ISSN 2319-2720

Volume 12, No.4, October - December 2023

International Journal of Computing, Communications and Networking

Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn011242023.pdf

https://doi.org/10.30534/ijccn/2023/011242023

# Comparative Analysis of Deadlock Detection Algorithm based on Blockchain

**Nabeel Aslam[1], Ahsan Ali[2], Arfan Shahzad[3]**

[1] Department of Computer Science, University of Engineering and Technology, Pakistan, nabeelaslam2000@gmail.com

[2] Department of Computer Science, University of Engineering and Technology, Pakistan, ahsanmsuet@gmail.com

[3] Department of Computer Science, University of Engineering and Technology, Pakistan, arfanskp@gmail.com

Received Date : October 11, 2023 Accepted Date : November 20, 2023 Published Date : December 07, 2023

**ABSTRACT**

The aim of the study is to compare the deadlock detection algorithms in distributed systems with respective Blockchain technology presented in this paper. Today, detecting deadlocks in distributed systems is a very important challenge. Without the proper deadlock detection mechanism, the system can get stuck in a reject state. The goal of this work is to figure out which algorithm is more suitable for deadlock detection in Blockchain technology based on these factors i-e Security, Time, Performance, Communication, and Correctness. Under the positivism paradigm. The descriptive research design and distributed technique are used to minimize the occurrence of deadlock and to identify the deadlock in parallel collective operation verified up to maximum threads. The algorithms for deadlock detection that are compared in this study are Scalable deadlock detection, Push-relabel algorithm, Knapp's, Fulgor, and Consensus based on Blockchain technology. Blockchain technology provides a secure environment and helps to build trust. According to this paper, the Fulgor algorithm is more effective at removing deadlocks and maintaining communication security between distributed systems. Both controlled and uncontrolled environments are tested with different algorithms and are compared to define efficiency side-by-side. Deadlock detection requires identifying some properties and message delays in the global state of the distributed system. The number of common parameters has been identified in the selected algorithms to detect deadlocks in a distributed system

**Key words:** Collective, Deadlock, Blockchain, Consensus, Unified Parallel Resources

## 1. INTRODUCTION

A distributed system can communicate with each other by exchanging messages. It consists of collection of processes which execute on separate computers. Such a system different from multi-processing system in terms of shared memory and delays in messages send/receive is not negotiable [2]. Deadlock is difficult to locate and fix in application program. Unified parallel C is used for parallel execution and on shared distributed memory. It is an extension of C programing language [3]. Unified parallel C used the global address space. UPC-Check and UPC-Spin is the tool used for deadlock detection. UPC-Check used the algorithm that automatically detect deadlock. The scalable detection algorithm is not used only for collective operation. The runtime complexity of scalable algorithm is O (1). The algorithm has been detecting lock. The runtime complexity of the algorithm is shown to be O(T) where T is the number of thread. The parallel collective operation verified up to 8192 threads. Using the deadlock detection algorithm UPC-Check detects all deadlock error involving collective operations.

The push-relabel algorithm is to find the payment deadlock and flow in the payment channel network. This algorithm enables a concurrent execution without violating constraints. The system based on Blockchain technology such as Bitcoin. It is due to their requirements and not able to scale to high transaction rates [7]. In order to allow payment between any two nodes. Whether the nodes directly connected or not in payment channel network in which payment can be routed over more than one hop. This study claims that routing on single path restrict the transferrable amount and missed the many payment opportunities due to total available capacity in the payment network. Eventually, unable to used resource efficiently due to failed payment. This study proposing multiple paths to payment flow for entertain large number transaction in this paper. The push-relabel is particular suitable for route selection in payment network.

The Fulgor algorithm to resolve the problem of deadlock detection by identifying the pre-lock edges in an order that make sure the progress and maintain the protocol's privacy. Bitcoin is a worldwide payment system and the transaction of Bitcoin maintained in digital or public ledger which is known as blockchain. Database is used among mutually distributed users. The nature of Bitcoin protocol limits the scalability of the payment network. It is only tens of transactions per second. To resolve the issue, a system of off-chain payment channel has been introduced. The user can broadcast the new transaction of the current balance to the blockchain. This approach helps to open network channel path between users. The number of payments with only few interactions with the underlying blockchain. In this system the payment transaction

is secured by the Bitcoin script. Many participants face the problem of transaction privacy and concurrency problem In this paper, formalize the privacy standard and check the tradeoff between concurrency and privacy of the transaction. The payment network implementing the non-blocking progress that eventually reduce the secrecy set for sender and receiver of a payment, thereby fading the privacy standards [6].

