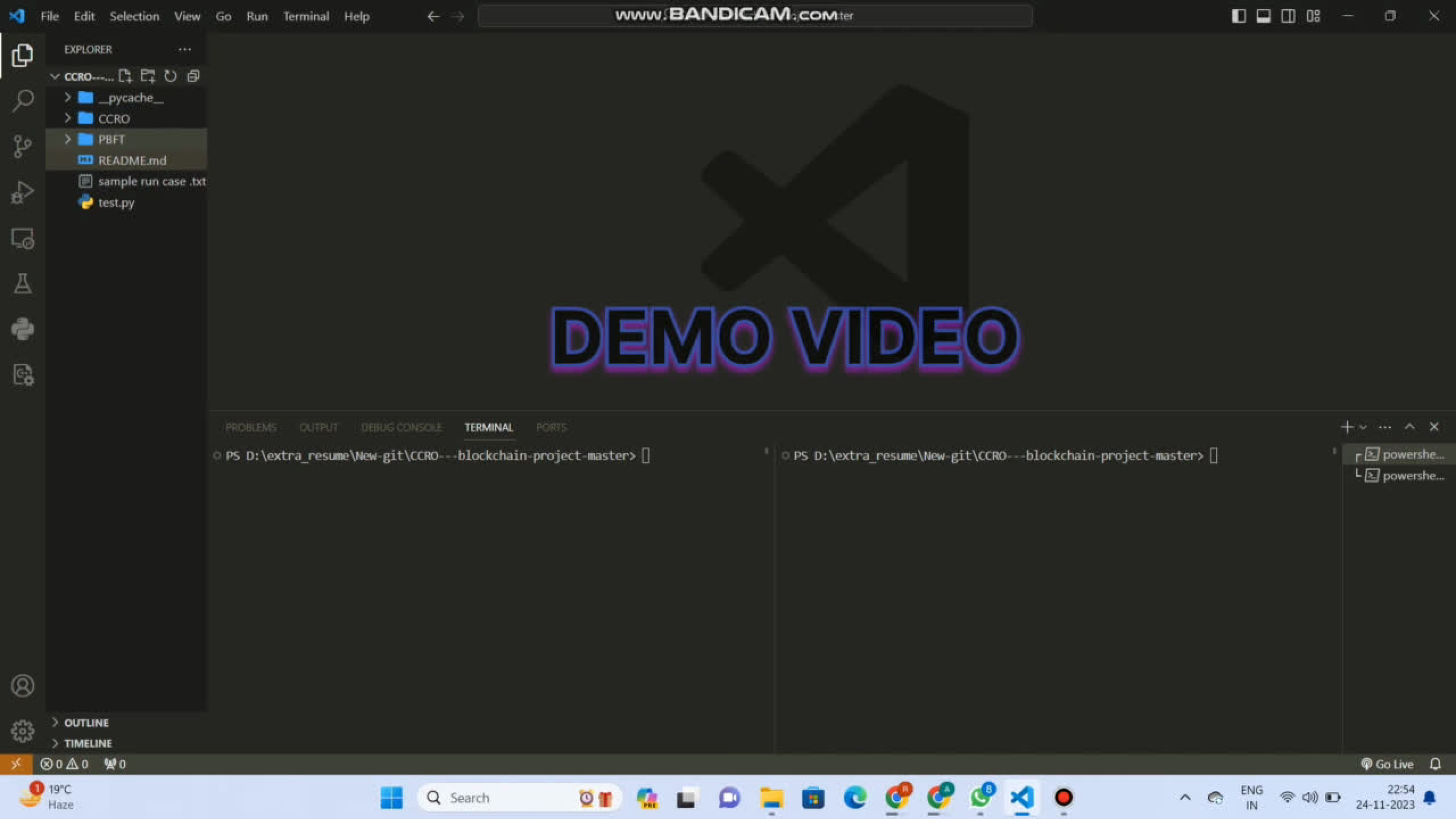
Consensus Flow



PBFT



CCRO


File Edit Selection View Go Run Terminal Help
www.BANDICAM.com
EXPLORER
CCRO---...
__pycache__
CCRO
PBFT
README.md
sample run case .txt
test.py
DEMO VIDEO
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS D:\extra_resume\New-git\CCRO---blockchain-project-master>
PS D:\extra_resume\New-git\CCRO---blockchain-project-master>
powershe...
powershe...
OUTLINE
TIMELINE
Go Live
19°C
Haze
Search
ENG
IN
22:54
24-11-2023

Result Comparision

The addition of communication node greatly reduces the message complexity in the consensus process and decreases the communication pressure of the system. It further shortens the consensus process cycle and effectively improves the efficiency of consensus.

	PBFT	CCRO
Consensus Time	**49.106875s**	**16.392194s**
Throughput	0.672 bytes/s	**2.013 bytes/s**
Message Complexity	o(n**2)	**O(2n+2)**
Latency	High	**Low**

Future Work and Scope

Domain Partitioning	Routing	Security analysis	
creating clusters for communication to handle tradeoff between no of nodes and latency,	Routing table domain based and complete nodes based	Node and fault tolerance	
Fixed entry point	**Real time trust assignment**		
Only entry from commander node was allowed. Should have been possible to exchange.	Trust is already assigned once and roles based on it. Should be updated at synchronizations.		
Hierarchical communication structure	**Lightweight Cryptography (ECC)**	**Adaptive domain formation**	**Hybrid consensus mechanism**
Organize nodes into levels, not just roles.	Like elliptic curve cryptography, and stream ciphers for security.	Create clusters based on work and demand instead of fixed,	use case based combinations with PoW, PoS etc

Resources

- *Jingchang Yu, Tao Shen, Fenhua Bai, Zhuo Yu, and Jianzhao Luo. 2022. A Blockchain Communication Resource Optimization Consensus Method. In Proceedings of the 2022 4th Blockchain and Internet of Things Conference (BIOTC '22). Association for Computing Machinery, New York, NY, USA, 107–114. https://doi.org/10.1145/3559795.3559810*
- PBFT implementation : https://github.com/rishnthan/practical-byzantine-fault-tolerance
- M. Hu, T. Shen, J. Men, Z. Yu and Y. Liu, "CRSM: An Effective Blockchain Consensus Resource Slicing Model for Real-Time Distributed Energy Trading," in IEEE Access, vol. 8, pp. 206876-206887, 2020, doi: 10.1109/ACCESS.2020.3037694.
- https://github.com/aclaussen1/CourseraCrypto-ConsensusFromTrust
- Bissias, George & Levine, Brian. (2020). Bobtail: Improved Blockchain Security with Low-Variance Mining. 10.14722/ndss.2020.23095.

Contributers

Great things in buisiness !

not that I'm so smart ?

R.Amshu naik
(B20CS046)

Tanisha Jain
(B20CS093)

Anirudh Bajaj
(B20CS005)

Seema
(B20CS064)

Diksha Jena
(B20CS013

Atul Khobragade
(B20CS027)

Tip: Collaboration makes teamwork easier! Click "Share" and invite your teammates to fill this up. Use this whiteboard page for bulletins, brainstorms, and other fun team ideas!

Back to Agenda Page

THANK YOU

NOVEMBER 2023

DEBASIS DAS