Blockchain depends upon the consensus algorithm to resolve the deadlock in different environment. Blockchain Consensus algorithm is designed by properly conducted analysis and verification [8]. The proof-of-stake in consensus algorithm is Tendermint tool. It is software that consists of majorly two components a blockchain consensus engine and generic application interface. The study has verified that the consensus protocol is deadlock free. Many platforms such as Ripple are already using blockchain technology to support smart contract which allow the execution of random codes in distributed environment. In the blockchain network there is a fact that no centralized authority. All the members always agree to add new block in the blockchain network. The nodes might get disconnected from the blockchain network [1]. A fault tolerance protocol is agreed by all the connected nodes which are required to resolve the potential conflict. Consensus protocol nodes provide the computing power to solve the problem in order to add new block to the blockchain network. The most famous consensus is Bitcoin that solve the cryptographic hash problem as proof of work. If a node tries to manipulate the blockchain and the other nodes detect the malicious node, the locked-up stakes are suspended. Participants in the Tendermint tool are called validators. It is responsible for creating new block in blockchain. The height of the blockchain increase when they added a new block to the chain.

Deadlock detection and deadlock prevention are not that much useful to deal with deadlock and the deadlock identification is difficult to do [9]. The study is tried to identify the process or operation that may cause of the potential deadlock to minimize the chance of occurrence Message might be missed because of breaking and re-transmission of message between processes. This study has proposed Knapp's algorithm that are consist of four classes of distributed deadlock detection algorithm which classified in the following. Diffusion computation, path-pushing, edge-chasing and the global state detection. The algorithm maintains wait for graph to detect the distributed deadlock whereas in diffusion computation It used to detect dead-locks in the blockchain network [8]. The snapshot in global state detection based algorithm used to detect the distributed deadlock and also determine the type of the deadlock. The goal of the study is to identify that which algorithm is more suitable among all of these to detect the deadlock in distributed system with respective to blockchain technology e.g. performance, security, communication and correctness [10]. To handle deadlock is very challenging task in distributed system. Deadlock in the communication system mainly occurred due to lost or corrupted signal rather than resource contention.

## 2. LITERATURE REVIEW

As a first step, it identified different sources of relevant publications and specific resource providers. The list of these publishers includes Springer Link, IEEE Xplore. Deadlock detection in blockchain technology is new and unexplored concept. The scalability of blockchain is a major issue today with many different methods and approaches. A blockchain is a sequence of block each block maintains a hash value and link to its previous block [4]. Blockchain network keep track of blockchain and validate new block to the blockchain. The Blockchain technology is a completely distributed and public database or digital ledger for any type data interchange. The essential unit of blockchain is a block that records number of transaction made in a given time. The decentralize property of blockchain make it more powerful

### 2.1 Push-relabel Algorithm

The payment network routing possesses many challenges. In this algorithm, focus on route selection e.g. finding a route in payment network that fulfill certain constraints, creates a list of routes from the set of channels. They discuss a payment as a flow and to elaborate the chance of combined multiple paths. Most of the existing method required the global knowledge and a centralized coordinator [11]. The approach in push-relabel algorithm allows a concurrent execution but solves a flow problem. The distributed algorithm in contrast, makes sure the selected route in a flow. Moreover, it can be executed concurrently without disturbing the constraints [4] Payment flows between pairs of nodes in the network in which node s want to send payment to node t. The payment channel network work as a peer-to-peer network in which nodes can communicate directly with each other. In order to process the number of payments, a path between s and t must exist. Every path is the combination of payment channels in Figure 1.

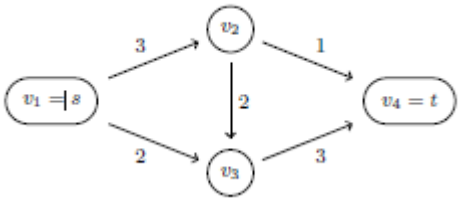


**Figure 1**: Payment Chanel network

### 2.2 Consensus algorithm

Each block in blockchain maintains the link to its previous block. The content of the existing block in blockchain cannot be change without modifying its hash value. The content of the block vary application to application. The header is used to store the signature of parent block [11]. A blockchain is a collection of nodes that are responsible for validating each new block in blockchain. Nodes can be categorized into two types on the bases of functionality, miners and validators. The Miners normally store only the last few blocks of the blockchain and for adding new blocks A validator store a

complete copy of blockchain and make sure the new block has been submitted by the miners is valid and fulfills the defined rules of blockchain [9]. According to the architecture of blockchain, it is possible for a node of network to be behaved like both a miner and validator at a same time. There is no centralized authority in blockchain. In proof of work the nodes are performing an operation that is agreed by a majority of nodes in the blockchain system [1]. To detect the participant's malicious activity and to solve the proof of work problem, new generation of blockchain like Ethereum have started to use the consensus algorithm as proof of stake.

### 2.3 Fulgor Algorithm

The payment channel network faces many difficulties such as privacy, concurrency routing and many more. Other solution proposed the network channel that reduces the time of coins that are locked in intermediate channels along with a payment path [12]. This study offers an algorithm to find multiple payment routes and ensure the privacy and scalability in the network. In which sender decide the route according to his criteria. A framework in payment channel allow user to execute small transfers without committing the transaction to the blockchain. They can update the balance of deposit by using smart contracts that ensure the agreement of both users on re-distribution of payment [5]. The capacity of channel is limited in each direction. The Bitcoin amount receives by each connected user in blockchain closing transaction according to the most recent distribution. A sender can send money to receiver even they do not open the channel between them. A deadlock occurs in payment network in which many simultaneous payment shares edges in their paths. Moreover, each payment in network holding an edge that does not capacity to entertain all transfer at a time that's why remaining payment wait for edge that is being held up another request of payment [18].

### 2.4 Scalable algorithm

Thread may cause of deadlock in distributed system due to out-of-order calls to collective operation. No-adherence can also a cause of deadlock of the program. However, this study introduces scalable algorithm to detect such type of error. Model checking tools like UPCSPIN and MPISPIN can detect all possible of condition of deadlock. DAMPI is a distributed deadlock detection algorithm and most practical method in term of scalability. In order to extend the limitation, utilize an efficient and flexible communication system to transfer record related to error detection between difference threads or processes. Scalable algorithm uses a different method to detect deadlock involving a collective operation. On-blocking communication between processes. The value passes to single valued arguments and the order of collective operation must be same on all process [14]. This research enhances this algorithm to detect deadlock involving locks and collective operation. The total number of threads represent by integer value. If the thread is completed its execution, then state of thread set to end of execution. The signature of collective process operation on a thread consists of the name of collective operation and the value which are passed to each argument of UPC on that particular thread.

### 2.5 Knapp's algorithm

It is easy to detect the deadlock in centralized system. Because centralized agent has complete information of all threads and process. Such can communicate directly with one another in which all thread in the set is waiting for an event to execute when a set of thread in a deadlocked state because of another thread in the set [13]. This study is mainly concerned about the resource acquisition and release. It can avoid deadlock by Knapp's algorithm and to overlook the issue by imagine that deadlock never occur in the blockchain system. The request for the resource can be entertain if there is no deadlock exists in the network. The system continuously checks the both safe and unsafe state in the system to detect the deadlock Figure 2.

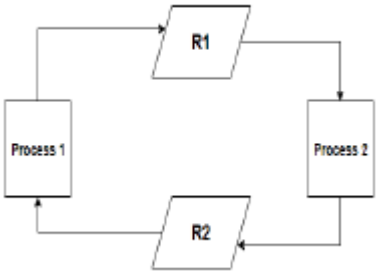


**Figure 2:** Deadlock situation

## 3. PROPOSED METHODOLGY

In the study, it checked which deadlock detection algorithm fulfills the research variables i.e. Security, Time, Performance, Cost, Communication and Correctness. It's compare different algorithm on the bases of previous study and representation of methodology in Figure 3.. There are no single criteria to judge these algorithms of deadlock detection. This study has considered approaches to deal with deadlock and malicious activity.

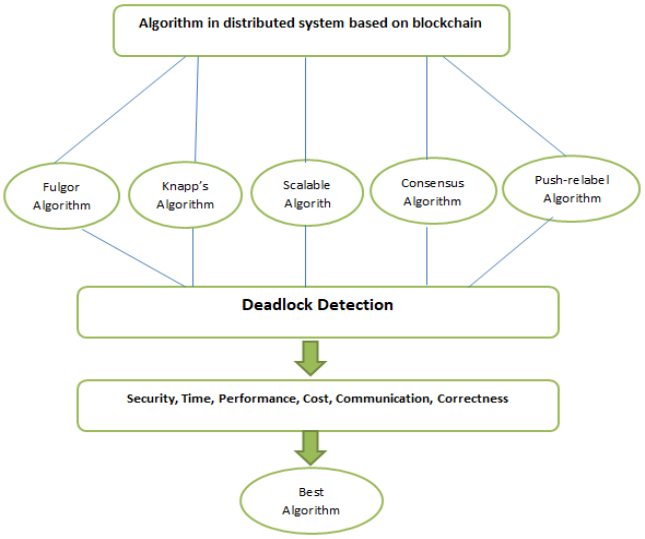


**Figure 3:** Methodology structure flow

There are five main steps of consensus algorithm are Propose, Prevote, Precommit, Commit and NewHeight as mentioned in below Figure 4.

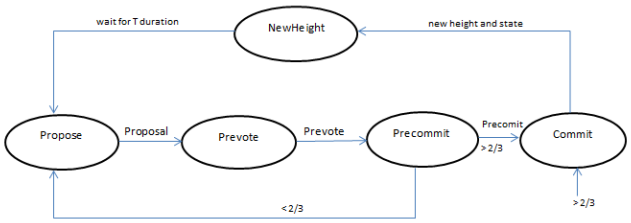


**Figure 4:** State machine of Consensus Algorithm

The above diagram is self-explanatory, as we added IP and location based checks with formal authentication [15]. In generic. In Prevote step, each validator request for a block and interact with its neighbor peer. A vote consists of the hash of block. All the nodes Prevote for their neighbors. In Pre commit step, the validator verifies that if it gets above 2/3 of Prevote for an acceptable block. If there is one, then the validator releases the existing lock on block and broadcast a Pre commit vote for this particular block. If the value less than 2/3 Prevote, then validator either lock or sign any block. At the end of Pre-commit, if the node has value more than 2/3 than it will proceed to commit step. In the last step two parallel conditions must be execute before the consensus algorithm back to propose step [9]. Finally, the node is to commits the block by the network so it can broadcast to other peers in blockchain [5]. The node must wait at least 2/3 commits of the current executing node block. After the duration complete, then consensus algorithm again moves to start from propose step.
The algorithm which provide the functionality of blocking protocol, maintain privacy and resolve the deadlock. The protocol maintains both concurrency and privacy of a transaction in the payment network. Each edge in the network has a unique IP address [16]. The user wants to send Bitcoin through an open channel. He will send a request to all edges to lock Bitcoin for amount of time. The request will be entertaining in lexicographic order according to edge ID. The time limit send to node in the network path should be long enough to enable a request to be sent to all nodes in the network path A large timespan allow malicious user to lock edge and prevent payment to transfer other peer in the network. If an edge does have capacity to lock another request, then it will send the abort message to sender through an open communication channel [19].

## 4. RESULTS AND DISCUSSION

In process normally deadlock arises when a process is in waiting state because the resource held by another one. In this case process unable to changes its state. In the communication system the reason behind the deadlock occurrence is due to lost or corrupt signal rather than the resource allocation. During the process of mining the check out the nodes of previous transaction to verify the give amount of crypto currency and check each amount of time it has to be adding to the chain to solve the complex problem of mathematical. The issue is to limit the possibility of a problematic entity to modify the Blockchain by false transactions [20]. The chance of attack is rare since the adding a new problematic block or manipulate a previous block to the chain would need control the most of the network nodes and make them agree for the change. It has to check the non-proposed block from the block chain network. It is just for the censorship or disruption of the service over the network. In both cases study tries to prevent from adding the malicious block in the Blockchain network. The proposer is choosing by round robin [17]. This study interested in an increase in transaction volume that can be accomplish this by joining the multiple paths. In this way, it can increase this volume of the transaction. The first result is to compare with single path route selection schemes

## 5. CONCLUSION

This study discussed that which approach is efficient for deadlock detection in block chain technology and for this used different protocol for the formal analysis and verification of the problematic nodes in the Blockchain network. It uses a consensus algorithm used the Tender mint and verified that it is free of deadlock. A new distributed and scalable deadlock algorithm for Unified collective operation is introduced. The algorithm has been proven to be correct and give the efficient run time of O (1). The algorithm has been extendable to detect deadlock that involve locks and runtime complexity of O (T). The payment channel network has to deal with different challenges such as concurrency and privacy. There is no routing algorithm offering full privacy and non-blocking progress. It transfers routes for a collection of payments in the network protocol that make sure that the network is deadlock free. The goal of the study is to identify which algorithm is more suitable among all of these to detect the deadlock in a distributed system with respect to Blockchain technology e.g. performance, security, communication and correctness. In the future, planning to modify the algorithm that chooses the proposer to avoid the nodes that are disconnected in the preceding nodes and implement a time lock protocol of consensus. It also works on synchronization and other prevention techniques to give more efficient result. It further proposed a protocol that ensures the desired privacy and deadlock free routings.

## ACKNOWLEDGEMENT

Special thanks to our teacher Muhammad Junaid Arshad for his support.

## REFERENCES

1. Alsaeedi, K., de Boer, F. S., & de Vink, E. (2018). **Deadlock detection for actor-based coroutines**. In International Symposium on Formal Methods. Springer.

2. Bhargavan, K., et al. (2016). **Formal verification of smart contracts**: Short paper. In Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security.
3. Daszczuk, W. B., & Zuberek, W. M. (2017). **Deadlock detection in distributed systems using the IMDS formalism and Petri nets**. In Advances in Dependability Engineering of Complex Systems. Springer, 118-130.
4. Decker, C., & Wattenhofer, R. (2015**). A fast and scalable payment network with bitcoin duplex micropayment channels**. In Symposium on Self-Stabilizing Systems. Springer.
5. Do-Mai, A.-T., Diep, T.-D., & Thoai, N. (2016**). Race condition and deadlock detection for large-scale applications**. 2016 15th International Symposium on Parallel and Distributed Computing (ISPDC). IEEE.
6. Dorri, A., et al. (2017). Blockchain: **A distributed solution to automotive security and privacy**. IEEE Communications Magazine, 55(12), 119-125.
7. Giachino, E., Laneve, C., & Lienhardt, M. (2016). **A framework for deadlock detection in core ABS. Software & Systems Modeling**, 15(4), 1013-1048.
8. Hussain, S., Sajjad, A., & Javed, Z. (2020). **Deadlock Detection in Distributed System** (No. 2476). EasyChair.
9. Jain, S., Kumar, N., & Chauhan, K. (Year not provided). **An Overview on Deadlock Resolution Techniques.**
10. Lazreg, A. B., Ben Arbia, A., & Youssef, H. (2020). **Cloudlet-Cloud Network Communication Based on Blockchain Technology**. 2020 International Conference on Information Networking (ICOIN). IEEE.
11. Lu, F., et al. (2019**). Deadlock detection-oriented unfolding of unbounded Petri nets**. Information Sciences, 497, 1-22.
12. Lu, W., et al. (2016). **A leader election based deadlock detection algorithm in distributed systems**. In Proceedings of the 1st international workshop on specification, comprehension, testing, and debugging of concurrent programs.
13. Lu, W., et al. (2017). **An efficient deadlock detection and resolution algorithm for generalized deadlocks**. INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING INFORMATION AND CONTROL, 13(2), 703-710.
14. Mitchell, D. P., & Merritt, M. J. (1984). **A distributed algorithm for deadlock detection and resolution**. In Proceedings of the third annual ACM symposium on Principles of distributed computing.
15. Rohrer, E., Laß, J.-F., & Tschorsch, F. (2017). **Towards a concurrent and distributed route selection for payment channel networks**. In Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, 411-419.
16. Roy, I., et al. (2013). **A scalable deadlock detection algorithm for UPC collective operations**. PGAS 13, 2-15.
17. Sherpa, S., Vicenciodelmoral, A., & Zhao, X. (2019). **Deadlock Detection for Concurrent Programs Using Resource Footprints**. In Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing Companion.
18. Shi, N. (2016). **A new proof-of-work mechanism for bitcoin**. Financial Innovation, 2(1), 31.
19. Singh, M., & Kim, S. (2018**). Branch-based blockchain technology in intelligent vehicle. Computer Networks**, 145, 219-231.
20. Thin, W. Y. M. M., et al. (2018). **Formal Analysis of a PoS Blockchain.**